

Cisco Identity Services Engine User Guide, Release 1.1

June 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-25537-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Identity Services Engine User Guide, Release 1.1
© 2012 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface xxix

Audience xxix

Document Organization xxx

Document Conventions xxxi

Documentation Updates xxxii

Related Documentation xxxii

Release-Specific Documents xxxiii

Platform-Specific Documents xxxiii

Notices xxxiv

OpenSSL/Open SSL Project xxxiv

License Issues xxxiv

Obtaining Documentation and Submitting a Service Request xxxvi

What's New in This Release xxxvii

Related Documentation xxxix

PART 1 **Introducing Cisco ISE**

CHAPTER 1 **Overview of Cisco ISE** 1-1

CHAPTER 2 **Understanding the User Interface** 2-1

Cisco ISE Internationalization and Localization 2-1

Inherent Usability 2-6

Elements of the User Interface 2-7

Primary Navigation Tabs and Menus 2-8

The Global Toolbar 2-9

Task Navigators 2-9

Getting Help 2-11

Global Help 2-11

Page-Level Help 2-11

Providing Feedback to Cisco 2-12

Introducing the Dashboard 2-12

Dashboard Elements 2-13

Drilling Down for Details 2-15

Common User Interface Patterns 2-16
Understanding the Impact of Roles and Admin Groups 2-19

PART 2 Administering Cisco ISE

CHAPTER 3 Cisco ISE Task Navigator 3-1
Navigating Multiple Task Procedures 3-1
Setup 3-3
Profiling 3-5
Basic User Authorization 3-6
Client Provisioning and Posture 3-7
Basic Guest Authorization 3-9
Advanced User Authorization 3-10
Advanced Guest Authorization 3-12

CHAPTER 4 Managing Identities and Admin Access 4-1
Configuring Access for Users, Endpoints, Admins, Groups, Permissions, and Accounts 4-2
Understanding User Identities, Groups, and Admin Access 4-2
Understanding Identity Management Terminology 4-4
Managing User Identity and Group Identity Types Using the User Interface 4-5
Network Access Users 4-9
Configuring Network Access and Sponsor Users 4-9
Endpoints 4-15
Configuring Endpoints 4-16
Filtering Endpoints 4-16
Creating an Endpoint 4-18
Editing an Endpoint 4-19
Deleting an Endpoint 4-20
Importing Endpoints 4-21
Importing Endpoints from an LDAP Server 4-22
Exporting Endpoints 4-25
Latest Network Scan Results 4-26
Understanding Admin Access Terminology 4-26
Managing Admin Access Types Using the User Interface 4-29
Configuring Cisco ISE Administrators 4-33
Configuring Admin Groups 4-37
Configuring User Identity Groups 4-40

Configuring Cisco ISE for Administrator Access Using an External Identity Store 4-44
External Authentication + External Authorization 4-45
External Authentication + Internal Authorization 4-47
Managing Admin Access (RBAC) Policies 4-49
Configuring RBAC Permissions 4-49
Configuring Menu Access Permissions 4-49
Viewing Predefined Menu Access Permissions 4-50
Creating Custom Menu Access Permissions 4-51
Updating Menu Access Permissions 4-52
Duplicating Menu Access Permissions 4-52
Deleting Menu Access Permissions 4-53
Configuring Data Access Permissions 4-53
Viewing Predefined Data Access Permissions 4-53
Creating Custom Data Access Permissions 4-54
Updating Data Access Permissions 4-55
Duplicating Data Access Permissions 4-55
Deleting Data Access Permissions 4-56
Configuring RBAC Policies 4-56
Using Predefined RBAC Policies 4-56
Creating Custom RBAC Policy 4-57
Configuring Settings for Accounts 4-60
Administrator Access Settings 4-60
Restricting Administrative Access to the Management Interfaces 4-61
Configuring a Password Policy for Administrator Accounts 4-62
Configuring Session Timeout for Administrators 4-64
Changing Administrator Name 4-65
Configuring Network Access for User Accounts 4-65
User Custom Attributes Policy 4-66
Configuring Network Access User Accounts 4-67
Endpoint Identity Groups 4-70
Filtering, Creating, Editing, and Deleting Endpoint Identity Groups 4-71
Filtering Endpoint Identity Groups 4-71
Creating, Editing, and Deleting an Endpoint Identity Group 4-73
Adding and Removing Endpoints in an Endpoint Identity Group 4-75
Adding Endpoints in an Endpoint Identity Group 4-76
Removing Endpoints in an Endpoint Identity Group 4-76

CHAPTER 5 **Managing External Identity Sources** 5-1

Certificate Authentication Profiles 5-2

Adding or Editing a Certificate Authentication Profile 5-2
Microsoft Active Directory 5-4
Key Features of the Integration of ISE and Active Directory 5-4
Integrating ISE with Active Directory 5-6
Enabling Active Directory Debug Logs 5-15
Supplemental Information 5-16
Configure Group Policy in Active Directory 5-16
Configure Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory 5-17
Configure AnyConnect Agent for Machine Authentication 5-17
LDAP 5-17
Key Features of Integration of ISE and LDAP 5-18
Adding and Editing LDAP Identity Sources 5-22
RADIUS Token Identity Sources 5-32
Key Features of the Integration of ISE and RADIUS Identity Source 5-33
Adding or Editing a RADIUS Token Server 5-36
Deleting a RADIUS Token Server 5-39
RSA Identity Sources 5-39
Integrating ISE with RSA SecurID Server 5-40
Adding and Editing RSA Identity Sources 5-42
Configuring RSA Prompts 5-48
Configuring RSA Messages 5-49
Identity Source Sequences 5-51
Creating Identity Source Sequences 5-52
Deleting Identity Source Sequences 5-53
Viewing and Monitoring the Identity Sources 5-54

CHAPTER 6 **Managing Network Devices** 6-1
Managing Network Devices 6-1
Adding and Editing Devices 6-3
Deleting a Device 6-6
Filtering Network Devices on the Network Devices Page 6-7
Configuring a Default Device 6-9
Managing Network Device Groups 6-10
Creating a Network Device Group 6-11
Editing a Network Device Group 6-12
Deleting a Network Device Group 6-13
Importing Network Devices and Network Device Groups 6-14
Exporting Network Devices and Network Device Groups 6-21

CHAPTER 7 **Managing Resources** 7-1

Dictionaries and Dictionary Attributes 7-1
Dictionary and Attribute User Interface 7-2
Configuring Dictionaries and Dictionary Attributes 7-2
Managing Dictionary Attributes in System-Defined Dictionaries 7-2
Configuring User-Defined Dictionaries and Dictionary Attributes 7-4
Configuring RADIUS Vendors 7-8
Creating and Editing RADIUS Vendors 7-9
Creating and Editing RADIUS VSAs 7-9
Deleting RADIUS Vendors 7-10
Importing and Exporting RADIUS Vendor Dictionary 7-11

CHAPTER 8 **Administering Cisco ISE** 8-1

Logging In 8-1
Administrator Lockout Following Failed Login Attempts 8-2
Enabling FIPS Mode in Cisco ISE 8-2
Cisco NAC Agent Requirements when FIPS Mode is Enabled 8-4
Configuring Cisco ISE for Administrator CAC Authentication 8-4
Preliminary Setup Done by ISE Administrator 8-5
Step 1: Enable FIPS Mode 8-6
Step 2: Configure Active Directory 8-6
Step 3: Create Certificate Authentication Profile 8-9
Step 4: Import CA Certificates into ISE Certificate Trust Store 8-9
Step 5: Configure CA Certificates for Revocation Status Check 8-10
Step 6: Enable Client Certificate-Based Authentication 8-12
Step 7: Configure Admin Group to AD Group Mapping 8-13
Step 8: Configure Admin Authorization Policy 8-16
Specifying Proxy Settings in Cisco ISE 8-17
System Time and NTP Server Settings 8-18
Configuring Email Settings 8-20
Configuring System Alarm Settings 8-21
Configuring Alarm Syslog Targets 8-22
Managing Software Patches 8-24
Installing a Software Patch 8-24
Rolling Back Software Patches 8-28
Viewing Patch Install and Rollback Changes in the Audit Report 8-29

CHAPTER 9 **Setting Up Cisco ISE in a Distributed Environment** 9-1

Understanding Node Types, Personas, Roles, and Services 9-2
Cisco ISE Deployment Terminology 9-2
Types of Nodes 9-2
Cisco ISE Nodes and Available Menu Options 9-4
Understanding Distributed Deployment 9-5
Guidelines for Setting Up a Distributed Deployment 9-6
Configuring a Cisco ISE Node 9-7
Configuring a Primary Administration Cisco ISE Node 9-11
Registering and Configuring a Secondary Node 9-13
Configuring Administration Cisco ISE Nodes for High Availability 9-15
Viewing Nodes in a Deployment 9-17
Managing Node Groups 9-19
Creating, Editing, and Deleting Node Groups 9-21
Changing Node Personas and Services 9-23
Configuring Monitoring ISE Nodes for Automatic Failover 9-24
Removing a Node from Deployment 9-26
Changing the IP Address of the Monitoring Node 9-27
Replacing the Cisco ISE Appliance Hardware 9-28

CHAPTER 10 **Setting Up Inline Posture** 10-1

Inline Posture Known Limitations 10-1
Understanding the Role of Inline Posture 10-1
Planning an Inline Posture Deployment 10-4
About Inline Posture Configuration 10-4
Choosing an Inline Posture Operating Mode 10-5
Best Practices for Inline Posture 10-7
Standalone Mode or High Availability 10-8
Inline Posture High Availability 10-9
Inline Posture Guidelines for Distributed Deployment 10-11
Deploying an Inline Posture Node 10-12
Configuring Inline Posture for High Availability 10-24
Configuring a High Availability Pair 10-25
Syncing an Inline Posture Node 10-28
Adding Inline Posture as a RADIUS Client 10-29
Monitoring an Inline Posture Node 10-30
Removing an Inline Posture Node from Deployment 10-31

Remote Access VPN Use Case 10-31
Configuring a Cisco ISE Deployment Using an Inline Posture Node 10-33

CHAPTER 11 **Setting Up Endpoint Protection Services** 11-1
About Endpoint Protection Services 11-1
EPS Functional Overview 11-1
Enabling and Disabling EPS 11-3
EPS Authorization 11-4
Controlling Endpoints 11-6
Monitoring EPS Data 11-8

CHAPTER 12 **Managing Licenses** 12-1
Understanding Licensing 12-1
Viewing Current Licenses 12-2
Viewing Licensing History 12-3
Adding and Upgrading Licenses 12-3
Removing Licenses 12-4

CHAPTER 13 **Managing Certificates** 13-1
Local Server Certificates 13-2
Viewing Local Certificates 13-3
Adding a Local Certificate 13-4
Importing a Server Certificate 13-5
Generating a Self-Signed Certificate 13-7
Generating a Certificate Signing Request 13-8
Binding a CA-Signed Certificate 13-10
Editing a Local Certificate 13-11
Deleting a Local Certificate 13-13
Exporting a Local Certificate 13-13
Certificate Signing Requests 13-15
Viewing and Exporting Certificate Signing Requests 13-15
Deleting a Certificate Signing Request 13-16
Certificate Authority Certificates 13-16
Viewing Certificate Authority Certificates 13-17
Adding a Certificate Authority Certificate 13-18
Editing a Certificate Authority Certificate 13-19
Deleting a Certificate Authority Certificate 13-22
Exporting a Certificate Authority Certificate 13-22

Importing Certificate Chains 13-23
Creating Certificate Trust Lists in the Primary ISE Node 13-23
Importing Root and CA Certificates into the CTL of the Primary Node 13-23
Importing the CA-Signed Certificate from the Secondary Node into the Primary Node's CTL 13-24
Importing the Self-Signed Certificate from the Secondary Node into the CTL of the Primary Node 13-24
OCSP Services 13-25
OCSP Certificate Status Values 13-25
OCSP High Availability 13-26
OCSP Failures 13-26
Viewing OCSP Services 13-27
Adding, Editing, or Duplicating OCSP Services 13-27
Deleting an OCSP Service 13-30
OCSP Statistics Counters 13-30
Monitoring OCSP 13-31
OCSP Monitoring Report 13-31

CHAPTER 14 **Logging 14-1**
Understanding Logging 14-1
Configuring Local Log Settings 14-2
Understanding Remote Logging Targets 14-2
Configuring Remote Logging Targets 14-2
Understanding Logging Categories 14-5
Searching Logging Categories 14-6
Editing Logging Categories 14-7
Viewing Message Catalog 14-8
Understanding Debug Log Configuration 14-8
Configuring Debug Log Level 14-9
Viewing Log Collection Status 14-11
Viewing Log Collection Details 14-11

CHAPTER 15 **Managing Cisco ISE Backup and Restore Operations 15-1**
Overview of Cisco ISE Backup and Restore 15-1
Supported Scenarios for Backup, Restore, and Upgrade 15-2
Configuring Repositories 15-3
Creating Repositories 15-3
Deleting Repositories 15-5
On-Demand Backup 15-5

Running On-Demand Backup 15-5
Scheduled Backups 15-6
Scheduling a Backup 15-7
Deleting a Scheduled Backup 15-9
Viewing Backup History 15-10
Restoring Data from a Backup 15-11
Viewing Restore History 15-12
Synchronizing Primary and Secondary Nodes in a Distributed Environment 15-12
Recovering Lost Nodes in Standalone and Distributed Deployments 15-13
Loss of All Nodes in a Distributed Setup, Recovery Using Existing IP Addresses and Hostnames 15-13
Loss of All Nodes in a Distributed Deployment, Recovery Using New IP Addresses and Hostnames 15-14
Standalone Deployment, Recovery Using Existing IP Address and Hostname 15-15
Standalone Deployment, Recovery Using New IP Address and Hostname 15-15
Configuration Rollback 15-16
Primary Node Failure in a Distributed Deployment 15-16
Secondary Node Failure in a Distributed Deployment 15-16

PART 3 **Managing Cisco ISE Policy Models**

CHAPTER 16 **Managing Authentication Policies** 16-1
Understanding Authentication Policies 16-1
Authentication Type, Protocols, and Databases 16-2
Authentication Policy Terminology 16-3
Simple Authentication Policies 16-4
Rule-Based Authentication Policies 16-5
Protocol Settings 16-10
Configuring EAP-FAST Settings 16-10
Generating the PAC for EAP-FAST 16-11
Configuring EAP-TLS Settings 16-12
Configuring PEAP Settings 16-12
Network Access Service 16-13
Allowed Protocols 16-13
Defining Allowed Protocols 16-14
Deleting Allowed Protocols 16-21
Proxy Service 16-21
Defining an External RADIUS Server 16-22
Creating RADIUS Servers 16-23

Editing RADIUS Servers 16-24
Deleting RADIUS Servers 16-25
Defining a RADIUS Server Sequence 16-25
Creating, Editing, and Duplicating RADIUS Server Sequences 16-25
Configuring the Simple Authentication Policy 16-26
Configuring a Simple Policy Using RADIUS Server Sequence 16-29
Configuring the Rule-Based Authentication Policy 16-29
Understanding the Authentication Policy User Interface Elements 16-30
Simple Conditions 16-31
Creating Simple Conditions 16-31
Deleting Simple Conditions 16-32
Compound Conditions 16-33
Creating Compound Conditions 16-33
Deleting Compound Conditions 16-35
Creating a Rule-Based Authentication Policy 16-36
Authentication Policy Built-In Configurations 16-38
Viewing Authentication Results 16-41

CHAPTER 17 **Managing Authorization Policies and Profiles** 17-1
Understanding Authorization Policies 17-1
Understanding Authorization Policy Terminology 17-2
Cisco ISE Authorization Policies and Profiles 17-5
Authorization Policy Window 17-5
Authorization Policies and Supported Dictionaries 17-8
Authorization Profile Window 17-8
Authorization Policy and Profile Guidelines 17-9
Authorization Policy and Profile User Interface 17-10
Authorization Policy, Rule, and Profile Configuration Defaults 17-10
Configuring Authorization Policies 17-14
Configuring Policy Elements Conditions 17-17
Simple Conditions 17-18
Compound Conditions 17-18
Configuring Authorization Policy Conditions 17-19
Configuring Time and Date Conditions 17-23
Configuring Permissions for Authorization Profiles 17-27
Configuring Permissions for Downloadable ACLs 17-33
Configuring DACLs 17-33
Configuring Policies for SGACLs 17-36

Machine Access Restriction and Active Directory Users 17-36

CHAPTER 18 **Configuring Endpoint Profiling Policies** 18-1

Profiling Service in Cisco ISE 18-2

Understanding the Profiling Service 18-2

Endpoint Profiling 18-3

Licenses for the Profiling Service 18-4

Deploying the Profiling Service 18-4

Configuring the Profiling Service in Cisco ISE 18-5

Profiled Endpoints Dashlet 18-6

Viewing Profiler Reports 18-7

Change of Authorization 18-8

CoA Exemptions 18-10

CoA Global Configuration 18-12

Configuring the Probes 18-12

Filtering Endpoint Attributes 18-14

Configuring the NetFlow Probe 18-14

Configuring the DHCP Probe 18-16

Configuring the DHCP SPAN Probe 18-18

Configuring the HTTP Probe 18-19

Configuring the RADIUS Probe 18-20

Configuring the Network Scan (NMAP) Probe 18-21

A Network Scan 18-22

Latest Network Scan Results 18-23

Configuring the DNS Probe 18-23

Configuring the SNMP Query Probe 18-25

CDP Attributes Collection 18-26

LLDP Attributes Collection 18-26

LLDP-MIB (v1) 18-27

Configuring the SNMP Trap Probe 18-28

Simple Network Management Protocol 18-30

Endpoint Profiling Policies 18-35

Filtering, Creating, Editing, Duplicating, Importing, and Exporting Endpoint Profiling Policies 18-37

Filtering Endpoint Policies 18-37

Creating an Endpoint Profiling Policy 18-40

A Quick Reference to Creating a New Endpoint Profiling Policy in Cisco ISE 18-44

Editing an Endpoint Profiling Policy 18-49

Deleting an Endpoint Profiling Policy 18-50

Duplicating an Endpoint Profiling Policy 18-50

Exporting Endpoint Profiling Policies 18-51
Importing Endpoint Profiling Policies 18-51
Endpoint Profiling 18-52
Filtering, Creating, Editing, and Deleting a Profiling Condition 18-53
Filtering Conditions 18-53
Creating a Profiling Condition 18-55
Editing a Profiling Condition 18-56
Deleting a Profiling Condition 18-57
Profiling Results 18-57
Profiling Exception Actions 18-58
Filtering, Creating, Editing, and Deleting a Profiling Exception Action 18-58
Filtering Exception Actions 18-59
Creating an Exception Action 18-61
Editing an Exception Action 18-61
Deleting an Exception Action 18-62
Profiling Network Scan Actions 18-62
Filtering, Creating, Editing, and Deleting a Profiling Network Scan Action 18-63
Filtering Network Scan Actions 18-63
Creating a Network Scan Action 18-65
Editing a Network Scan Action 18-66
Deleting a Network Scan Action 18-67
Endpoint Profiling by Integrating Network Mapper in Cisco ISE 18-67
Endpoint Scan 18-68
Endpoint Profiling by Using an IOS Sensor on a Network Access Device 18-69
Integrating an IOS Sensor with Cisco ISE 18-69
An IOS Sensor and Analyzers 18-70
Endpoint Profiling in Cisco ISE with an IOS Sensor Enabled on NADs 18-71
Auto Smartports Configuration in Cisco ISE 18-72
macro auto execute 18-73
RADIUS Accounting Reports 18-74
Excluding Static Endpoints in Advanced Licenses 18-74
IP Address and MAC Address Binding in Cisco ISE 18-75
Integrating Cisco ISE with Cisco Network Admission Control Appliance 18-75
Configuring Cisco Clean Access Managers in Cisco ISE 18-76
Filtering, Adding, Editing, and Deleting Clean Access Managers in Cisco ISE 18-77
Filtering Cisco Clean Access Managers in Cisco ISE 18-78
Adding Cisco Clean Access Managers to Cisco ISE 18-80
Editing Cisco Clean Access Managers in Cisco ISE 18-80
Deleting Cisco Clean Access Managers in Cisco ISE 18-81

CHAPTER 19 **Configuring Client Provisioning Policies** 19-1

Client Provisioning Overview 19-1
Cisco ISE Agents 19-1
Cisco NAC Agent for Windows Clients 19-1
Cisco NAC Agent for Macintosh Clients 19-2
NAC Web Agent 19-3
Agent and Client Machine Operating System Compatibility 19-3
Adding and Removing Agents and Other Resources 19-4
Viewing and Displaying Client Provisioning Resources 19-4
Adding Client Provisioning Resources to Cisco ISE 19-5
Adding Client Provisioning Resources from a Remote Source 19-5
Adding Client Provisioning Resources from a Local Machine 19-6
Creating Agent Customization Files to Add to Cisco ISE 19-7
Creating Agent Profiles 19-12
Creating Windows Agent Profiles in Cisco ISE 19-12
Creating Mac OS X Agent Profiles in Cisco ISE 19-14
Modifying Windows and Mac OS X Agent Profiles in Cisco ISE 19-15
Agent Profile Parameters and Applicable Values 19-16
Deleting Client Provisioning Resources 19-24
Provisioning Client Machines with the Cisco NAC Agent MSI Installer 19-24
Setting Up Global Client Provisioning Functions 19-26
Enabling and Disabling the Client Provisioning Service 19-26
Downloading Client Provisioning Resources Automatically 19-27
Configuring Client Provisioning Resource Policies 19-28
Client-side Installation and Log-In 19-30
Viewing Client Provisioning Reports and Events 19-36
Viewing Client Provisioning Reports in Cisco ISE 19-36
Viewing Client Provisioning Event Logs in Cisco ISE 19-40

CHAPTER 20 **Configuring Client Posture Policies** 20-1

Posture Service 20-2
Understanding the Posture Service 20-3
Posture and Client Provisioning Services 20-4
Posture and Client Provisioning Policies Flow 20-5
Licenses for the Posture Service 20-5
Deploying the Posture Service 20-6
Configuring the Posture Service in Cisco ISE 20-6
Posture Compliance Dashlet 20-8
Viewing Posture Reports 20-8

Posture Administration Settings in Cisco ISE 20-9
Posture General Settings 20-10
Posture Reassessments 20-12
Initiating and Requesting a PRA 20-13
PRA Failure Actions 20-13
User Identity Group (Role) Assignment 20-14
PRA Report Tracking and Enforcement 20-15
PRA Enforcement During Distributed System Failure 20-15
Configuring Client Posture Periodic Reassessments 20-15
Posture Updates 20-22
Dynamic Posture Updates 20-22
Offline Posture Updates 20-24
Posture Acceptable Use Policy 20-24
Configuring Acceptable Use Policies 20-26
Client Posture Assessments in Cisco ISE 20-32
Client Posture Assessment Policies 20-33
Simplified Posture Policy Configuration 20-34
Creating, Duplicating, and Deleting Client Posture Policies 20-35
Creating a New Posture Policy 20-35
Duplicating a Posture Policy 20-40
Deleting a Posture Policy 20-40
Posture Assessment and Remediation Options in Cisco ISE 20-41
Custom Conditions for Posture 20-42
File Conditions 20-44
Configuring File Conditions 20-44
Viewing File Conditions 20-44
Creating, Duplicating, Editing, and Deleting a File Condition of FileExistence Type 20-45
Creating, Duplicating, Editing, and Deleting a File Condition of FileDate Type 20-47
Creating, Duplicating, Editing, and Deleting a File Condition of FileVersion Type 20-50
Filtering File Conditions 20-53
Registry Conditions 20-55
Configuring Registry Conditions 20-55
Viewing Registry Conditions 20-56
Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryKey Type 20-56
Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValue Type 20-59
Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValueDefault Type 20-63
Filtering Registry Conditions 20-66
Application Conditions 20-68

Configuring Application Conditions 20-69
Viewing Application Conditions 20-69
Creating, Duplicating, Editing, and Deleting an Application Condition 20-69
Filtering Application Conditions 20-71
Service Conditions 20-74
Configuring Service Conditions 20-75
Viewing Service Conditions 20-75
Creating, Duplicating, Editing, and Deleting a Service Condition 20-75
Filtering Service Conditions 20-77
Compound Conditions 20-80
Configuring Compound Conditions 20-80
Viewing Compound Conditions 20-81
Creating, Duplicating, Editing, and Deleting a Compound Condition 20-81
Filtering Compound Conditions 20-84
Antivirus and Antispyware Compound Conditions 20-86
Antivirus Compound Conditions 20-88
Configuring Antivirus Compound Conditions 20-88
Creating, Duplicating, Editing, and Deleting an Antivirus Compound Condition 20-88
Filtering Antivirus Compound Conditions 20-92
Antispyware Compound Conditions 20-94
Configuring Antispyware Compound Conditions 20-94
Creating, Duplicating, Editing, and Deleting an Antispyware Compound Condition 20-95
Filtering Antispyware Compound Conditions 20-98
Dictionary Simple Conditions 20-100
Configuring Dictionary Simple Conditions 20-100
Creating, Duplicating, Editing, and Deleting a Dictionary Simple Condition 20-100
Filtering Dictionary Simple Conditions 20-102
Dictionary Compound Conditions 20-104
Configuring Dictionary Compound Conditions 20-104
Creating, Duplicating, Editing, and Deleting a Dictionary Compound Condition 20-105
Filtering Dictionary Compound Conditions 20-108
Posture Results 20-111
Custom Posture Remediation Actions 20-112
Configuring Custom Posture Remediation Actions 20-113
File Remediation 20-114
Viewing, Adding, and Deleting a File Remediation 20-115
Filtering File Remediations 20-116
Link Remediation 20-119

Adding, Duplicating, Editing, and Deleting a Link Remediation 20-119
Filtering Link Remediations 20-122
Antivirus Remediation 20-124
Adding, Duplicating, Editing, and Deleting an Antivirus Remediation 20-125
Filtering Antivirus Remediations 20-127
Antispyware Remediation 20-130
Adding, Duplicating, Editing, and Deleting an Antispyware Remediation 20-130
Filtering Antispyware Remediations 20-133
Launch Program Remediation 20-135
Adding, Duplicating, Editing, and Deleting a Launch Program Remediation 20-135
Filtering Launch Program Remediations 20-139
Windows Update Remediation 20-141
Adding, Duplicating, Editing, and Deleting a Windows Update Remediation 20-142
Filtering Windows Update Remediations 20-146
Windows Server Update Services Remediation 20-148
Adding, Duplicating, Editing, and Deleting a Windows Server Update Services Remediation 20-149
Filtering Windows Server Update Services Remediations 20-153
Client Posture Assessment Requirements 20-155
Creating, Duplicating, and Deleting Client Posture Requirements 20-157
Creating a New Posture Requirement 20-157
Duplicating a Posture Requirement 20-161
Deleting a Posture Requirement 20-161
Custom Authorization Policies for Posture 20-162
Standard Authorization Policies for a Posture 20-163
Creating, Duplicating, and Deleting a Standard Authorization Policy for a Posture 20-164
Custom Permissions for Posture 20-167

CHAPTER 21 **User Access Management** 21-1
Overview 21-2
Guest Services Functionality 21-2
NAD with Central WebAuth 21-3
Wireless LAN Controller with Local WebAuth 21-4
Wired NAD with Local WebAuth 21-5
Device Registration WebAuth 21-8
Cisco ISE Guest Service Components 21-11
Cisco ISE Guest Service Default Portals 21-11
Guest Licensing 21-12

Guest High Availability and Replication 21-13
Guest Service Control 21-14
Operating System and Browser Support 21-14
Configuring Guest Policy Conditions 21-14
Simple Conditions 21-14
Creating Simple Conditions 21-15
Compound Conditions 21-15
Creating Compound Conditions 21-16
Sponsor Group Policy 21-16
Creating a New Sponsor Group Policy 21-17
Sponsor Groups 21-20
Creating and Editing Sponsor Groups 21-21
Deleting the Sponsor Group 21-22
Mapping Active Directory Groups to Sponsor Groups 21-23
Creating and Testing Sponsor User to Access the Sponsor Portal 21-24
Creating Guest Users 21-26
SMTP Server Settings for Email Notifications 21-27
General Settings 21-27
Setting Ports for the Sponsor and Guest Portals 21-28
Purging Guest User Records 21-28
Sponsor Settings 21-29
Specifying an Authentication Source 21-29
Specifying a Simple URL for Sponsor Portal Access 21-30
Creating a Custom Portal Theme 21-31
Applying Language Templates 21-34
Internationalization and Localization 21-35
Configuring Sponsor Language Templates 21-37
Configuring a Template to Create a Single Guest Account 21-40
Configuring a Template for Guest Notification 21-41
Guest Settings 21-45
Configuring Details Policy 21-45
Configuring Guest Language Templates 21-47
Multi-Portal Configurations 21-49
Hosting Multiple Portals 21-50
Sample HTML Code for Creating Portal Pages 21-54
Configuring Guest Portal Policy 21-68
Configuring Guest Password Policy 21-69
Time Profiles 21-70

Adding, Editing, or Duplicating Time Profiles 21-71
Deleting Time Profiles 21-72
Configuring Guest Username Policy 21-73
Monitoring Sponsor and Guest Activity 21-74
Audit Logging 21-75

CHAPTER 22 **Configuring Cisco Security Group Access Policies** 22-1
Understanding the SGA Architecture 22-1
SGA Features and Terminology 22-2
SGA Requirements 22-4
Configuring ISE to Enable the SGA Solution 22-5
Configuring SGA Settings on the Switches 22-6
Configuring SGA Devices 22-6
Configuring Security Group Access Settings 22-8
Configuring Security Group Access AAA Servers 22-9
Adding and Editing Security Group Access AAA Servers 22-10
Configuring Security Groups 22-10
Adding and Editing Security Groups 22-11
Configuring Security Group Access Control Lists 22-12
Adding and Editing Security Group Access Control Lists 22-13
Mapping Security Groups to Devices 22-14
Adding and Editing Security Group Mappings 22-14
Configuring SGA Policy by Assigning SGTs to Devices 22-16
Assigning Security Groups to Users and End Points 22-17
Egress Policy 22-18
Viewing the Egress Policy 22-19
Source Tree 22-20
Destination Tree 22-20
Matrix View 22-20
Sorting and Filtering Egress Policy Table 22-22
Quick Filter 22-22
Advanced Filter 22-23
Presetting Filters 22-25
Configuring Egress Policy Table Cells 22-25
Adding and Editing the Mapping of Egress Policy Cells 22-25
Editing the Default Policy 22-26
Deleting a Mapping of a Cell 22-27
Configuring SGT and SGACL from Egress Policy 22-27
Push Button 22-28

Monitor Mode 22-28
Monitoring the Monitor Mode 22-28
The Unknown Security Group 22-30
Default Policy 22-30
OOB SGA PAC 22-31
SGA PAC Provisioning 22-31
Generating an SGA PAC from the Settings Screen 22-31
Generating an SGA PAC from the Network Devices Screen 22-32
Generating an SGA PAC from the Network Devices List Screen 22-33
Monitoring SGA PAC 22-33
PAC Provisioning Report 22-33
SGA CoA 22-34
CoA Supported Network Devices 22-34
Environment CoA 22-35
Initiating Environment CoA 22-36
Per Policy CoA 22-37
Update RBACL Named List CoA 22-37
Update SGT Matrix CoA 22-38
Policies Update CoA 22-39
SGA CoA Summary 22-40
Monitoring SGA CoA 22-40
SGA CoA Alarms 22-41
SGA CoA Report 22-41

PART 4 **Monitoring and Troubleshooting Cisco ISE**

CHAPTER 23 **Monitoring and Troubleshooting** 23-1
Understanding Monitoring and Troubleshooting 23-1
User Roles and Permissions 23-2
Monitoring and Troubleshooting Database 23-3
Configuring Devices for Monitoring 23-3
Cisco ISE Dashboard Monitoring 23-3
Dashlets 23-4
Metric Meters 23-9
Monitoring the Network 23-10
Monitoring Network Process Status 23-10
Managing Alarms 23-11
Understanding Alarms 23-11
Viewing, Editing, and Resolving Alarms 23-13

Viewing and Filtering Alarm Schedules 23-14
Creating, Editing, and Deleting Alarm Schedules 23-15
Creating, Assigning, Disabling, and Deleting Alarm Rules 23-16
Available Alarm Rules 23-18
Passed Authentication 23-19
Failed Authentication 23-19
Authentication Inactivity 23-20
ISE Configuration Changes 23-20
ISE System Diagnostics 23-21
ISE Process Status 23-21
ISE Health System 23-21
ISE AAA Health 23-22
Authenticated But No Accounting Start 23-22
Unknown NAD 23-22
External DB Unavailable 23-23
RBACL Drops 23-24
NAD-Reported AA Down 23-24
Monitoring Live Authentications 23-25
Monitoring Guest Activity 23-27
Monitoring Data Collections 23-28
Troubleshooting the Network 23-29
Viewing and Editing Failure Reasons 23-29
Troubleshooting Network Access 23-29
Performing Connectivity Tests 23-30
Using Diagnostic Troubleshooting Tools 23-31
Troubleshooting RADIUS Authentications 23-31
Executing a Network Device Command 23-33
Evaluating a Network Device Configuration 23-33
Troubleshooting Posture Data 23-34
Troubleshooting with TCP Dump 23-35
Comparing SGACL Policies 23-37
Comparing SXP-IP Mappings 23-38
Comparing IP-SGT Pairs 23-38
Comparing SGT Devices 23-39
Obtaining Additional Troubleshooting Information 23-40
Downloading Support Bundles 23-40
Downloading Debug Logs 23-43
Monitoring Administration 23-45
Backing Up and Restoring the Monitoring Database 23-45

Configuring Data Purging 23-46
Scheduling Full and Incremental Backups 23-48
Performing On-Demand Backups 23-50
Restoring the Monitoring Database 23-51
Viewing Log Collections 23-53
Specifying Email Settings 23-53
Configuring System Alarm Settings 23-54
Configuring Alarm Syslog Targets 23-54

CHAPTER 24 **Reporting** 24-1

Report Basics 24-1
Understanding Reports View and Interactive Viewer 24-2
Running, Viewing, and Navigating Reports 24-3
Exporting and Printing Reports 24-4
Deleting Reports 24-5
Catalog Reports 24-6
Accessing Catalog Reports 24-6
Customizing Catalog Reports 24-7
Restoring Default Report Settings 24-7
Favorite Reports 24-8
Adding Favorite Reports 24-8
Viewing Report Parameters 24-9
Editing or Deleting Favorite Reports 24-10
Shared Reports 24-10
System Reports 24-11
Organizing and Formatting Report Data 24-12
Working with the Interactive Viewer Toolbar 24-12
Grouping, Sorting, and Hiding Data 24-13
Grouping Data 24-13
Sorting Data 24-14
Hiding and Displaying Report Items 24-16
Hiding and Displaying Column Data 24-16
Changing Column Layouts 24-17
Creating Report Calculations 24-21
Filtering Report Data 24-24
Working with Aggregate Data 24-28
Working with Charts 24-29
Formatting Reports 24-32
Editing and Formatting Labels 24-32

Formatting Data Types 24-33
Applying Conditional Formats 24-36
Setting and Removing Page Breaks 24-37
Saving Customized Reports 24-39
Working with Active RADIUS Sessions 24-39
Available Reports 24-42

PART 5 Reference

APPENDIX A User Interface Reference A-1
Operations A-1
Authentications A-1
Alarms A-3
Alarms Inbox A-3
Rules A-5
Schedules A-14
Reports A-15
Catalog A-15
Favorites A-23
Report Context Menus A-23
Data Formatting A-26
Filters A-38
Troubleshoot A-40
General Tools A-40
Security Group Access Tools A-47
Policy A-54
Authentication A-54
Administration A-58
System > Settings > Monitoring A-58
Alarm Syslog Targets A-59
Email Settings A-59
Failure Reasons Editor A-59
System Alarm Settings A-60
System > Maintenance > Data Management > Monitoring Node A-61
Full Backup On Demand A-61
Scheduled Backup A-62
Data Purging A-62
Data Restore A-63

APPENDIX B **Network Access Flows** B-1

Network Access Use Cases B-2

RADIUS-Based Protocols Without EAP B-2

Password Authentication Protocol B-3

Challenge Handshake Authentication Protocol B-4

Microsoft Challenge Handshake Authentication Protocol version 1 B-4

Microsoft Challenge Handshake Authentication Protocol version 2 B-4

RADIUS-Based EAP Protocols B-4

Extensible Authentication Protocol-Message Digest 5 B-6

Lightweight Extensible Authentication Protocol B-6

Protected Extensible Authentication Protocol B-6

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling B-7

APPENDIX C **Switch Configuration Required to Support Cisco ISE Functions** C-1

Enable Your Switch to Support Standard Web Authentication C-2

Define a Local User Name and Password for Synthetic RADIUS Transactions C-2

Set the NTP Server to Ensure Accurate Log and Accounting Timestamps C-2

Enable AAA Functions C-3

RADIUS Servers Configuration C-3

Enable RADIUS Change of Authorization (CoA) C-4

Enable Device Tracking and DHCP Snooping C-4

Enable 802.1X Port-Based Authentication C-4

Use EAP for Critical Authentications C-4

Throttle AAA Requests Using Recovery Delay C-4

Define VLANs Based on Enforcement States C-5

Define Local (Default) ACLs on the Switch C-5

Enable Cisco Security Group Access Switch Ports C-6

Enable EPM Logging C-8

Enable SNMP Traps C-8

Enable SNMP v3 Query for Profiling C-8

Enable MAC Notification Traps for Profiler to Collect C-8

Configure the RADIUS Idle-Timeout C-8

APPENDIX D **Troubleshooting Cisco ISE** D-1

Installation and Network Connection Issues D-2

Unknown Network Device D-3

CoA Not Initiating on Client Machine D-3

Users Are Assigned to Incorrect VLAN During Network Access Sessions D-3
Client Machine URL Redirection Function Not Working D-4
Cisco ISE Profiler is Not Able to Collect Data for Endpoints D-5
RADIUS Accounting Packets (Attributes) Not Coming from Switch D-5
Policy Service ISE Node Not Passing Traffic D-6
Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation D-7
Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working D-7
Licensing and Administrator Access D-8
Certificate Expired D-8
Configuration and Operation (Including High Availability) D-9
Client Machines Are Not Able to Authenticate D-9
Users Are Not Appropriately Redirected to URL D-9
Cannot Download Remote Client Provisioning Resources D-10
Lost Monitoring and Troubleshooting Data After Registering Policy Service ISE Node to Administration ISE Node D-10
Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8 D-11
Data Out of Sync Between Primary And Secondary ISE Nodes D-11
External Authentication Sources D-12
User Authentication Failed D-12
Missing User for RADIUS-Server Test Username in Cisco ISE Identities D-12
Connectivity Issues Between the Network Access Device (Switch) and Cisco ISE D-13
Active Directory Disconnected D-13
Cisco ISE Node Not Authenticating with Active Directory D-14
RADIUS Server Error Message Entries Appearing in Cisco ISE D-14
RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE) D-15
Client Access, Authentication, and Authorization D-17
Cannot Authenticate on Profiled Endpoint D-17
Quarantined Endpoints Do Not Renew Authentication Following Policy Change D-18
Endpoint Does Not Align to the Expected Profile D-19
User is Unable to Authenticate Against the Local Cisco ISE Identity Store D-19
Certificate-Based User Authentication via Supplicant Failing D-20
802.1X Authentication Fails D-21
Users Are Reporting Unexpected Network Access Issues D-22
Authorization Policy Not Working D-23
Switch is Dropping Active AAA Sessions D-24
URL Redirection on Client Machine Fails D-24
Agent Download Issues on Client Machine D-26
Agent Login Dialog Not Appearing D-27
Agent Fails to Initiate Posture Assessment D-27

Agent Displays “Temporary Access” **D-28**
Cisco ISE Does Not Issue CoA Following Authentication **D-28**
Error Messages **D-29**
ACTIVE_DIRECTORY_USER_INVALID_CREDENTIALS **D-29**
ACTIVE_DIRECTORY_USER_AUTH_FAILED **D-29**
ACTIVE_DIRECTORY_USER_PASSWORD_EXPIRED **D-30**
ACTIVE_DIRECTORY_USER_WRONG_PASSWORD **D-30**
ACTIVE_DIRECTORY_USER_ACCOUNT_DISABLED **D-30**
ACTIVE_DIRECTORY_USER_RESTRICTED_LOGON_HOURS **D-30**
ACTIVE_DIRECTORY_USER_NON_COMPLIANT_PASSWORD **D-30**
ACTIVE_DIRECTORY_USER_UNKNOWN_DOMAIN **D-31**
ACTIVE_DIRECTORY_USER_ACCOUNT_EXPIRED **D-31**
ACTIVE_DIRECTORY_USER_ACCOUNT_LOCKED_OUT **D-31**
ACTIVE_DIRECTORY_GROUP_RETRIEVAL_FAILED **D-31**
ACTIVE_DIRECTORY_MACHINE_AUTHENTICATION_DISABLED **D-31**
ACTIVE_DIRECTORY_ATTRIBUTE_RETRIEVAL_FAILED **D-32**
ACTIVE_DIRECTORY_PASSWORD_CHANGE_DISABLED **D-32**
ACTIVE_DIRECTORY_USER_UNKNOWN **D-32**
ACTIVE_DIRECTORY_CONNECTION_FAILED **D-32**
ACTIVE_DIRECTORY_BAD_PARAMETER **D-32**
ACTIVE_DIRECTORY_TIMEOUT **D-33**
Configure NADs for ISE Monitoring **D-33**
Troubleshooting APIs **D-34**
Contacting the Cisco Technical Assistance Center **D-35**

GLOSSARY

INDEX



Preface

Revised: June 20, 2013, OL-25537-01

This guide describes how to use Cisco Identity Services Engine (Cisco ISE).

This chapter introduces the purpose, scope, and organization of this guide and covers the following topics:

- Audience
- Document Organization
- Document Conventions
- Documentation Updates
- Related Documentation
- Notices
- Obtaining Documentation and Submitting a Service Request

Audience

This guide is written for network security administrators who are responsible for setting up and maintaining network and application security. This guide assumes that you have a working knowledge of networking principles and applications, and have experience as a network system administrator.

Document Organization

The topics in this guide are grouped into introduction, functional tasks, and reference categories, and are organized in the following way:

Part	Chapter
Part 1: Introducing Cisco ISE	
	Overview of Cisco ISE
	Understanding the User Interface
Part 2: Administering Cisco ISE	
	Cisco ISE Task Navigator
	Managing Identities and Admin Access
	Managing External Identity Sources
	Managing Network Devices
	Managing Resources
	Administering Cisco ISE
	Setting Up Cisco ISE in a Distributed Environment
	Setting Up Inline Posture
	Setting Up Endpoint Protection Services
	Managing Licenses
	Managing Certificates
	Logging
	Managing Cisco ISE Backup and Restore Operations
Part 3: Managing Cisco ISE Policy Models	
	Managing Authentication Policies
	Managing Authorization Policies and Profiles
	Configuring Endpoint Profiling Policies
	Configuring Client Provisioning Policies
	Configuring Client Posture Policies
	User Access Management
	Configuring Cisco Security Group Access Policies
Part 4: Monitoring and Troubleshooting Cisco ISE	
	Monitoring and Troubleshooting
	Reporting

Part	Chapter
Part 5: Reference	
	Appendix A, User Interface Reference
	Appendix B, Network Access Flows
	Appendix C, Switch Configuration Required to Support Cisco ISE Functions
	Appendix D, Troubleshooting Cisco ISE
	Glossary

Note Cisco sometimes updates the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Document Conventions

This guide uses the convention whereby the symbol ^ represents the key labeled *Control*. For example, the key combination **^z** means "Hold down the **Control** key while you press the **z** key."

Command descriptions use these conventions:

- Examples that contain system prompts denote interactive sessions and indicate the commands that you should enter at the prompt. The system prompt indicates the current level of the EXEC command interpreter. For example, the prompt `Router>` indicates that you should be at the *user* level, and the prompt `Router#` indicates that you should be at the *privileged* level. Access to the privileged level usually requires a password.
- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([ ]) are optional.
- Alternative keywords from which you must choose one are grouped in braces ({ }) and separated by vertical bars (|).

Examples use these conventions:

- Terminal sessions and sample console screen displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).
- Default responses to system prompts are in square brackets ([]).
- An exclamation point (!) at the beginning of a line indicates a comment line.

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Note Means *reader take note*. Notes identify important information that you should think about before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

Documentation Updates

The following table lists the creation and update history of this document.

Table 1 Updates to Cisco Identity Services Engine User Guide, Release 1.1

Date	Description
8/16/12	Resolved defects CSCtz86916, CSCub05495, and CSCub53923
5/28/12	Added information on Remote Access VPN. See Remote Access VPN Use Case, page 31 for information on remote VPN Access.
4/18/12	Resolved CSCtz12146
4/3/12	Resolved CSCty98730
4/2/12	Resolved CSCtz00715, CSCty85856
3/30/12	Resolved CSCty75746
3/28/12	Resolved CSCty89763, CSCty67468, and CSCts84532
3/19/12	Cisco Identity Services Engine, Release 1.1

Related Documentation

This section provides lists of the following types of documents that are relevant to this release of Cisco ISE:

- Release-Specific Documents, page xxxiii
- Platform-Specific Documents, page xxxiii

Release-Specific Documents

Table 2 lists the product documentation available for the Cisco ISE Release. General product information for Cisco ISE is available at http://www.cisco.com/go/ise. End-user documentation is available on Cisco.com at http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.

Table 2 Product Documentation for Cisco Identity Services Engine

Document Title	Location
Release Notes for the Cisco Identity Services Engine, Release 1.1	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
Cisco Identity Services Engine Network Component Compatibility, Release 1.1	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
Cisco Identity Services Engine User Guide, Release 1.1	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine Hardware Installation Guide, Release 1.1	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
Cisco Identity Services Engine CLI Reference Guide, Release 1.1	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine API Reference Guide, Release 1.1	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
Cisco Identity Services Engine Troubleshooting Guide, Release 1.1	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
Regulatory Compliance and Safety Information for Cisco Identity Services Engine, Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html

Platform-Specific Documents

Links to other platform-specific documentation are available at the following locations:

- Cisco ISE
  http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
- Cisco Secure ACS
  http://www.cisco.com/en/US/products/ps9911/tsd_products_support_series_home.html
- Cisco NAC Appliance
  http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html

- Cisco NAC Profiler
  http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html
- Cisco NAC Guest Server
  http://www.cisco.com/en/US/products/ps10160/tsd_products_support_series_home.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See the following information for the actual license texts. Both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL, please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY

THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.



What's New in This Release

This section describes new features, updates, and changes that have been added to the Cisco Identity Services Engine (ISE) documentation for this release.

New in Cisco Identity Services Engine, Release 1.1

Table 1 Updates for the Cisco Identity Services Engine User Guide, Release 1.1

Feature	Location
Active Directory	• Microsoft Active Directory, page 5-4
Administration	• Changing Administrator Name, page 4-65 • Support for Microsoft Internet Explorer version 9 and FireFox 9 on the Cisco ISE administrative GUI, see Logging In, page 8-1 • New look-and-feel for the Cisco ISE Admin user interface, see Understanding the User Interface, page 2-1 for an overview • Configuring Cisco ISE for Administrator Access Using an External Identity Store, page 4-44
Common Access Card	• Configuring Cisco ISE for Administrator CAC Authentication, page 8-4
Egress Policy	• Egress Policy, page 22-18
Endpoint Protection Services	• Chapter 11, "Setting Up Endpoint Protection Services"
Federal Information Processing Standards (FIPS) 140-2 support	• Enabling FIPS Mode in Cisco ISE, page 8-2 • Adding and Editing Devices, page 6-3 • Configuring a Default Device, page 6-9 • Generating a Self-Signed Certificate, page 13-7 • Generating a Certificate Signing Request, page 13-8 • Creating RADIUS Servers, page 16-23

Table 1 Updates for the Cisco Identity Services Engine User Guide, Release 1.1 (continued)

Feature	Location
Guest	• Wireless LAN Controller with Local WebAuth, page 21-4 • Device Registration WebAuth, page 21-8 • Specifying a Simple URL for Sponsor Portal Access, page 21-30 • Creating a Custom Portal Theme, page 21-31
Internationalization and Localization	• Cisco ISE Internationalization and Localization, page 2-1
Migration and Upgrade	• ISE 1.1 Migration Tool changes • Upgrading the Cisco ISE chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*
Network Time Protocol (NTP)	• System Time and NTP Server Settings, page 8-18
Online Certificate Status Protocol (OCSP)	• OCSP Services, page 13-25
Posture	• Simplified Posture Policy configuration – Chapter 20, "Simplified Posture Policy Configuration" – Chapter 20, "Creating a New Posture Policy" – Chapter 20, "Creating a New Posture Requirement"
Profiler	• IOS Sensor for Profiling – Chapter 18, "Endpoint Profiling by Using an IOS Sensor on a Network Access Device." • NMAP Profiler – Chapter 18, "Configuring the Network Scan (NMAP) Probe." – Chapter 18, "Endpoint Scan." – Chapter 18, "Profiling Network Scan Actions." • Profile LLDP information via an SNMP Probe – Chapter 18, "Configuring the SNMP Query Probe."
Security Group Access (SGA)	• SGA CoA, page 22-34 • Egress Policy, page 22-18 • Generating the PAC for EAP-FAST, page 16-11
Security Group Access Control List (SGACL)	• SGA CoA, page 22-34 • Monitor Mode, page 22-28

Table 1 Updates for the Cisco Identity Services Engine User Guide, Release 1.1 (continued)

Feature	Location
Security Group Tag (SGT) name download	• Adding and Editing Security Groups, page 22-11
Virtual Machine (VM)	• Configuring the Cisco ISE 3300 Series Appliance chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1* • Performing Post Installation Tasks chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1* • Installing the Cisco ISE System Software on a VMware Virtual Machine chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*

Related Documentation

- General product information for Cisco ISE is available at http://www.cisco.com/go/ise.
- End-user documentation is available on Cisco.com at http://www.cisco.com/en/US/products/ps11640/tsd_products_support_series_home.html.



PART 1

Introducing Cisco ISE



CHAPTER 1

Overview of Cisco ISE

Cisco Identity Services Engine (ISE) is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. The unique architecture of Cisco ISE allows enterprises to gather real-time contextual information from networks, users, and devices. The administrator can then use that information to make proactive governance decisions by tying identity to various network elements including access switches, wireless LAN controllers (WLCs), virtual private network (VPN) gateways, and data center switches. Cisco ISE is a key component of the Cisco Security Group Access Solution.

Cisco ISE is a consolidated policy-based access control system that incorporates a superset of features available in existing Cisco policy platforms. Cisco ISE performs the following functions:

- Combines authentication, authorization, accounting (AAA), posture, and profiler into one appliance
- Provides for comprehensive guest access management for the Cisco ISE administrator, sanctioned sponsor administrators, or both
- Enforces endpoint compliance by providing comprehensive client provisioning measures and assessing device posture for all endpoints that access the network, including 802.1X environments
- Provides support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network
- Enables consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed
- Employs advanced enforcement capabilities including security group access (SGA) through the use of security group tags (SGTs) and security group access control lists (SGACLs)
- Supports scalability to support a number of deployment scenarios from small office to large enterprise environments

The following key functions of Cisco ISE enable you to manage your entire access network.

Provide Identity-Based Network Access

The Cisco ISE solution provides context-aware identity management in the following areas:

- Cisco ISE determines whether users are accessing the network on an authorized, policy-compliant device.
- Cisco ISE establishes user identity, location, and access history, which can be used for compliance and reporting.
- Cisco ISE assigns services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).
- Cisco ISE grants authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.

For more information, see Chapter 4, "Managing Identities and Admin Access."

Manage Various Deployment Scenarios

You can deploy Cisco ISE across an enterprise infrastructure, supporting 802.1X wired, wireless, and virtual private networks (VPNs).

The Cisco ISE architecture supports both stand-alone and distributed (also known as "high-availability" or "redundant") deployments where one machine assumes the primary role and another "backup" machine assumes the secondary role. Cisco ISE features distinct configurable personas, services, and roles, which allow you to create and apply Cisco ISE services where they are needed in the network. The result is a comprehensive Cisco ISE deployment that operates as a fully functional and integrated system.

You can deploy Cisco ISE nodes with one or more of the Administration, Monitoring, and Policy Service personas—each one performing a different vital part in your overall network policy management topology. Installing Cisco ISE with an Administration persona allows you to configure and manage your network from a centralized portal to promote efficiency and ease of use.

You can also choose to deploy the Cisco ISE platform as an Inline Posture node to perform policy enforcement and execute Change of Authorization (CoA) requests where users are accessing the network via WLCs and/or VPN concentrators that do not support the necessary functionality to facilitate Cisco ISE policy management.

For more information, see:

- Chapter 9, "Setting Up Cisco ISE in a Distributed Environment"
- Chapter 10, "Setting Up Inline Posture"

Provide Basic User Authentication and Authorization

User authentication policies in Cisco ISE enable you to provide authentication for a number of user login session types using a variety of standard authentication protocols including, but not limited to, Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Protected Extensible Authentication Protocol (PEAP), and Extensible Authentication Protocol (EAP). Cisco ISE specifies the allowable protocol(s) that are available to the network devices on which the user tries to authenticate and specifies the identity sources from which user authentication is validated.

Cisco ISE allows for a wide range of variables within authorization policies to ensure that only authorized users can access the appropriate resources when they access the network. The initial release of Cisco ISE supports only RADIUS-governed access to the internal network and its resources.

At the most fundamental level, Cisco ISE supports 802.1X, MAC authentication bypass (MAB), and browser-based Web authentication login for basic user authentication and access via both wired and wireless networks. Upon receiving an authentication request, the "outer part" of the authentication policy is used to select the set of protocols that are allowed to be used when processing the request. Then, the "inner part" of the authentication policy is used to select the identity source that is used to authenticate the request. The identity source may consist of a specific identity store or an identity store sequence that lists a set of accessible identities until the user received a definitive authorization response.

Once authentication succeeds, the session flow proceeds to the authorization policy. (There are also options available that allow Cisco ISE to process the authorization policy even when the authentication did not succeed.) Cisco ISE enables you to configure behavior for "authentication failed," "user not found," and "process failed" cases, and also to decide whether to reject the request, drop the request (no response is issued), or continue to the authorization policy. In cases where Cisco ISE continues to perform authorization, you can use the "AuthenicationStaus" attribute in the "NetworkAccess" dictionary to incorporate the authentication result as part of the authorization policy.

The authorization policy result is Cisco ISE assigning an authorization profile that might also involve a downloadable ACL specifying traffic management on the network policy enforcement device. The downloadable ACL specifies the RADIUS attributes that are returned during authentication and that define the user access privileges granted once authenticated by Cisco ISE.

For more information, see:

- Chapter 16, "Managing Authentication Policies"
- Chapter 17, "Managing Authorization Policies and Profiles"

Support for FIPS 140-2 Implementation

Cisco ISE, Release 1.1 introduces Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance. FIPS 140-2 is a United States government computer security standard that is used to accredit cryptographic modules. Cisco ISE uses an embedded FIPS 140-2 implementation using validated C3M and Cisco ACS NSS modules, per FIPS 140-2 Implementation Guidance section G.5 guidelines.

In addition, the FIPS standard places limitations on the use of certain algorithms, and in order to enforce this standard, you must enable FIPS operation in Cisco ISE. Cisco ISE enables FIPS 140-2 compliance via RADIUS Shared Secret and Key Management measures and provides SHA-256 encryption and decryption capabilities for certificates. While in FIPS mode, any attempt to perform functions using a non-FIPS compliant algorithm fails, and, as such, certain authentication functionality is disabled.

When you turn on FIPS mode in Cisco ISE, the following functions are affected:

- IEEE 802.1X environment
  - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-Transport Layer Security (EAP-TLS)
  - PEAP
  - RADIUS

Note Other protocols like EAP-Message Digest 5 (EAP-MD5), Lightweight Extensible Authentication Protocol (LEAP), and PAP are not compatible with a FIPS 140-2 compliant system and are disabled while Cisco ISE is in FIPS mode.

- Secure Shell (SSH) clients can only use SSHv2
- Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL)
- Inline Posture node RADIUS Key Wrap
- HTTPS protocol communication for both Administrator ISE nodes and Inline Posture nodes

For more information, see the specific FIPS 140-2 configuration options:

- Chapter 6, "Managing Network Devices"
- Chapter 8, "Administering Cisco ISE" (Enabling FIPS Mode in Cisco ISE, page 8-2)
- Chapter 13, "Managing Certificates"
- Chapter 16, "Managing Authentication Policies"

Support Common Access Card Functions

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee of, for example, the U.S. Department of

Defense (DoD). Access via the CAC requires a card reader into which the user inserts the card and enters a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

Benefits of using a CAC card to authenticate include these:

- Common Access Card X.509 certificates are the identity source for 802.1X EAP-TLS authentication.
- Common Access Card X.509 certificates are also the identity source for authentication and authorization to Cisco ISE administration.

Cisco ISE only supports login to the administrator user interface. It does not support CAC authentication for the following access methods:

- You cannot use CAC authentication login to manage the Cisco ISE Command Line Interface.
- External REST API (Monitoring and Troubleshooting) and Endpoint Protection Services APIs are outside the scope of the CAC authentication.
- Guest Services and Guest Sponsor Administration access does not support the CAC authentication method in Cisco ISE.

For more information on setting up Cisco ISE up for CAC authentication, see Chapter 8, “Administering Cisco ISE.”

Incorporate Client Posture Assessment

To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you to validate and maintain security capabilities on any client machine that accesses the protected network. By employing posture policies that are designed to ensure that the most up-to-date security settings or applications are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses the network meets, and continues to meet, the defined security standards for enterprise network access. Posture compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the time of user login, as well as any time a periodic reassessment takes place.

Posture assessment and compliance takes place using one of the following agent types available in Cisco ISE:

- Cisco NAC Web Agent—A temporal agent the user installs on his/her system at the time of login that is no longer visible on the client machine once the login session terminates.
- Cisco NAC Agent—A persistent agent that, once installed, remains on a Windows or Mac OS X client machine to perform all user login and security compliance functions for Windows XP, Windows Vista, Windows 7, or Mac OS 10.5 and 10.6 clients, respectively.

For more information, see:

- Chapter 19, “Configuring Client Provisioning Policies”
- Chapter 20, “Configuring Client Posture Policies”

Define Sponsors and Manage Guest Sessions

Cisco ISE administrators and employees that are granted appropriate access to the Cisco ISE guest registration portal as guest sponsors can create temporary guest login accounts and specify available network resources to allow guests, visitors, contractors, consultants, and customers to access the network. Guest access sessions have expiration timers associated with them, so they are effective in controlling guest access to a specific day, time period, and so forth.

All aspects of a guest user session (including account creation and termination) are tracked and recorded in Cisco ISE so that you can provide audit information and troubleshoot session access, as necessary.

For more information, see:

- Chapter 21, "User Access Management"
- *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1*

Manage Wireless and VPN Traffic with Inline Posture Nodes

Inline Posture nodes are gatekeeping nodes that enforce Cisco ISE access policies and handle CoA requests. After initial authentication (using EAP/802.1X and RADIUS), client machines must still go through posture assessment. The posture assessment process determines whether the client should be restricted, denied, or allowed full access to the network. When a client accesses the network through a WLC or VPN device, the Inline Posture node has the responsibility for the policy enforcement and CoA that the other network devices are unable to accommodate. It is for this reason that a Cisco ISE can be deployed as an Inline Posture node behind other network access devices on your network, such as WLCs and VPN concentrators.

For more information, see Chapter 10, "Setting Up Inline Posture."

Profile Endpoints on the Network

The Profiler service assists in identifying, locating, and determining the capabilities of all endpoints on your network (known as identities in Cisco ISE), regardless of their respective device types, in order to ensure and maintain appropriate access to your enterprise network. The Cisco ISE Profiler function uses a number of probes to collect attributes for all endpoints on your network, and pass them to the Profiler analyzer where the known endpoints are classified according to their associated policies and the identity groups.

For more information, see Chapter 18, "Configuring Endpoint Profiling Policies."

Install on a Variety of Hardware and VMware Platforms

Cisco ISE comes preinstalled on a range of physical appliances with various performance characteristics. The Cisco Application Deployment Engine (ADE) and Cisco ISE software run on either a dedicated Cisco ISE 3300 Series appliance or on a VMware server (Cisco ISE VM). The Cisco ISE software image does not support the installation of any other packages or applications on this dedicated platform. The inherent scalability of Cisco ISE allows you to add appliances to a deployment and increase performance and resiliency, as needed.

For more detailed information on hardware platforms and installing Cisco ISE, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*



CHAPTER 2

Understanding the User Interface

This chapter introduces the Cisco Identity Service Engine (ISE) user interface in the following topics:

- Cisco ISE Internationalization and Localization, page 2-1
- Inherent Usability, page 2-6
- Elements of the User Interface, page 2-7
- Introducing the Dashboard, page 2-12
- Common User Interface Patterns, page 2-16
- Understanding the Impact of Roles and Admin Groups, page 2-19

Cisco ISE Internationalization and Localization

Cisco ISE internationalization adapts the user interface for supported languages. Localization of the user interface incorporates locale-specific components and translated text.

In Cisco ISE, Release 1.1 internalization and localization support is focused on the text and information that is presented to the end user (connecting to Cisco ISE). This includes support for non-English text in UTF-8 encoding to the end-user facing portals and on selective fields on the Cisco ISE Admin user interface.

This section covers the following topics:

- Supported Languages, page 2-2
- UTF-8 Character Data Entry, page 2-2
- Portal Localization, page 2-3
- UTF-8 Credential Authentication, page 2-4
- UTF-8 Policies and Posture Assessment, page 2-4
- Cisco NAC and MAC Agent UTF-8 Support, page 2-5
- UTF-8 Support for Messages Sent to Supplicant, page 2-5
- Reports and Alerts UTF-8 Support, page 2-5
- UTF-8 Support Outside the User Interface, page 2-6
- Support for Importing and Exporting UTF-8 Values, page 2-6

Supported Languages

Cisco ISE, Release 1.1 provides localization and internalization support for the following languages and browser locales:

Table 2-1 Supported Languages and Browser Locales

Language	Browser Locale
Chinese traditional	zh-tw
Chinese simplified	zh-cn
English	en
French	fr-fr
German	de-de
Italian	it-it
Japanese	ja-jp
Korean	ko-kr
Portuguese	pt-br (Brazilian)
Russian	ru-ru
Spanish	es-es

Internationalization and localization applies to all supported internet browsers. For more information, see the *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

UTF-8 Character Data Entry

Cisco ISE administrative user interface fields that are exposed to the end user through the Cisco NAC agent, supplicants, or the sponsor portal, guest portal, and client provisioning portals, support UTF-8 character sets for all languages. Character values are stored in UTF-8 in the administration configuration database, and are then viewed in UTF-8 as entered.

UTF-8 is a multibyte character encoding for the unicode character set, which includes many different language character sets, including Hebrew, Sanskrit, Arabic, and many more. The ISE user interface supports UTF-8 characters in a number of input fields. When the user-entered UTF-8 characters appear in reports and user interface components, they are displayed correctly.

Note Many more character sets are supported in ISE user interface input fields (UTF-8) than are currently supported for localizations (for translated text) in portals and end-user messages.

For a complete list of UTF-8 character data entry fields, see UTF-8 Character Support in the User Interface, page 21-36.

Portal Localization

Internationalizing includes input that is configured by the end user, or Cisco ISE administrator configurations that are displayed in any of the following user portals:

- Sponsor Portal, page 2-3
- Guest Portal, page 2-3
- Client Provisioning Portal, page 2-4

Sponsor Portal

The Sponsor portal user interface is localized into all supported languages and locales. This includes text, labels, messages, field names, and button labels. The predefined text per language is configurable on the Cisco ISE Admin user interface, and you can add additional languages. For more information, see Configuring Sponsor Language Templates, page 21-37.

Note If an undefined locale is requested by a client browser, the English locale default portal is displayed. This means that if the browser requests a locale that is not mapped to a template in ISE, the English template is presented. See Table 2-1 for a list of supported Languages and Browser Locales

Sponsor portal fields support UTF-8 char sets. UTF-8 values are stored in the administrative configuration database and viewed in UTF-8 in the Sponsor portal as entered. Guest accounts accept plain text and .csv files with UTF-8 values. The following table lists the UTF-8 Sponsor portal fields.

Guest account list	• Filter value edit box
Create guest account	• First name • Last name • Email address • Company • Optional data
Create random guest accounts	• User name prefix
Settings customizations	• Email

Guest Portal

The Guest portal can be localized to present user interface elements in all left-to right language locales. This includes text, field names, button labels, and messages. You can configure supported language templates on the administrative portal. For more information, see Configuring Sponsor Language Templates, page 21-37.

Note Currently, ISE does not support right-to-left languages, such as Hebrew or Arabic, even though the character sets themselves are supported.

You can customize the Guest portal by uploading HTML pages to Cisco ISE. When you upload customized pages, you are responsible for the appropriate localization support for your deployment. Cisco ISE provides a localization support example with sample HTML pages, which you can use as a guide. ISE provides the ability to upload, store, and render custom internationalized HTML pages.

Default templates for supported languages are included in a standard Cisco ISE installation. If an undefined locale is requested by the client browser, the English locale default portal is displayed.

The following are the Guest portal input fields to support UTF-8:

- Login user name
- All fields on the self-registration page

Client Provisioning Portal

The Client Provisioning portal interface has been localized for all supported language locales. This includes text, labels, messages, field names, and button labels. If an undefined locale is requested by a client browser, the English locale default portal is displayed.

Currently, language templates are not supported for the Client Provisioning portal, as they are for the Admin, Guest, and Sponsor portals.

Note NAC and MAC agent installers are not localized, nor are WebAgent pages.

For more information on client provisioning, see Chapter 19, "Configuring Client Provisioning Policies."

UTF-8 Credential Authentication

Network access authentication supports UTF-8 username and password credentials. This includes RADIUS, EAP, RADIUS proxy, RADIUS token, web authentication from the Guest and Administrative portal login authentications. This provides end users network access with a UTF-8 user name and password, as well as administrators with UTF-8 credentials. UTF-8 support for user name and password applies to authentication against the local identity store as well as external identity stores.

UTF-8 authentication depends on the client supplicant that is used for network login. Some Windows native supplicants do not support UTF-8 credentials. If you are experiencing difficulties with a Windows native supplicant, the following Windows hotfixes may be helpful:

- http://support.microsoft.com/default.aspx?scid=kb;EN-US;957218
- http://support.microsoft.com/default.aspx?scid=kb;EN-US;957424

Note RSA (Rivest, Shamir, and Adleman) does not support UTF-8 users, hence UTF-8 authentication with RSA is not supported. Likewise, RSA servers, which are compatible with ISE 1.1, do not support UTF-8.

UTF-8 Policies and Posture Assessment

Policy rules in Cisco ISE that are conditioned on attribute values may include UTF-8 text. Rule evaluation supports UTF-8 attribute values. In addition, you can configure conditions with UTF-8 values through the Administrative portal.

Posture requirements can be modified as File, Application, and Service conditions based on a UTF-8 character set. This includes sending UTF-8 requirement values to the NAC agent. The NAC agent then assesses the endpoint accordingly, and reports UTF-8 values, when applicable.

Cisco NAC and MAC Agent UTF-8 Support

The Cisco NAC agent supports internationalization of text, messages, and any UTF-8 data that is exchanged with ISE. This includes requirement messages, requirement names, and file and process names that are used in conditions.

The following limitations apply:

- UTF-8 support applies to Windows-based NAC agents only.
- Cisco NAC and MAC agent interfaces currently do not support localization.

Note WebAgent does not support UTF-8 based rules and requirements. For Cisco NAC agent versions supported by Cisco ISE, Release 1.1, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

If an acceptable use policy (AUP) is configured, the policy pages are provided on the client side, based on the browser locale and the set of languages that are specified in the configuration. The administrator is responsible for providing a localized AUP bundle or site URL.

UTF-8 Support for Messages Sent to Supplicant

RSA prompts and messages are forwarded to the supplicant using a RADIUS attribute REPLY-MESSAGE, or within EAP data. If the text contains UTF-8 data, it is displayed by the supplicant, based on the client's local operating system language support. Some Windows-native supplicants do not support UTF-8 credentials.

Note Cisco ISE prompts and messages may not be in sync with the locale of the client operating system on which the supplicant is running. It is the responsibility of the administrator to align the end user supplicant locale with the languages that are supported by Cisco ISE.

Reports and Alerts UTF-8 Support

Monitoring and troubleshooting reports and alerts support UTF-8 values for relevant attributes, for Cisco ISE supported languages, in the following ways:

- Viewing live authentications
- Viewing catalog reports
- Viewing detailed pages of report records
- Exporting and saving reports
- Viewing the Cisco ISE dashboard
- Viewing alert information
- Viewing tcpdump data

UTF-8 Support Outside the User Interface

This section covers the areas outside the ISE user interface that provide UTF-8 support.

Debug Log and CLI-Related UTF-8 Support

Attribute values and posture condition details appear in some debug logs; therefore, all debug logs accept UTF-8 values. Downloading debug logs provides raw UTF-8 data that can be viewed by the administrator with a UTF-8 supported viewer.

Note Microsoft Office Excel is not a supported viewer.

ACS Migration UTF-8 Support

Cisco ISE, Release 1.1 allows for the migration of ACS UTF-8 configuration objects and values. Migration of some UTF-8 objects may not be supported by ISE UTF-8 languages, which might render some of the UTF-8 data that is provided during migration as unreadable using Administrative portal or report methods.

For a complete list of ACS migration issues, see the *Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.*

Note It is the responsibility of the administrator to convert unreadable UTF-8 values (that are migrated from ACS) into ASCII text.

Support for Importing and Exporting UTF-8 Values

You can import or export users to a file and have the UTF-8 values for the fields retained. You can import plain text csv files. The user information is stored as UTF-8 and is presented accordingly in the user list of the Administrative portal. Exported files are provided as csv files.

Note A csv file must be saved in UTF-8 format using an application that supports the UTF-8 format.

UTF-8 Support on REST

UTF-8 values are supported on external REST communication. This applies to configurable items that have UTF-8 support in the Cisco ISE user interface, with the exception of admin authentication. Admin authentication on REST requires ASCII text credentials for login.

For information on supported REST APIs, see the *Cisco Identity Services Engine API Reference Guide, Release 1.1.*

Inherent Usability

The Cisco ISE user interface centralizes network identity management, while providing drill-down access to granular data across the network. The Cisco ISE user interface makes it easier for you to get the information you need to make critical decisions in a timely fashion by providing the following:

- Data based on user roles and their respective tasks
- A centralized administration workspace

- At-a-glance statistics for monitoring network-wide health and security
- Simplified visualizations of complex data

Functional User Interface

The Cisco ISE user interface is role-based and tailored to your job function. Elements that are associated with tasks that are outside of your job description are deactivated or not shown at all.

Menu structures within the user interface link roles to job functions, thereby determining the available permissions. It is possible to be assigned to multiple roles, depending on the nature of your job. For more information, see Understanding the Impact of Roles and Admin Groups, page 2-19.

Centralizing the Administration

The Cisco ISE user interface allows you to perform all necessary network administration tasks from one window. The Cisco ISE home page, also known as the dashboard, is the landing page, displaying real-time monitoring and troubleshooting data. The navigation tabs and menus at the top of the window provide point-and-click access to all other administration features. For more information, see Primary Navigation Tabs and Menus, page 2-8.

At-a-Glance Monitoring

The dashboard consists of dashlets and meters that provide a visual overview of network health and security. These tools allow you to act on issues as they arise. Similar to the warning light on an automobile dashboard, you must go directly to the problem area to resolve an issue that appears on the ISE dashboard. For information on the individual dashboard elements, see Introducing the Dashboard, page 2-12.

Simplifying Complex Data

Dashboard elements visually convey complex information in a simplified format. This display allows you to quickly analyze data and drill down for in-depth information if needed. Dashlets utilize a variety of elements to display data, including sparklines, stack bars, and metric meters. For more information, see Dashboard Elements, page 2-13.

Elements of the User Interface

The ISE user interface provides an integrated network administration console from which you can manage various identity services. These services include authentication, authorization, posture, guest, profiler, as well as monitoring, troubleshooting, and reporting. All of these services can be managed from a single console window called the Cisco ISE dashboard.

This section is an introduction to navigation elements that are incorporated into the Cisco ISE user interface, and covers the following topics:

- Primary Navigation Tabs and Menus, page 2-8
- The Global Toolbar, page 2-9
- Task Navigators, page 2-9
- Getting Help, page 2-11
- Providing Feedback to Cisco, page 2-12

Primary Navigation Tabs and Menus

This section introduces the Cisco ISE primary navigation tabs and the associated menus.

Primary Navigation Tabs

The primary navigation tabs span the top of the Cisco ISE window. Administrators can perform various tasks from the Cisco ISE dashboard depending on their assigned access roles. The major tasks are performed from the following high-level tabs in the user interface:

- Home—This tab is the landing page when you first log into the Cisco ISE console. This page provides a real-time view of all the services running on the Cisco ISE network. You can view more detailed information by double-clicking elements on the page.
- Operations—This tab provides access to tools for monitoring live authentications, querying historical data through reports, and troubleshooting network services. It also provides information on real-time alarms as they occur on the network.
- Policy—This tab provides access to tools for managing network security in the areas of authentication, authorization, profiling, posture, client provisioning. Secure Group Access and select policy elements have direct links for ease of use.
- Administration—This tab provides access to tools for administering the ISE network in these functional areas: System, Identity Management, Network Resources, and Guest Management.

The following illustration shows the Operations primary navigation tab, and its related subtabs. A quicker way to access the navigation tab functionality is through the navigation tab menus, as described in Easy-Access Menus, page 2-8.

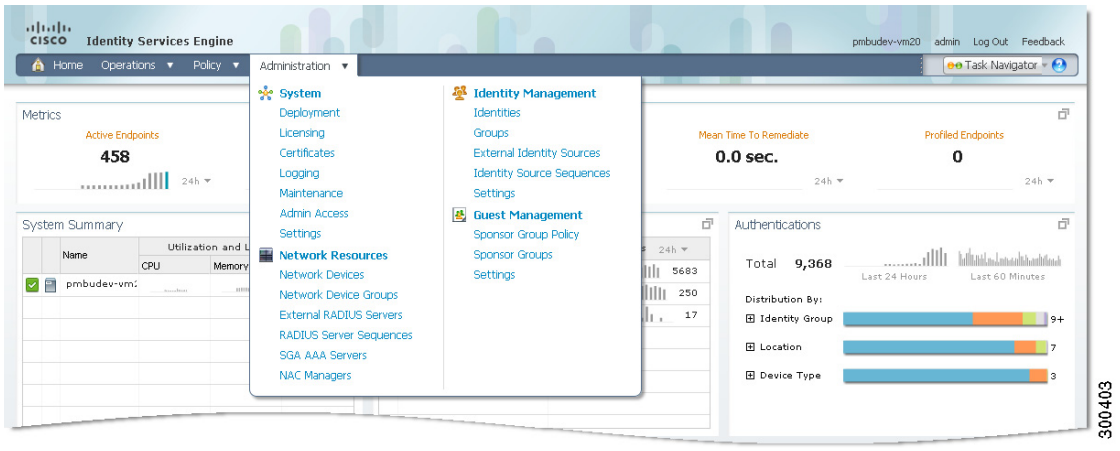
Figure 2-1 Primary Navigation Tabs



Easy-Access Menus

An easy-access menu is a pop-up menu that provides quick access to the features that are associated with a primary navigation tab. Mouse over the title of a navigation tab to bring up the associated menu. Clicking the name links on the menu takes you directly to the feature page. The following illustration is an example of the Administration menu.

Figure 2-2 Navigation Tab Menu



The Global Toolbar

The Global Toolbar is always available at the bottom of the Cisco ISE window, providing instantaneous access to the complete Cisco ISE online Help system and a summary of alarm notifications. Mouse over the Help icon to access the available online Help.

Mouse over the Alarms icon to display the summarized Alarms page, with a list of recent system alarms and the ability to filter for alarms of a specific nature. You can also drill down for detailed information on individual alarms.

Figure 2-3 Global Toolbar



For more information:

- Getting Help, page 2-11.
- Managing Alarms, page 23-11.

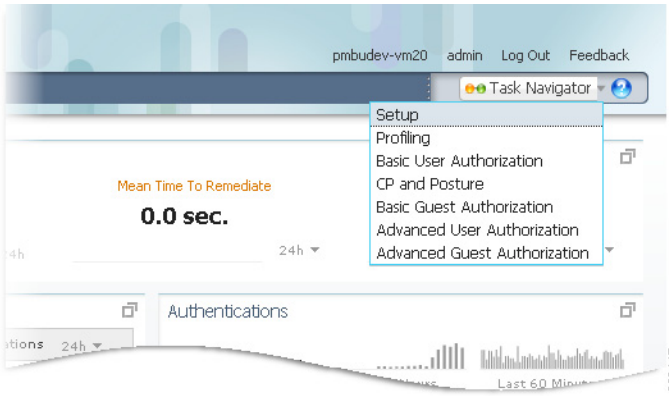
Task Navigators

Task Navigators are visual guides for navigating through procedures whose tasks span multiple screens, such as ISE system setup and profiling. The linear presentation visually outlines the order in which the tasks should be completed, while also providing direct links to the screens where the tasks are performed.

You access Task Navigators from the drop-down menu in the upper right corner of the ISE window. You can choose from the following Task Navigators:

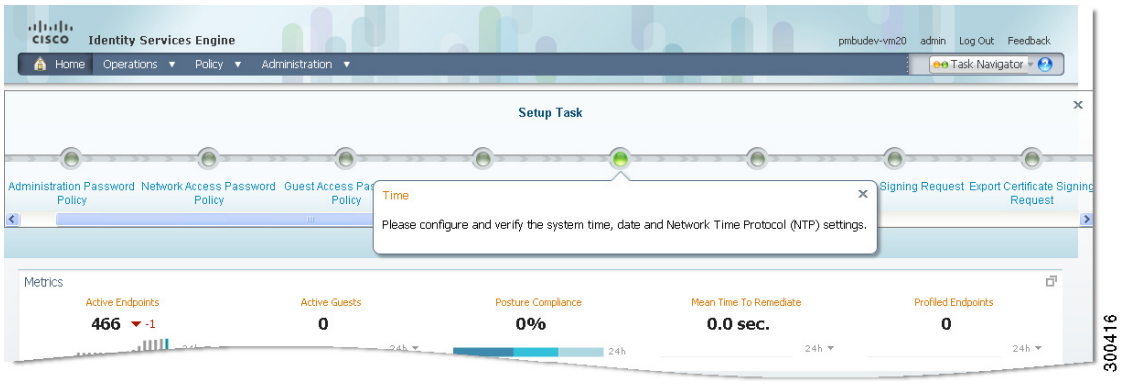
- Infrastructure—Process for fine tuning your ISE network with advanced configuration tasks
- Profiling—Process for profiling endpoints
- Setup—Process for setting up your ISE network after an initial installation

Figure 2-4 Task Navigator Menu



The task navigator displays a series of tasks along a line in the order in which they should be performed, from left to right. Hovering over a task bullet displays a quick view dialog with information on the task. You can close the task navigator at any time by clicking the X icon in the upper right corner.

Figure 2-5 Task Navigator Dialog



Clicking a bullet icon takes you directly to the page where you can begin the associated task.

Task Navigators are a quick reference that you may need to rely on at first. As you complete the tasks and become familiar with the processes, you will quickly outgrow that necessity. For this reason, you can show and hide Task Navigators as needed.

For information on the individual Task Navigators and how to use them, see Chapter 3, "Cisco ISE Task Navigator."

Getting Help

It is easy to get answers to your questions and find information on topics related to Cisco ISE with the following Help tools:

- Global Help, page 2-11
- Page-Level Help, page 2-11

Note You can be a part of improving Cisco ISE by voicing your opinion on specific features or requesting future enhancements by going to Providing Feedback to Cisco, page 2-12.

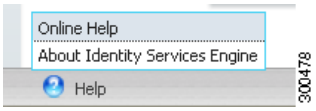
Global Help

The Global Help icon is located in the bottom left corner of the Global Toolbar in the Cisco ISE window. Global Help provides quick access to Cisco ISE comprehensive online Help.

To launch Global Help, complete the following steps:

Step 1 On the global toolbar, move your cursor over the Help icon.

Step 2 Choose **Online Help** from the pop-up menu.



A new browser window appears displaying the Cisco ISE Online Help.

Page-Level Help

You can access contextual (page-level) Help by clicking the Help icon that appears in the upper right corner of the Cisco ISE window. Page-level help provides information on the features, functions, and tasks associated with the current selected page in the Cisco ISE user interface.

To access Help for a current page, complete the following steps:

Step 1 Navigate to a page in the Cisco ISE user interface.

Step 2 In the upper right corner of the Cisco ISE window, click the blue **Help** icon. A browser window appears with links to the Help topics relating to that page.

Providing Feedback to Cisco

You can help improve Cisco ISE by providing feedback to Cisco directly from the Cisco ISE user interface.

To provide feedback on Cisco ISE, complete the following steps:

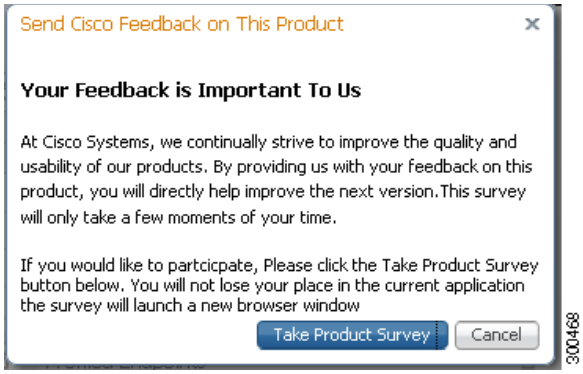
Step 1 Click the **Feedback** link in the upper right corner of the Cisco ISE window to bring up the Send Cisco Feedback on this Product dialog.

Step 2 Click **Take the Product Survey** in the lower right corner of the dialog to launch the survey wizard.

Step 3 Choose the answers that relate to your experience, enter personal comments as desired, and then submit your response.

Your answers and comments are reviewed by the Cisco ISE product team, and are taken into serious consideration.

Figure 2-6 Cisco ISE Feedback Survey



Introducing the Dashboard

The Cisco ISE dashboard is a centralized management window that displays live consolidated and correlated statistical data. The dashboard provides an at-a-glance status of the devices that are accessing your network, and its real-time data is essential for effective monitoring and troubleshooting.

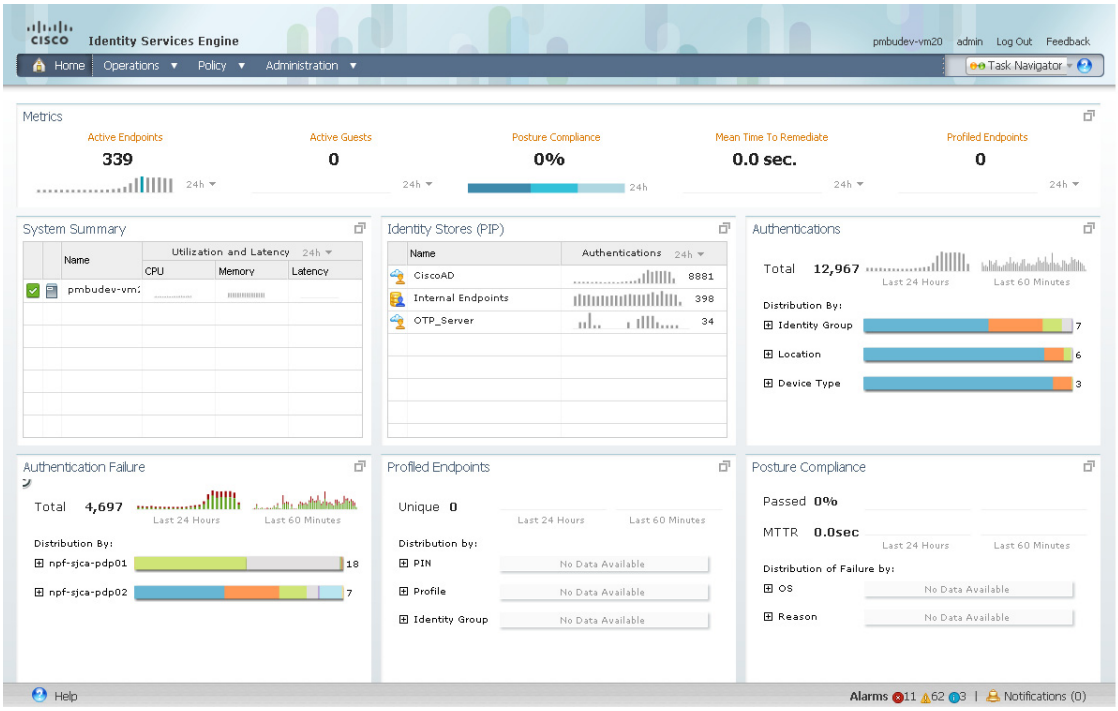
The dashboard uses a variety of elements to convey complex data in simplified formats. Dashboard elements show activity over 24 hours, unless otherwise noted. However, you can mouse over elements to view data for the last 60 minutes in the tooltip display.

Note You must have Adobe Flash Player installed on the Cisco ISE administration node to view the dashlets and meters on the Cisco ISE dashboard. For information on the current recommended version, see the *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

This section introduces the elements that comprise the dashboard, explains how to interpret the different visual representations of data, and covers the following topics:

- Dashboard Elements, page 2-13
- Drilling Down for Details, page 2-15

Figure 2-7 Cisco ISE Dashboard Example



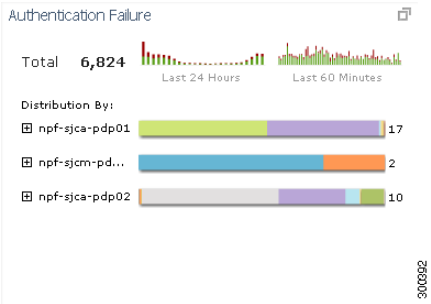
Dashboard Elements

This section introduces dashboard elements, and explains how to interpret the visual data.

Dashlets

Dashlets are individual panels on the dashboard that summarize important statistics about the devices and users that are accessing the network, and the overall health and security of the network. Each dashlet contains an independent function, and can display the statistical data that is related its function in a variety of ways.

Figure 2-8 Dashlet Example



Sparklines

Sparklines are a method of visualizing data with vertical lines that depict trends over time. A sparkline is a small version of a bar chart that portrays utilization or relative load on the system. Taller bars mean there was a higher load at a particular time.

Most sparklines are grouped in time increments. A 24-hour time increment shows 24 sparklines. A 60-minute time increment displays 60 sparklines. For data represented in 24-hour increments only, you can mouse over a sparkline to view data for the last 60 minutes in the tooltip display.

Hover your cursor over a sparkline to bring up a quick view display that explains the data. Click a sparkline to bring up a visual report for the function. For more information, see Viewing Deep-Drill Reports, page 2-16.

Percentages are absolute, but numbers are relative, such as the display “Total: 154” shown in the following example.

Figure 2-9 Sparklines

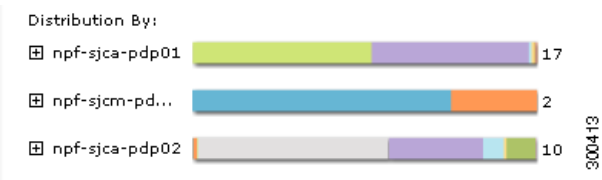


Stack Bars

Stack bars are a method of visualizing data with horizontal blocks of color that depict the distribution of parameters. Color is used as a dividing element, so you can easily see where one parameter ends and another begins. The number of distributions within a stack bar are limited to 10. For this reason, only top 10 distributions are shown.

Hover your cursor over a color area to bring up a quick view display that explains the data.

Figure 2-10 Stack Bars

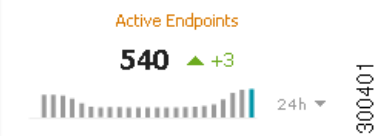


Metric Meters

Metric meters are the small panels that line the top of the dashboard, and summarize the most important statistics regarding the devices that are accessing the network. Metric meters provide an at-a-glance view of network health and performance.

The number display depicts change, similar to a stock market index. Sparklines convey trending and provide the time range selector, which lets you toggle the time interval between 60 minutes or 24 hours. Stack bars represent the distribution of a parameter.

Figure 2-11 Metric Meter

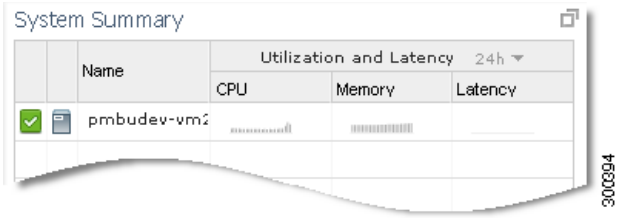


Color and Meaning

In some dashlets, color is used to convey meaning. In general, stack bars use color to mark the boundary points between one data measurement and another. In other dashlets, colors convey a different meaning, such as system health classifications:

- Healthy = Green
- Warning = Yellow
- Critical = Red
- No information = Gray

Figure 2-12 Dashboard Color Significance



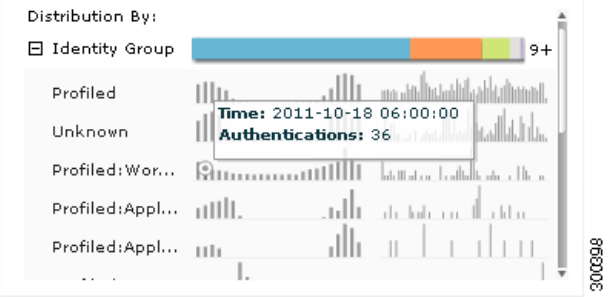
Drilling Down for Details

You can expand some dashlets to see a granular view of the data. Click sparklines to access a deep-drill report.

Expanding Dashlets

If data is available, a plus sign (+) appears next to an item in a dashlet. To view the data, click the plus sign (+). In the following illustration, an Identity Group stack bar is expanded to show a breakdown of authentication identity group data. Place your cursor over a sparkline to display granular authentication details.

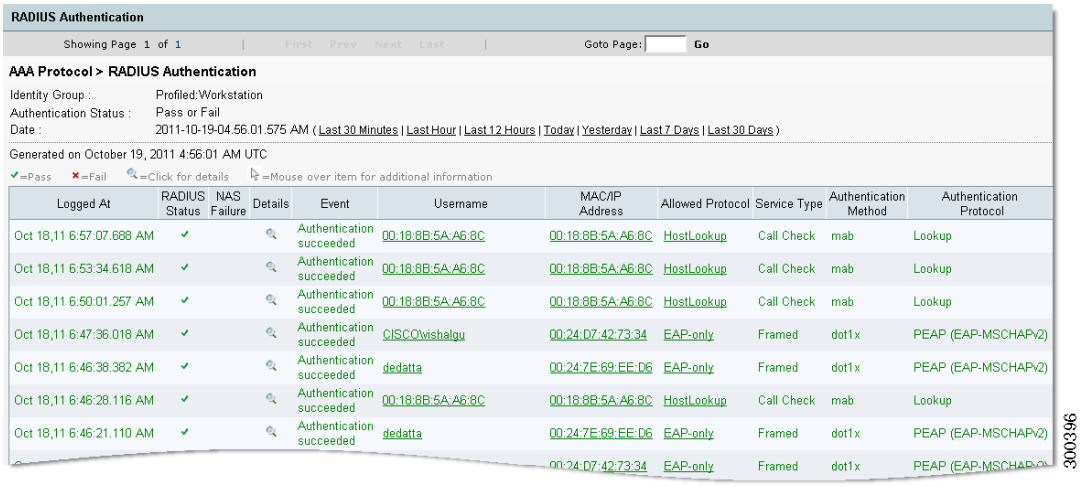
Figure 2-13 Expanded Dashlet



Viewing Deep-Drill Reports

Double-click a sparkline to view an in-depth report of the information. Double-clicking a sparkline in the dashlet that is shown in Figure 2-13 generated and displayed the RADIUS Authentications report that is shown in Figure 2-14.

Figure 2-14 Deep-Drill Report



Common User Interface Patterns

There are several types of cross-functional user interface patterns that enhance usability:

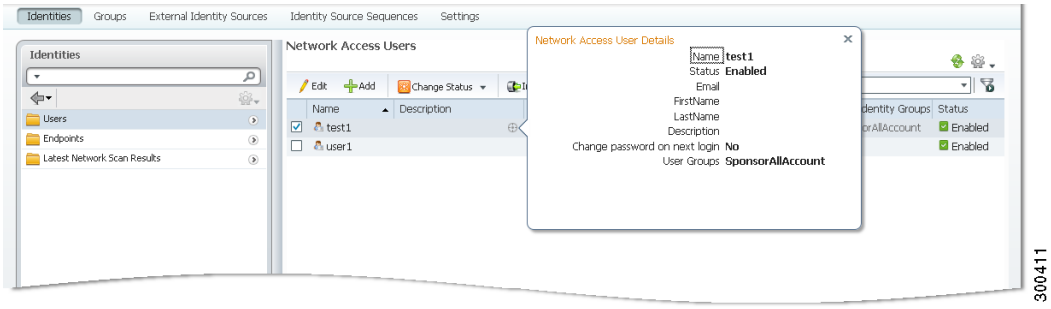
- Quick Views, page 2-17
- Anchored Overlays, page 2-17
- Object Selectors, Navigation Paths, and Object Buttons, page 2-17
- Format Selectors, page 2-18
- Expression Builders, page 2-18

This section covers patterns that occur throughout the Cisco ISE user interface, although the examples shown are associated with Policy tab functions.

Quick Views

A Quick View dialog appears when you place your cursor over a Quick View arrow icon, showing the details of the associated object. In Figure 2-15, the Quick View dialog shows the information for the selected user. To close a Quick View, click the X icon in the upper right corner of the dialog.

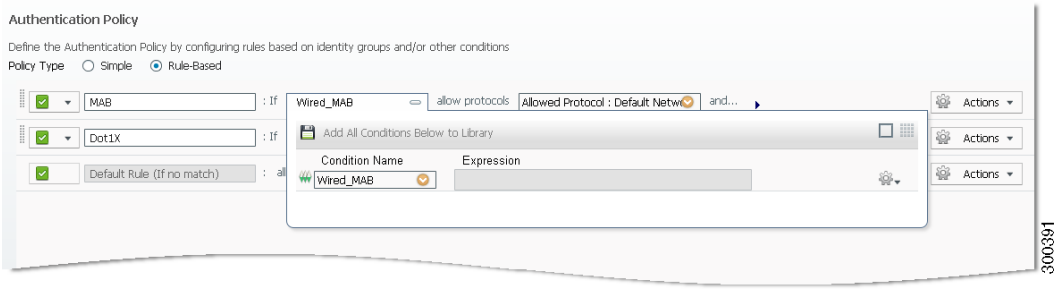
Figure 2-15 Quick View Dialog



Anchored Overlays

An anchored overlay is a stationary pop-up panel that allows you to choose options for a function without having to leave the screen. An anchored overlay is linked to a specific functional element, such as the one that is shown in Figure 2-16. After completing your selections on the anchored overlay, click outside the dialog to close the overlay.

Figure 2-16 Anchored Overlay



Object Selectors, Navigation Paths, and Object Buttons

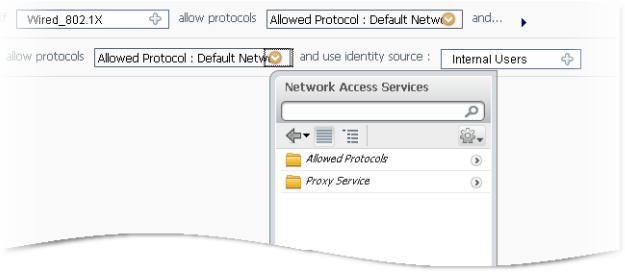
An object selector is a pop-up dialog that displays options for a selected function, as shown in Figure 2-17. An object selector is often linked to another dialog, such as an anchored overlay. Other user interface elements are incorporated into the object selector, such as a search dialog, navigation path, action button, and format selector.

The search dialog is self-explanatory, but these elements may not be familiar to you:

- Navigation path: Click the arrow to display navigation options.
- Action icon: Click the gear-shaped icon to display the drop-down menu from which you can choose an action.

After you make a selection, the dialog closes automatically. For more information, see Format Selectors, page 2-18.

Figure 2-17 Object Selector Dialog



Note When you create nested child objects under **Administration > Identity Management > Groups** (Guest, SponsorAllAccount, SponsorGroupAccounts, SponsorOwnAccount, and so on), you can view and access child objects up to the 15th level in the Object Selector tree view. You must use the pane on the right to view and access child objects that exist beyond the 15th level.

Format Selectors

A format selector is an icon or set of icons in a window, screen, or dialog that allows you to change the display of the data. In many cases, you can choose to view the data in rows or in a tabbed display.

Figure 2-18 Format Selectors

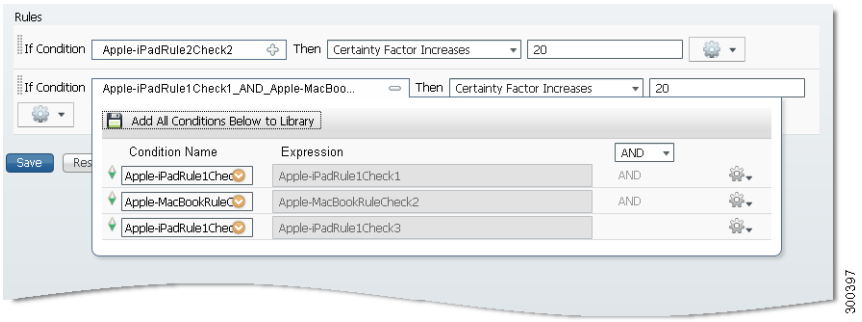


Expression Builders

An expression builder is a pop-up dialog that makes it easier to create expressions, such as those used for authorization policies. You can make your selections interactively to quickly create an expression, such as the one shown in Figure 2-19. Click outside the expression builder to automatically close the dialog.

For information on how to use expression builders to create policies, see Chapter 16, “Managing Authentication Policies.”

Figure 2-19 Expression Builder



Understanding the Impact of Roles and Admin Groups

Cisco ISE provides role-based access control (RBAC) policies that ensure security by restricting administrative privileges. RBAC policies are associated with default admin groups to define roles and permissions. A standard set of permissions (for menu as well as data access) is paired with each of the predefined admin groups, and is thereby aligned with the associated role and job function.

RBAC restricts system access to authorized users through the use of roles that are then associated with admin groups. Each admin group has the ability to perform certain tasks with permissions that are defined by an RBAC policy. Policies restrict or allow a person to perform tasks that are based on the admin group (or groups) to which that person is assigned. You can be assigned to multiple roles, which provides you with privileges for each role to which you are assigned.

Warning **Read-only functionality is unavailable for any administrative access in Cisco ISE, Release 1.1. Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any screen that it can access.**

A specialized administrator role has the ability to customize permissions and admin groups and to create custom policies. The default Cisco ISE RBAC policies cannot be modified, however. For information on the default groups and their assigned permissions, see Chapter 4, "Managing Identities and Admin Access."

Note Some features in the user interface require certain permissions for their use. If a feature is unavailable, or you are not allowed to perform a specific task, your admin group may not have the necessary permissions to perform the task that utilizes the feature. Resources are accessed based on permission, which can be tracked via ise-rbac.log. For more information, see Chapter 4, "Managing Identities and Admin Access."



PART 2

Administering Cisco ISE



CHAPTER 3

Cisco ISE Task Navigator

This chapter introduces the Cisco Identity Service Engine (ISE) Task Navigators, and covers the following topics:

- Navigating Multiple Task Procedures, page 3-1
- Setup, page 3-3
- Profiling, page 3-5
- Basic User Authorization, page 3-6
- Client Provisioning and Posture, page 3-7
- Basic Guest Authorization, page 3-9
- Advanced User Authorization, page 3-10
- Advanced Guest Authorization, page 3-12

Navigating Multiple Task Procedures

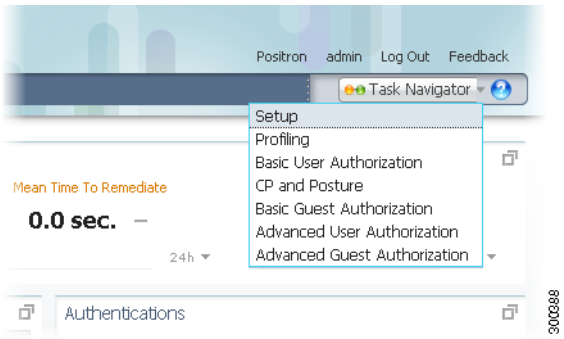
Task Navigators provide a visual path through Cisco ISE administration and configuration processes, which span multiple user interface screens. The linear presentation of the Task Navigator outlines the order in which the tasks should be completed, while also providing direct links to the screens where you perform the tasks.

Note Task Navigators do not retain information about the tasks you have completed. It is a visual guide that takes you directly to the user interface screens where you perform its related tasks.

Task Navigator Menu

The Task Navigator menu appears in the upper right corner of the Cisco ISE window.

Figure 3-1 Task Navigator Menu



Bringing Up and Using a Task Navigator

Each option on the Task Navigator menu brings up a pop-up dialog that shows a list of tasks arranged along a line. The tasks are arranged in the order in which they should be performed, from left to right.

To bring up and use a task navigator, complete the following steps:

Step 1 Right-click the **Task Navigator** menu, and choose one of the following options from the drop-down menu:

- Setup—Perform the first part of the Cisco ISE setup process.
- Profiling—Profile endpoints.
- Basic User Authorization—Establish basic user authorization.
- Client Provisioning and Posture—Configure client provisioning and posture.
- Basic Guest Authorization—Establish basic guest authorization.
- Advanced User Authorization—Establish user authorization, along with client provisioning and posture.
- Advanced Guest Authorization—Establish guest authorization, along with client provisioning and posture.

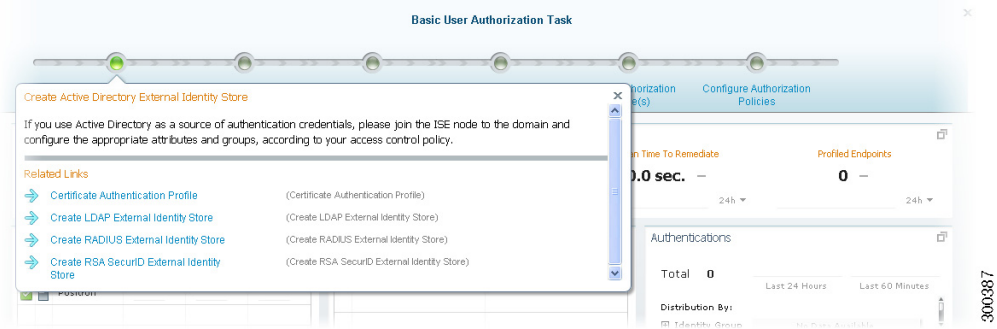
The Task Navigator you selected appears at the top of the window.

Step 2 Complete the tasks in the order in which they appear, starting from the left and moving to the right.

Note Task Navigators do not retain information about the tasks you have completed. It is a visual guide that takes you directly to the user interface screens where you perform its related tasks.

Step 3 To display information about the tasks, hover your cursor over the task bullet. A quick view dialog appears.

Figure 3-2 Basic User Authorization Task



Step 4 To begin a task, click the radio button icon. The page changes, taking you directly to the place where you can begin the task.

Step 5 After completing the last task on the navigation path, click the X icon in the upper right-hand corner to close the dialog.

Next Steps

See the other sections in this chapter for information on each of the Task Navigator options.

Setup

Table 3-1 lists the initial tasks you perform to setup your Cisco ISE network. Links to detailed information about the tasks are provided for your convenience.

Table 3-1 Setup Task Map

Task	Description	User Interface Navigation Path	Documentation Link
1. Administrator password policy	Verify the password policy for Cisco ISE administrators to make sure it is in accordance with your company security policy.	Administration > System > Admin Access > Settings > Password Policy	Configuring a Password Policy for Administrator Accounts, page 4-62
2. Network access password policy	Verify the password policy for internal users who are requesting network access to make sure it is in accordance with your company security policy.	Administration > Identity Management > Settings > User Password Policy	Configuring a User Password Policy for the Network Access User Account, page 4-67
3. Guest access password policy	Verify the password policy for internal users who are requesting network access to make sure it is in accordance with your company security policy.	Administration > Guest Management > Settings > Guest > Password Policy	Configuring Guest Password Policy, page 21-69

Table 3-1 Setup Task Map (continued)

Task	Description	User Interface Navigation Path	Documentation Link
4. Licensing	Verify that you have the correct licensing for the products you purchased.	Administration > System > Licensing > Current Licenses	Adding and Upgrading Licenses, page 12-3
5. Time	Configure and verify the system time, date, and NTP settings.	Administration > System > Settings > System Time	System Time and NTP Server Settings, page 8-18
6. Proxy	Configure the appropriate proxy server settings so that the Cisco ISE node can communicate externally for updates.	Administration > System > Settings > Proxy	Specifying Proxy Settings in Cisco ISE, page 8-17
7. Certificate signing request	Create a certificate signing request (CSR).	Administration > System > Certificates > Local Certificates	Generating a Certificate Signing Request, page 13-8
8. Export certificate signing request	Export the CSR to be submitted to the appropriate Certificate Authority (CA) for your company.	Administration > System > Certificates > Certificate Signing Requests	Viewing and Exporting Certificate Signing Requests, page 13-15
9. Certificate authority certificates	Import the necessary CA certificates to establish trusts for internode communication, Cisco ISE administration, and client authentication.	Administration > System > Certificates > Certificate Authority Certificates	Adding a Certificate Authority Certificate, page 13-18
10. Monitoring and troubleshooting email settings	Configure the correct Simple Mail Transfer Protocol (SMTP) server so that alarms can be sent to the appropriate operations team.	Administration > System > Settings > Monitoring > Email Settings	Configuring Email Settings, page 8-20
11. Monitoring and troubleshooting system alarm settings	Configure the necessary alarm settings so that they meet your operational requirements.	Administration > System > Settings > Monitoring > System Alarm Settings	Configuring System Alarm Settings, page 8-21
12. System logging settings	Configure logging functions, to ensure proper event management operations for your environment.	Administration > System > Logging > Local Log Settings	Chapter 14, “Logging.”
13. Scheduled backup	Configure an automated backup schedule that is based on your data recovery policy.	Administration > System > Maintenance > Data Management > Administration Node > Scheduled Backup	Scheduling a Backup, page 15-7

Table 3-1 Setup Task Map (continued)

Task	Description	User Interface Navigation Path	Documentation Link
14. Distributed deployment	Verify the proper number, type, and synchronization status of the Cisco ISE nodes in your installation.	Administration > System > Deployment	• To configure nodes in your deployment, see the following: – Configuring a Cisco ISE Node, page 9-7 – Registering and Configuring a Secondary Node, page 9-13 • To verify the synchronization status of the nodes in your deployment, see Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 15-12.

Profiling

Table 3-2 lists the tasks you perform to establish profiling for endpoints. Links to detailed information about the tasks are provided for your convenience.

Table 3-2 Task Navigator: Profiling

Task	Description	User Interface Navigation Path	Documentation Link
1. Node sensor configuration	Review each of the Cisco ISE nodes in your deployment and verify that the profiling sensor probes for all of the nodes are configured properly.	Administration > System > Deployment > [Choose a Node] > Edit > Profiling Configuration	Configuring the Probes, page 18-12
2. Verify/Create profiler conditions	Verify or create new profiler conditions for your profiling requirements.	Policy > Policy Elements > Conditions > Profiling > Conditions	Creating a Profiling Condition, page 18-55
3. Verify/Create profiler policy	Verify or create profiler policies using the profiler conditions.	Policy > Profiling > Profiling Policies > Endpoint Policies	Creating an Endpoint Profiling Policy, page 18-40
4. Create Downloadable ACLs[1]	Create appropriate downloadable ACLs for security enforcement.	Policy > Policy Elements > Results > Authorization > Downloadable ACLs > DACL Management > Add	Configuring DACLs, page 17-33

Table 3-2 Task Navigator: Profiling (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Create authorization profiles	Create authorization profiles that are based on the types of privileges that are used for your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles > Add	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28
6. Create authorization rules for profiled endpoints	Create authorization rules for profiled endpoints that are pertinent to your environment.	Policy > Authorization > Standard	Understanding Authorization Policies, page 17-1

1. Downloadable Access Control Lists (ACLs)

Basic User Authorization

The process for setting up basic user authorization involves the use of multiple screens in the user interface. Table 3-3 lists the tasks you perform. Links to detailed information about the tasks are provided for your convenience.

Table 3-3 Task Navigator: Basic User Authorization

Task	Description	User Interface Navigation Path	Documentation Link
1. Create Active Directory External Identity Store	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups, according to your access control policy.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating ISE with Active Directory, page 5-6
2. Create Identity Source Sequences	Create identity source sequences that are based on the external identity stores you created in the previous task.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
3. Verify Authentication Policy	Create or modify the authentication policy to include any new identity source sequences that were created in Task 2.	Policy > Authentication	• For simple authentication policy, see Configuring the Simple Authentication Policy, page 16-26. • For rule-based authentication policy, see Configuring the Rule-Based Authentication Policy, page 16-29.
4. Create Downloadable ACLs	Create the appropriate downloadable ACLs for security enforcement, as necessary.	Policy Elements > Results > Authorization > Downloadable ACLs	Creating and Configuring Permissions for a New DACL, page 17-33

Table 3-3 Task Navigator: Basic User Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Create Authorization Profile(s)	Create authorization profiles that are based on the types of privileges that are used for your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28
6. Create Authorization Policy	Create an authorization policy to grant the appropriate access privileges for your implementation.	Policy > Authorization	Creating a New Authorization Policy, page 17-14

Client Provisioning and Posture

Table 3-4 lists the tasks you perform to establish client provisioning and posture. After login and successful posture, you may also have to perform additional tasks in posture on Acceptable Use Policy and Reassessments, which are not part of this flow. Links to detailed information about the tasks are provided for your convenience.

Table 3-4 Task Navigator: Client Provisioning and Posture

Task	Description	User Interface Navigation Path	Documentation Link
1. Configure Posture updates URL	Initial compliance module download (posture updates) takes 15 to 20 minutes for the first time.	Administration > System > Settings > Posture > Updates	For posture updates through web and offline, see Posture Updates, page 20-22.
2. Configure client provisioning settings	Configure the client provisioning update feed URL.	Administration > System > Settings > Client Provisioning	Setting Up Global Client Provisioning Functions, page 19-26
3. Manual client provisioning resources download and create agent profiles	Download client provisioning resources which you can add from local and remote resources. Create client provisioning agent profiles which you can add from local and remote resources.	Policy > Policy Elements> Results > Client Provisioning > Resources > Add	• For downloading client provisioning resources, see Adding Client Provisioning Resources to Cisco ISE, page 19-5. • For creating client provisioning agent profiles, see Creating Agent Profiles, page 19-12.
4. Create client provisioning policy	Create client provisioning policies that are based on identity groups and operating systems.	Policy > Client Provisioning	Configuring Client Provisioning Resource Policies, page 19-28

Table 3-4 Task Navigator: Client Provisioning and Posture (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Verify/create posture conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined simple conditions are downloaded to Cisco ISE. Create simple conditions for posture as needed.	Policy > Policy Elements > Conditions > Posture	To create the posture simple conditions, see the following: • File Conditions, page 20-44 • Registry Conditions, page 20-55 • Application Conditions, page 20-68 • Service Conditions, page 20-74
6. Verify/create posture compound conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined compound conditions and antivirus and antispyware support chart updates are downloaded to Cisco ISE. Create posture compound conditions using posture simple conditions that are already created.	Policy > Policy Elements > Conditions > Posture	To create posture compound conditions, see the following: • Compound Conditions, page 20-80 • Antivirus Compound Conditions, page 20-88 • Antispyware Compound Conditions, page 20-94
7. Create remediation actions	Create remediation actions, which are listed in alphabetical order.	Policy > Policy Elements > Results > Posture > Remediation Actions	To create remediation actions, see Configuring Custom Posture Remediation Actions, page 20-113.
8. Verify/Create posture requirements	Create posture requirements using posture simple conditions, or compound conditions.	Policy > Policy Elements > Results > Posture > Requirements	Client Posture Assessment Requirements, page 20-155
9. Verify/Create posture policy	Create posture policies using posture requirements.	Policy > Posture	Client Posture Assessment Policies, page 20-33

Basic Guest Authorization

Table 3-5 lists the tasks you perform to establish basic authorization for guests. Links to detailed information about the tasks are provided for your convenience.

Table 3-5 Task Navigator: Basic Guest Authorization

Task	Description	User Interface Navigation Path	Documentation Link
1. Create Active Directory External Identity Store	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups according to your access control policy. In this task, the Active Directory configuration permits employees to use the Guest portal to achieve network access in situations where their endpoint is not working properly, or is not supported.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating ISE with Active Directory, page 5-6
2. Create Identity Source Sequences	Create identity source sequences that are based on the external identity stores you created in the previous task, as necessary.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
3. Configure guest settings	Configure guest settings, as per guest requirements.	Administration > Guest Management > Settings > Guest > Multi-portal Configurations	Multi-Portal Configurations, page 21-49
4. Configure self-service guest settings	Configure self-service guest settings, if “allow for self-service” is selected in the Task 3 configuration.	Administration > Guest Management > Settings > Guest > Portal policy	Configuring Guest Portal Policy, page 21-68
5. Create time profile	Create a guest time profile.	Administration > Guest Management > Settings > Guest > Time profiles	Time Profiles, page 21-70
6. Configure sponsor authentication identity sequence	Provide a sponsor authentication source.	Administration > Guest Management > Settings > Sponsor > Authentication source	Specifying an Authentication Source, page 21-29
7. Create guest sponsor group	Create a guest sponsor group for sponsor login.	Administration > Guest Management > Sponsor Groups	Sponsor Groups, page 21-20
8. Create sponsor policy	Create a guest sponsor login policy.	Administration > Guest Management > Sponsor Group Policy	Sponsor Group Policy, page 21-16

Advanced User Authorization

Table 3-6 lists the tasks you perform for more advanced authorization for users. Links to detailed information about the tasks are provided for your convenience.

Table 3-6 Task Navigator: Advanced User Authorization

Task	Description	User Interface Navigation Path	Documentation Link
1. Create Active Directory external identity store	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups, according to your access control policy. Internal guest users do not require an Active Directory Identity Store setup.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating ISE with Active Directory, page 5-6
2. Create identity source sequences	Create identity source sequences that are based on the external identity stores you created in the previous task, as necessary.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
3. Verify authentication policy	Create or modify the authentication policy to include any new identity source sequences that you created in the previous task.	Policy > Authentication	• For simple authentication policy, see Configuring the Simple Authentication Policy, page 16-26. • For rule-based authentication policy, see Configuring the Rule-Based Authentication Policy, page 16-29.
4. Configure Posture Updates URL	Initial compliance module download (posture updates) takes 15 to 20 minutes for the first time.	Administration > System > Settings > Posture > Updates	For posture updates through web and offline, see Posture Updates, page 20-22.
5. Configure client provisioning settings	Configure the client provisioning update feed URL.	Administration > System > Settings > Client Provisioning	Setting Up Global Client Provisioning Functions, page 19-26
6. Manual client provisioning resources	Download client provisioning resources which you can add from local and remote resources. Create client provisioning agent profiles which you can add from local and remote resources.	Policy > Policy Elements> Results > Client Provisioning > Resources > Add	• For downloading client provisioning resources, see Adding Client Provisioning Resources to Cisco ISE, page 19-5. • For creating client provisioning agent profiles, see Creating Agent Profiles, page 19-12.

Table 3-6 Task Navigator: Advanced User Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
7. Create client provisioning policy	Create client provisioning policies that are based on identity groups and operating systems.	Policy > Client Provisioning	Configuring Client Provisioning Resource Policies, page 19-28
8. Verify/create posture conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined simple conditions are downloaded to Cisco ISE. Create simple conditions for posture as needed.	Policy > Policy Elements > Conditions > Posture	To create posture simple conditions, see the following: • File Conditions, page 20-44 • Registry Conditions, page 20-55 • Application Conditions, page 20-68 • Service Conditions, page 20-74
9. Verify/create posture compound conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined compound conditions and antivirus and antispyware support chart updates are downloaded to Cisco ISE. Create posture compound conditions using posture simple conditions that are already created.	Policy > Policy Elements > Conditions > Posture	To create posture compound conditions, see the following: • Compound Conditions, page 20-80 • Antivirus Compound Conditions, page 20-88 • Antispyware Compound Conditions, page 20-94
10. Create Remediation actions	Create remediation actions, which are listed in alphabetical order.	Policy > Policy Elements > Results > Posture > Remediation Actions	To create remediation actions, see Configuring Custom Posture Remediation Actions, page 20-113.
11. Verify/create posture requirements	Create posture requirements using posture simple conditions, or compound conditions.	Policy > Policy Elements > Results > Posture > Requirements	Client Posture Assessment Requirements, page 20-155
12. Verify/create posture policy	Create posture policies using posture requirements.	Policy > Posture	Client Posture Assessment Policies, page 20-33
13. Create downloadable ACLs	Create the appropriate downloadable ACLs for enforced security, as necessary.	Policy Elements > Results > Authorization > Downloadable ACLs	Creating and Configuring Permissions for a New DACL, page 17-33

Table 3-6 Task Navigator: Advanced User Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
14. Create authorization profiles	Create authorization profiles that are based on the types of privileges that apply to your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28
15. Authorization policies	Create an authorization policy to grant the appropriate access privileges. Choose the conditions and/or attributes in each rule to define an overall network access policy. Create pre-posture and post-posture authorization policies.	Policy > Authorization	Creating a New Authorization Policy, page 17-14

Advanced Guest Authorization

Table 3-7 lists the tasks you perform for more advanced authorization for guests. Links to detailed information about the tasks are provided for your convenience.

Table 3-7 Task Navigator: Advanced Guest Authorization

Task	Description	User Interface Navigation Path	Documentation Link
1. Create Active Directory external identity store	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups, according to your access control policy.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating ISE with Active Directory, page 5-6
2. Create identity source sequences	Create identity source sequences that are based on the external identity stores you created in Task 1, as per requirements.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
3. Configure guest settings	Configure guest settings, as per guest requirements.	Administration > Guest Management > Settings > Guest > Multi-portal Configuration	Multi-Portal Configurations, page 21-49
4. Configure for self-service guest settings	Configure self-service guest settings, if “allow for self-service” was selected in Task 3.	Administration > Guest Management > Settings > Guest > Portal Policy	Configuring Guest Portal Policy, page 21-68

Table 3-7 Task Navigator: Advanced Guest Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Create time profile	Create a guest time profile.	Administration > Guest Management > Settings > Guest > Time Profiles	Time Profiles, page 21-70
6. Configure sponsor authentication identity sequence	Provide a sponsor authentication source.	Administration > Guest Management > Settings > Sponsor > Authentication Source	Specifying an Authentication Source, page 21-29
7. Create guest sponsor group	Create a guest sponsor group for sponsor login.	Administration > Guest Management > Sponsor Groups	Sponsor Groups, page 21-20
8. Create sponsor policy	Create a guest sponsor login policy.	Administration > Guest Management > Sponsor Group Policy	Sponsor Group Policy, page 21-16
9. Verify authentication policy	Create or modify the authentication policy to include any new identity source sequences that you created in the Task 8.	Policy > Authentication	• For simple authentication policy, see Configuring the Simple Authentication Policy, page 16-26. • For rule-based authentication policy, see Configuring the Rule-Based Authentication Policy, page 16-29.
10. Configure Posture Updates URL	Initial compliance module download (posture updates) takes 15 to 20 minutes for the first time.	Administration > System > Settings > Posture > Updates	For posture updates through web and offline, see Posture Updates, page 20-22.
11. Configure client provisioning settings	Configure the client provisioning update feed URL.	Administration > System > Settings > Client Provisioning	Setting Up Global Client Provisioning Functions, page 19-26
12. Manual client provisioning resources	Download client provisioning resources which you can add from local and remote resources. Create client provisioning agent profiles which you can add from local and remote resources.	Policy > Policy Elements> Results > Client Provisioning > Resources > Add	• For downloading client provisioning resources, see Adding Client Provisioning Resources to Cisco ISE, page 19-5. • For creating client provisioning agent profiles, see Creating Agent Profiles, page 19-12.
13. Create client provisioning policy	Create client provisioning policies that are based on identity groups and operating systems.	Policy > Client Provisioning	Configuring Client Provisioning Resource Policies, page 19-28

Table 3-7 Task Navigator: Advanced Guest Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
14. Verify/create posture conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined simple conditions are downloaded to Cisco ISE. Create simple conditions for posture as needed.	Policy > Policy Elements > Conditions > Posture	To create posture simple conditions, see the following: • File Conditions, page 20-44 • Registry Conditions, page 20-55 • Application Conditions, page 20-68 • Service Conditions, page 20-74
15. Verify/create posture compound conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined compound conditions and antivirus and antispyware support chart updates are downloaded to Cisco ISE. Create posture compound conditions using posture simple conditions that are already created.	Policy > Policy Elements > Conditions > Posture	To create posture compound conditions, see the following: • Compound Conditions, page 20-80 • Antivirus Compound Conditions, page 20-88 • Antispyware Compound Conditions, page 20-94
16. Create remediation actions	Create remediation actions, which are listed in alphabetical order.	Policy > Policy Elements > Results > Posture > Remediation Actions	To create remediation actions, see Configuring Custom Posture Remediation Actions, page 20-113.
17. Verify/create posture requirements	Create posture requirements using posture simple conditions, or compound conditions.	Policy > Policy Elements > Results > Posture > Requirements	Client Posture Assessment Requirements, page 20-155
18. Verify/create posture policy	Create posture policies using posture requirements.	Policy > Posture	Client Posture Assessment Policies, page 20-33
19. Create downloadable ACLs	Create the appropriate downloadable ACLs, as needed for enforced security.	Policy Elements > Results > Authorization > Downloadable ACLs	Creating and Configuring Permissions for a New DACL, page 17-33
20. Create authorization profiles	Create authorization profiles that are based on the types of privileges that apply to your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28

Table 3-7 Task Navigator: Advanced Guest Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
21. Authorization policies	Create an authorization policy to grant the appropriate access privileges. Choose the conditions and attributes in each rule to define the overall network access policy. Create pre-posture and post-posture authorization policies.	Policy > Authorization	Creating a New Authorization Policy, page 17-14



CHAPTER 4

Managing Identities and Admin Access

This chapter describes how Cisco Identity Services Engine (ISE) manages its network identities and access to its resources using role-based access control policies, permissions, and settings. Cisco ISE allows you to limit access to a set of network resources or allows a certain type of system operation to be performed based on the identity of individual users, a user group or members, or an endpoint based on its corresponding role. Each role in Cisco ISE defines a set of access policies, permissions, or settings.

A user, user group or member, or an endpoint is recognized by the Cisco ISE network according to its network identity. Once identified, the network grants the access and privileges that are defined and associated with the identity. The following topics provide information and details necessary for understanding the concepts that affect how you manage identities and network access in Cisco ISE:

- Configuring Access for Users, Endpoints, Admins, Groups, Permissions, and Accounts, page 4-2
- Understanding User Identities, Groups, and Admin Access, page 4-2
- Understanding Identity Management Terminology, page 4-4
- Network Access Users, page 4-9
- Endpoints, page 4-15
- Latest Network Scan Results, page 4-26
- Understanding Admin Access Terminology, page 4-26
- Managing Admin Access (RBAC) Policies, page 4-49
- Configuring Settings for Accounts, page 4-60
- Endpoint Identity Groups, page 4-70

Note When you are ready to start configuring access for the Cisco ISE network users, endpoints, administrators, groups, permissions, and accounts, see Configuring Access for Users, Endpoints, Admins, Groups, Permissions, and Accounts, page 4-2.

Configuring Access for Users, Endpoints, Admins, Groups, Permissions, and Accounts

This section is the starting point for configuring access for Cisco ISE network access and sponsor users, endpoints, administrators, user groups, permissions, accounts, and endpoint groups as described in the following topics:

- Configuring Network Access and Sponsor Users, page 4-9
- Configuring Endpoints, page 4-16
- Configuring Cisco ISE Administrators, page 4-33
- Configuring Admin Groups, page 4-37
- Configuring User Identity Groups, page 4-40
- Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-71
- Configuring Menu Access Permissions, page 4-49
- Configuring Data Access Permissions, page 4-53
- Configuring Network Access for User Accounts, page 4-65
- Configuring Network Access User Accounts, page 4-67

Understanding User Identities, Groups, and Admin Access

Once identified and authenticated, each Cisco ISE user, group, or endpoint can access system resources or services and perform network management tasks for which they are authorized. Identification and authentication requires the use of credentials (such as usernames, passwords, certificates, or one-time passwords) that verify each administrator, network access user, user or admin group member, and endpoint as being legitimate and authorized to perform the tasks or activities associated with its identity.

Note An identity role is a set of administrative tasks, each with an associated set of permissions that apply to network users, administrators, groups, or endpoints. For example, an administrator can have more than one predefined role, and a role can apply to multiple administrators.

Identity roles limit each network access user, administrator, or endpoint to a specific set of privileges and access, which is based on identity, type of administrative group in which they belong, or type of endpoint. Each member of an administrative group shares a common set of group-based privileges that are granted to that group. Cisco ISE supports a number of administrative groups, each with a unique set of privileges.

Groups are a collection of individual users or endpoints that share a common set of privileges that allow them to access a specific set of Cisco ISE services and functionality. For example, if you belong to the Change User Password admin group, you can change administrative passwords for other users.

Cisco ISE contains a variety of administrative groups, each with its own set of privileges. Whenever a user is assigned to an administrative group, that user is automatically promoted to an Admin user for that group, and shares the same privileges as every other member of that group.

Note Only the administrator who creates an administrative group can add, delete, or modify the members of that group. Simply being a member of an administrative group does not give that member any administrative privileges over that group.

The Cisco ISE security model limits administrators to creating administrative groups that contain the same set of privileges that the administrator has, which is based on the administrative role of the user as defined in the Cisco ISE database. In this way, administrative groups form the basis for defining privileges for accessing the Cisco ISE systems.

Admin access is the mechanism by which the network resources, services, or functions are defined by your role, and this mechanism affects access for every user, group, or endpoint. Role-based access determines what each entity can access, which is controlled with an access control policy. Role based access also determines the administrative role that is in use, the admin group in which the entity belongs, and the corresponding permissions and settings based upon the role of the entity.

There are three functional groupings for identity management and admin access in Cisco ISE, with each group containing one or more components:

- **Identities**
  - Users—Defined based on user data and assigned role (for details, see Table 4-1). This component is where you can configure a network access user identity for accessing resources and services in a Cisco ISE network.
  - Endpoints—Defined based on the MAC address, device policy, and device identity group to which this endpoint belongs (for details, see Table 4-1). This component is where you can configure a network-capable device identity that can connect to and access resources and services in a Cisco ISE network.

Note In a Cisco ISE network, endpoints represent the total number of supported users and devices. This endpoint can be any combination of users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or other types of network devices. A distinction is made only in the following identity definitions to differentiate between network access users and Cisco ISE network endpoints.

- **Groups**
  - User Identity Groups—Defined based on group name, description, members, group type, and assigned role (for details, see Table 4-1). This component is where you can configure a user group by the group or role name that can access resources and services in a Cisco ISE network.
  - Endpoint Identity Groups—Defined based on group name, description, parent group, and endpoint type (for details, see Table 4-1). This component is where you can configure an endpoint group by the group or device name that can access resources and services in a Cisco ISE network.
- **Admin Access**
  - Policies—Role-based access control (RBAC) policies defined by rule name, groups, and permissions (for details, see Table 4-10). This component is where you can configure RBAC policies that allow admin groups to access resources and services in a Cisco ISE network.
  - Administrators—Defined based on admin user data, admin group, and assigned role (for details, see Table 4-10). This component is where you can create and manage administrators who can access resources and services in a Cisco ISE network.

- Admin Groups—Defined based on group name, description, members, group type, and assigned role (for details, see Table 4-10). This component is where you can create and manage administrator groups who can access resources and services in a Cisco ISE network.
- Permissions—Defined based on group name and role, description, and menu and data access permissions (for details, see Table 4-10). This component is where you can create and manage menu and data access permissions for admin groups to access resources and services in a Cisco ISE network.
- Settings—Defined based on IP address access permissions, password policy, and session timeout values (for details, see Table 4-10). This component is where you can create and manage IP address-based access, password policy, and session timeout settings for users and groups to access resources and services in a Cisco ISE network.

For more information:

The following topics provide information about identity management and admin access terminology and the related user interface that is used in the Cisco ISE network:

- For more information on identity management terminology, see Understanding Identity Management Terminology, page 4-4.
- For more information on managing user and group identities, see Managing User Identity and Group Identity Types Using the User Interface, page 4-5.
- For more information on admin access terminology, see Understanding Admin Access Terminology, page 4-26.

Understanding Identity Management Terminology

Table 4-1 defines and describes basic identity management terminology that applies to the users, groups, group members, and endpoints in ISE.

Table 4-1 ISE Identity Management Terminology

Term	Description	Identity Role
User	User identity is like a container that holds information elements about each user, which form network access credentials for this user. Each user's identity is defined by data that can include username, email address, password, account description, associated administrative group, user group, and role. A user role is a set of permissions that determine what tasks a user can perform or what services can be accessed on the ISE network.	User (for example, a network access user)
Group	Group identity is composed of information elements that identify and describe a specific group of users that belong to the same administrative group. A group name is also a description of the functional role that the members of this group have. A group is a listing of the users that belong to this group. A group role is the set of permissions that determine the tasks each member of this group can perform or the services that can be accessed on the Cisco ISE network. Because common privileges are assigned to a group, any member of that group has that defined set of permissions.	Group (for example, the System Admin group)

Table 4-1 ISE Identity Management Terminology (continued)

Term	Description	Identity Role
Group Member	Group members are individual users that belong to a specific administrative group, and are listed in the Member User table for the group. The Member User table includes information about each member, including the user status (Enabled or Disabled), email address, user name, and user information (using the format: First Name, Last Name). Groups allow you to map individual users to a group, and in this way, confer a role-based identity and privileges associated with the group on each member. By using the Member User table, Cisco ISE allows you to filter entries in a group and add or remove entries in the table. Because group identity and privileges are shared by all members of the group, being a member of a group can also be used as a condition in authorization policies. A group member role is a set of permissions that determine the tasks a user (by virtue of being a member of a group) can perform or the services that can be accessed on the Cisco ISE network.	Group member (for example, a member of the Network Device Admin group)
Endpoints	From the Cisco ISE network perspective, concurrent endpoints can be users, personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, or any other devices supported by the Cisco ISE network. However, from the perspective of the identity role of a specific network device, an endpoint identity defines these items: • The network-capable device type • How the device connects to your Cisco ISE network • The network resources that can be used through wired, wireless network access devices (NADs), or by using a virtual private network (VPN) connection An endpoint role is a set of permissions that determine the tasks that the device can perform or services that can be accessed on the Cisco ISE network.	Endpoint device (for example, an iPhone device)

For more information:

- For more information on administrators and admin groups, see Table 4-10.
- For more information on permissions and settings, see Table 4-10.
- For more information on admin group role types, see Table 4-11.

Managing User Identity and Group Identity Types Using the User Interface

Use the Cisco ISE dashboard as your starting point for displaying and performing the operations that allow you to manage network access users, endpoints, user identity, and endpoint identity groups. You perform management operations by using the controls, tabs, and navigation pane options for the following tasks:

- To configure users—Choose **Administration > Identity Management > Identities**
- To configure Endpoints—Choose **Administration > Identity Management > Identities > Endpoints**

- To configure user identity groups—Choose **Administration > Identity Management > Groups > User Identity Groups**
- To configure endpoint identity groups—Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**

The following identifies the Cisco ISE user interface tab or menu option choices needed to perform tasks associated with users and endpoints:

- Identities—Users
  - Display the currently configured user identities.
  - Create new user identities.
  - Modify or delete existing user identities.
  - Change the status of existing user identities.
  - Import or export user identities using comma-separated value (.csv) files.
  - Duplicate an existing user identity (you can use this identity as a template to create other user identities).
  - Filter or search for existing user identities based on search criteria you configure.
- Identities—Endpoints
  - Display the currently configured endpoint identities.
  - Create new endpoint identities.
  - Modify or delete existing endpoint identities.
  - Import or export endpoint identities using .csv files.
  - Filter or search for existing endpoint identities based on search criteria you configure.

The following identifies the ISE user interface tab or menu option choices needed to perform tasks that are associated with User Identity Groups and Endpoint Identity Groups:

- Identity Groups—User Identity Groups
  - Display the currently configured user identity groups.
  - Create new user identity groups.
  - Modify or delete existing user identity groups.
  - Import or export user identity groups using .csv files.
  - Filter or search for existing user identity groups based on search criteria you configure.
- Identity Groups—Endpoint Identity Groups
  - Display the currently configured endpoint identity groups.
  - Create new endpoint identity groups.
  - Modify or delete existing endpoint identity groups.
  - Filter or search for existing endpoint identity groups based on search criteria you configure.

Table 4-2 lists the configurable user and group identity values you can set using the controls and options available in the Identities tab.

Table 4-2 Cisco ISE User and Group Identity Values

Tab or Sub Tab	User Interface Page Functions	Panel	Values
Identities: Users			
Your starting point for managing network access user values	• Edit • Add • Change Status • Import • Export • Delete • Duplicate • Filter	Network Access User	• Name* • Email
		Password	• Password* • Re-Enter Password*
		User Information	• First Name • Last Name
		Account Options	• Description • Password Change check box (change on next login)
		User Group	• Group affiliation
		Status	• Enabled • Disabled
Identities: Endpoints			
Your starting point for managing endpoint values	• Edit • Create • Delete • Import • Export • Filter	Endpoints	• MAC Address* • Policy Assignment • Identity Group Assignment

Table 4-2 Cisco ISE User and Group Identity Values (continued)

Tab or Sub Tab	User Interface Page Functions	Panel	Values
Groups: User Identity Groups			
Your starting point for managing user identity group and member values	• Edit • Add • Delete • Filter • Import • Export	Identity Group	• Name* • Description
		Member Users	• Users – Status – Email – Username – First Name – Last Name
Groups: Endpoint Identity Groups			
Your starting point for managing endpoint identity group values	• Edit • Create • Delete • Filter	Endpoint Group List	• Name* • Description • Parent Group
		Endpoints	• Identity Group Endpoints – MAC Address

Note Configurable values marked with an asterisk (*) are required.

When you create an identity, you can configure or assign account options using the Account Options panel. To configure or assign account options, check the **Password Change** check box, which prompts each user to change their password at the next login.

Note Only administrators that belong to the Identity Admin group are allowed to perform this same function for administrators.

To complete the configuration using your choices for user or endpoint identity types, click **Submit** to create these identities in the ISE database.

For more information:

- For more information on configuring users, see Configuring Network Access and Sponsor Users, page 4-9.
- For more information on configuring endpoints, see Endpoints, page 4-15.
- For more information on configuring user identity groups, see Configuring User Identity Groups, page 4-40.
- For more information on configuring endpoint identity groups, see Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-71.
- For more information on configuring endpoints in an endpoint identity group, see Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-71.

Network Access Users

A network user is a Cisco ISE user that is authorized to access the ISE network resources based on identity. The network access user identity contains information about the user and forms the network access credentials for the user (and can consist of username, email address, password, account description, associated administrative group, user group, and role).

To support Cisco ISE sponsor groups, you need to explicitly create a sponsor user to be associated with a predefined sponsor group. A sponsor user can be considered as another type of network access user and is created using the same process in the following procedure.

For specific details about sponsor users and sponsor groups, see the *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1*.

Configuring Network Access and Sponsor Users

The Network Access Users window lets you display, create, modify, delete, change the status, import or export users, duplicate, or search for attributes of Cisco ISE network access users. The following topics are covered in this section:

- Displaying Existing Network Access Users, page 4-9
- Creating a New Network Access or Sponsor User, page 4-10
- Modifying an Existing Network Access User, page 4-10
- Deleting an Existing Network Access User, page 4-11
- Changing the Status of an Existing Network Access User, page 4-11
- Importing or Exporting Existing Network Access Users, page 4-12
- Duplicating an Existing Network Access User, page 4-13
- Searching for Specific Attributes in an Existing Network Access User, page 4-13

Warning **Read-only functionality is unavailable for any administrative access in Cisco ISE, Release 1.1. Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any screen that it can access.**

Note You can change the order in which the user groups are listed, and the order is obeyed once it is saved. Be advised that the visual display reverts to alphabetical order, even though the user groups are processed in the newly specified order.

Displaying Existing Network Access Users

Use this procedure to display all existing locally configured network access users.

To display existing network access users, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all existing locally defined network access users.

Step 2 (Optional) To create a new network access user, click the **Action** icon and choose **Create A Network Access User**.

Creating a New Network Access or Sponsor User

Use this procedure to create and configure new locally configured network access users or the required sponsor user that is necessary for Cisco ISE sponsor groups.

For specific details about sponsor users and sponsor groups, see the *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1*.

To create a new network access user or sponsor user, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all locally configured network access users.

Step 2 Click **Add (+)** to create a new network access user.

The Network Access User page appears.

Step 3 Enter values for the following Network Access User fields (for details, see Network Access Users in Table 4-2 on page 4-7).

- Network Access User and Status

Note Do not include spaces in network access user names.

- Password
- User Information
- Account Options
- User Groups

Note You can change the order in which the user groups are listed, and the order is obeyed once it is saved. Be advised that the visual display reverts to alphabetical order, even though the user groups are processed in the newly specified order.

Step 4 Click **Submit** to create a new network access user or sponsor user in the Cisco ISE database.

Modifying an Existing Network Access User

Use this procedure to modify the configuration values for an existing locally configured network access user.

To modify an existing network access user, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all locally configured network access users.

Step 2 Check the check box that corresponds to the network access user that you want to modify, and click **Edit**.

The corresponding Network Access User page appears.

Step 3 Modify the values in the Network Access User fields that you want to change.

- Network Access User and Status
- Password
- User Information
- Account Options
- User Groups

Note You can change the order in which the user groups are listed, and the order is obeyed once it is saved. Be advised that the visual display reverts to alphabetical order, even though the user groups are processed in the newly specified order.

Step 4 Click **Save** to save your modified network access user in the Cisco ISE database.

Deleting an Existing Network Access User

Use this procedure to delete an existing locally configured network access user.

To delete an existing network access user, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all locally configured network access users.

Step 2 Check the check box that corresponds to the network access user that you want to delete.

Step 3 Click **Delete** to delete the network access user you selected.

Step 4 Click **OK** in the confirmation dialog box to confirm that you want to delete this network access user.

The Network Access User page appears with the modified status.

Changing the Status of an Existing Network Access User

Use this procedure to change the status of an existing locally configured network access user.

To change the status of an existing network access user, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all locally configured network access users.

Step 2 Check the check box that corresponds to the network access user whose status you want to change, and click **Change Status > Change Status of Selected**.

The Network Access User page appears with the modified status.

Importing or Exporting Existing Network Access Users

Use the following procedures to import or export locally configured network access users.

To import existing network access users, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all locally configured network access users.

Step 2 Click **Import** to import network access users from a comma-delimited text file.

The Import Users from File page appears.

- In the **File** field, enter the filename containing the network access users to import, or click **Browse** and navigate to the location where the file resides.
- Check the **Create new user(s) and update existing user(s) with new data** check boxes if you want to both create new network access users and update existing network access users.



Note If this check box option is not selected during the import process, only a new user (or users) is created and existing users are not affected by any updates.

Step 3 (Optional) If you do not have a comma-delimited text file, click **Generate a Template** to create this type of file, which includes the following data fields:

- User Name
- First Name
- Last Name
- Email
- User Details
- Password
- Is Password Encrypted True/False
- Enable User Yes/No

Step 4 (Optional) Click **Go Back** to return to the previous window if you decide not to perform an import operation.

Step 5 Click **Save** to save your changes to the Cisco ISE database.

Use this procedure to import locally configured network access users.

To export existing network access users, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all locally configured network access users.

Step 2 Check the check box that corresponds to the network access user(s) that you want to export.

Step 3 Click **Export Selected**.

The Export Network Access User window is displayed, where you are required to enter a key for encrypting the password in the **Key** field.

Step 4 Click **Start Export** to create a users.csv file with the network access user(s) that you selected to export.

The Opening users.csv dialog box appears with two options to choose.

a. Click the **Open with** radio button and choose the application to use to open the users.csv file from the drop-down list (the default is Microsoft Office Excel).

   Click **Other...** to display additional choices.

b. Once you have made your choice, click the **Save File** radio button to save the users.csv file in the format you selected.

Note Check the **Do this automatically for files like this from now** on check box to standardize this process.

c. Click **OK** to export the users.csv file containing the network access users you selected.

Duplicating an Existing Network Access User

Use this procedure to duplicate an existing network access user.

To duplicate an existing network access user, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all locally configured network access users.

Step 2 Check the check box that corresponds to the network access user that you want to duplicate, and click **Duplicate**.

The Network Access Users window appears with the duplicated status.

Step 3 Modify the duplicated network access user as necessary.

Step 4 Click **Submit** to save this new network access user.

Searching for Specific Attributes in an Existing Network Access User

Use this procedure to search for an existing network access user based on specific attributes.

To search for an existing network access user using specific attributes, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Users**.

The Network Access Users window appears listing all locally configured network access users.

Step 2 Click **Filter** and choose from one of the following options:

- Quick Filter (see Step 3)
- Advanced Filter (see Step 4)

Step 3 To perform a Quick Filter, perform the following:

a. Enter search criteria in one or more of the following attribute fields:
   - Status
   - Name

- Description
- First Name
- Last Name
- User Identity Groups
- Admin

b. To filter, click the **Go** button in each field.

Network access user entries that match the specified attribute(s) are displayed in the Network Access Users page.

Step 4 To perform an Advanced Filter, perform the following:

a. Create a matching rule in the **Filter** drop-down list by choosing one of the following options:

- Admin
- Description
- First Name
- Last Name
- Name
- Status
- User Identity Groups

b. In the second drop-down list, choose one of the following options:

- Contains
- Does not contain
- Does not equal
- Ends with
- Is empty
- Is exactly (or equals)
- Is greater than
- Is greater than or equal to
- Is less than
- Is less than or equal to
- Is not empty
- Starts with

c. In the text box, enter your desired search value.

d. Click **Go** to launch the filter process, or click plus (**+**) to add additional search criteria.

e. Click **Clear Filter** to reset the filter process.

Endpoints

An endpoint is typically a network-capable device that connects to your network and uses the resources on your network through wired and wireless NADs and VPNs. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, and fax machines.

The MAC address of an endpoint, expressed in hexadecimal form, is always used to represent the endpoint on your network. An endpoint can be profiled statically when you create the endpoint by using its MAC address, and associating a profile to it along with an endpoint identity group in Cisco ISE.

When endpoints are discovered on your network, they can be profiled dynamically based on the configured endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.

Policy Assignment

If you do not have a matching profiling policy, you can assign an unknown profiling policy. The endpoint is therefore profiled as Unknown. The endpoint that does not match any profile is grouped within the Unknown identity group. The endpoint profiled to the Unknown profile requires that you create a profile with an attribute or a set of attributes collected for that endpoint.

Identity Group Assignment

You can assign an endpoint to an identity group when you create an endpoint statically, or when you do not want to use the Create matching identity group option during evaluation of the endpoint profiling policy for an endpoint. If you do not choose the Static Group Assignment option, then the endpoint is automatically assigned to the matching identity group the next time during evaluation of the endpoint profiling policy.

Static Assignment

You can change the assignment of an endpoint from static to dynamic or from dynamic to static on the Endpoints page. The Endpoints page displays the static assignment status of endpoints as true when an endpoint is created statically, or false when the Static Assignment check box is unchecked during editing an endpoint on the Endpoints page.

Static Group Assignment

You can assign an endpoint to an identity group statically. In such cases, the profiling service does not change the identity group the next time during the policy evaluation for these endpoints, which are previously assigned dynamically to endpoint identity groups in Cisco ISE.

The following section describes the procedure on how to manage endpoints in Cisco ISE:

Configuring Endpoints, page 4-16

Related Topics:

Endpoint Identity Groups, page 4-70

Note For more information on endpoints and endpoint profiling in Cisco ISE networks, see Chapter 18, “Configuring Endpoint Profiling Policies”.

Configuring Endpoints

The Endpoints page allows you to display, configure, and manage endpoints on your network, which provides an option to filter endpoints. You can create an endpoint statically on the Endpoints page. The Endpoints page displays the list of all the endpoints and their associated profiles, MAC addresses, and the status of static assignment as true or false.

This section describes the basic operations that allow you to manage an endpoint, an identity that accesses your network. The following topics are covered in this section:

- Filtering Endpoints, page 4-16
- Creating an Endpoint, page 4-18
- Editing an Endpoint, page 4-19
- Deleting an Endpoint, page 4-20
- Importing Endpoints, page 4-21
- Importing Endpoints from an LDAP Server, page 4-22
- Exporting Endpoints, page 4-25

Filtering Endpoints

You can use the Show drop-down list, or the filter icon to both invoke a quick filter and close it on the Endpoints page. A quick filter is a simple filter that you can use to filter endpoints on the Endpoints page. The quick filter filters endpoints based on field descriptions, such as the endpoint profile, MAC address, and the static status that is assigned to endpoints when they are created on the Endpoints page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the filtering results, on the Endpoints page. The advanced filter filters endpoints based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option, which lists all the preset filters. This option allows you to manage preset filters. Once you have created and saved a preset filter, you can choose a preset filter from the list of filtered results on the Endpoints page. You can also edit preset filters and remove them from the preset filters list.

To filter endpoints on the Endpoints page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears, which lists all the endpoints that are discovered on your network.

Step 2 From the Endpoints page, click the Show drop-down to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 4-3.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 4-17 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 4-17.

Note To return to the endpoints list, choose **All** from the Show drop-down list to display all the endpoints without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters endpoints based on each field description on the Endpoints page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Endpoints page. If you clear the field, it displays the list of all the endpoints on the Endpoints page.

Step 1 To filter, click the **Go** button within each field to refresh the page with the results that are displayed on the Endpoints page.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter endpoints by using variables that are more complex. It contains one or more filters that filter endpoints based on the values that match the field descriptions. A filter on a single row filters endpoints based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter endpoints by using any one or all of the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove a filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save.** Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Note Any preset filter that you create and save is browser-based only and is only accessible using the same browser type (preset filters are not saved in the Cisco ISE database). For example, any preset filter you create and save using a Firefox version 3.6.x browser will not be accessible by a Microsoft Internet Explorer (IE8) browser (or vice versa).

Table 4-3 describes the fields that allow you to filter endpoints on the Endpoints page.

Table 4-3 Filtering Endpoints

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Endpoint Profile	This field enables you to filter endpoints by the name of the endpoint profile.
	MAC Address	This field enables you to filter endpoints by the MAC address of the endpoint.
	Static Assignment	This field enables you to filter endpoints by the endpoint static assignment status.
Advanced Filter	Choose the field description from the following: • Endpoint Profile • MAC address • Static Assignment	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter endpoints.
	Value	From the Value field, choose the value for the field description that you selected against which the endpoints are filtered.

Creating an Endpoint

You can create a new endpoint statically by using the MAC address of an endpoint on the Endpoints page. You have an option to choose an endpoint profiling policy, and an identity group on the Endpoints page for static assignment. Cisco ISE does not reassign the profiling policy and the identity group for statically assigned endpoints.

To create an endpoint on the Endpoints page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

Step 2 From the Endpoints page, choose **Create**.

The New Endpoint page appears.

Step 3 Modify the values on the New Endpoint page, as shown in Table 4-4.

Step 4 Click **Submit**.

The endpoint that you create appears on the Endpoints page.

Step 5 Click **Cancel** to return to the Endpoints page.

Alternatively, you can click the **Endpoint List** link from the New Endpoint page to return to the Endpoints page.

Table 4-4 describes the fields that allow you to create an endpoint on the Endpoints page.

Table 4-4 Creating Endpoints

Field Name	Description
MAC Address	Enter the MAC address in hexadecimal form (for example, nn:nn:nn:nn:nn:nn). If you do not enter the MAC address in hexadecimal form, this field prompts you with the following message: Invalid MAC address. Please enter MAC address as nn:nn:nn:nn:nn:nn
Policy Assignment	From the Policy Assignment field, click the drop-down arrow to view the predefined endpoint profiling policies that can be assigned. Choose an endpoint profiling policy.
Identity Group Assignment	From the Identity Group Assignment field, click the drop-down arrow to view existing identity groups in the system. Choose an identity group.

Editing an Endpoint

You can only edit the endpoint profiling policy that is assigned to endpoints and the identity group while editing endpoints.

To edit an endpoint on the Endpoints page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

Step 2 From the Endpoints page, choose an endpoint, and then choose **Edit**.

Here, you can edit the endpoint profiling policy and the identity group for the selected endpoint. The Attribute List displays the attributes captured for that selected endpoint when created.

Note Click **Delete** to delete an endpoint from the edit page, which removes the endpoint on the Endpoints page. Click **Yes** to delete the endpoint, or click **No** to return to the edit page from the dialog.

Step 3 Modify the values on the edit page, as shown in Table 4-5.

Note You can only edit the endpoint profiling policy and the identity group for an endpoint.

Step 4 Click **Submit**.

The endpoint that you edit appears on the Endpoints page.

Step 5 Click **Cancel** to return to the Endpoints page.

Alternatively, you can click the **Endpoint List** link to return to the Endpoints page.

Table 4-5 describes the fields that allow you to edit an endpoint on the Endpoints page.

Table 4-5 Editing Endpoints

Field Name	Description
MAC address	The MAC address of the selected endpoint is displayed in hexadecimal form.
Policy Assignment	From the Policy Assignment field, click the drop-down arrow to view the predefined endpoint profiling policies that can be assigned. Choose an endpoint profiling policy.
Static Assignment	To change the dynamic status that is assigned to the endpoint, check the Static Assignment check box.
Identity Group Assignment	From the Identity Group Assignment field, click the drop-down arrow to view existing identity groups in the system. Choose an identity group.
Static Group Assignment	To change a dynamic assignment of an endpoint identity group to static, check the Static Group Assignment check box. If the check box is not checked, then the endpoint identity group is dynamic as assigned by the profiler based on policy configuration.

Deleting an Endpoint

You can delete all the endpoints or only the endpoints that you choose from the list on the Endpoints page. The Delete menu has two options: Delete All, which allows you to delete all the endpoints from the list on the Endpoints page, or Delete Selected, which allows you to delete endpoints that you choose from the list on the Endpoints page.

You can also delete an endpoint on the edit page of an endpoint.

To delete an endpoint from the Endpoints page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

Step 2 From the Endpoints page, choose **Delete**.

The Delete Selected and Delete All options appear.

Step 3 From the Endpoints page, choose endpoints that you want to delete from the list.

Step 4 Choose **Delete Selected** or **Delete All**.

A confirmation dialog appears. If endpoints are filtered on the Endpoints page, only those filtered endpoints are deleted from the Endpoints page when you are using the **Delete All** option.

Step 5 Click **OK** to delete endpoints or click **Cancel** to return to the Endpoints page.

Importing Endpoints

You can import endpoints from a comma-separated values (CSV) file in which the list of endpoints appears with the MAC address and the endpoint profiling policy details separated by a comma. The CSV file contains a header row that has two columns that list the MAC address of endpoints in one column, and endpoint profiling policies assigned to those endpoints in the next column.

If the CSV file contains endpoints that have their MAC addresses, and their assigned endpoint profiling policy is the Unknown profile, then those endpoints are immediately reprofiled in Cisco ISE to the matching endpoint profiling policies. However, they are not statically assigned to the Unknown profile. If endpoints do not have profiles assigned to them in the CSV file, then they are assigned to the Unknown profile and reprofiled to the matching endpoint profiling policies.

For example, Table 4-6 shows how Cisco ISE reprofiles Unknown profiles that match the Xerox_Device profile during import. It also shows how Cisco ISE reprofiles an endpoint that is unassigned.

Table 4-6 Unknown Profiles: Import From a File

MAC	Endpoint Profiling Policy Assigned Before Import in Cisco ISE	Endpoint Profiling Policy Assigned After Import in Cisco ISE
00:00:00:00:01:02	Unknown	Xerox-Device
00:00:00:00:01:03	Unknown	Xerox-Device
00:00:00:00:01:04	Unknown	Xerox-Device
00:00:00:00:01:05	If there is no profile assigned to an endpoint, then it is assigned to the Unknown profile, and also reprofiled to the matching profile.	Xerox-Device

If the CSV file contains endpoints that have their MAC addresses, and their assigned endpoint profiling policy is the static assignment, then they are not reprofiled during import. If endpoints are assigned to invalid profiles in the CSV file, then they are not imported because there are no matching profiles in Cisco ISE.

For example, Table 4-7 shows how Cisco ISE retains the Cisco-Device profile, the static assignment of an endpoint during import. It also shows that endpoints are not imported when they are assigned to invalid profiles in the CSV file.

Table 4-7 Static Assignment: Import From a File

MAC	Endpoint Profiling Policy Assigned Before Import in Cisco ISE	Endpoint Profiling Policy Assigned After Import in Cisco ISE
00:00:00:00:01:02	Cisco-Device	Cisco-Device
00:00:00:00:01:03	Unknown	Xerox-Device
00:00:00:00:01:04	Unknown	Xerox-Device
00:00:00:00:01:05	If an endpoint such as 00:00:00:00:01:05 is assigned to an invalid profile other than the profiles that are available in Cisco ISE, then Cisco ISE displays a warning message that the policy name is invalid and the endpoint will not be imported.	The endpoint is not imported because there is no matching profile in Cisco ISE.

Generating a Template

By default, you can use the Generate a Template link to create a CSV file in the Microsoft Office Excel application and save the file locally on your system. When you click the Generate a Template link, the Cisco ISE server displays the Opening template.csv dialog.

This dialog allows you to open the template.csv file, or save the template.csv file locally on your system. If you choose to open the template.csv file from the dialog, the file opens in the Microsoft Office Excel application. The file contains a header row that displays the MAC and Endpoint Policy columns.

Table 4-8 displays the header row in the template.csv file that is created by using the Generate a Template link:

Table 4-8 CSV Template File

MAC	Endpoint Policy
00:1f:f3:4e:c1:8e	Cisco-Device

To import endpoints from a CSV file on the Endpoints page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

Step 2 From the Endpoints page, choose **Import**.

Step 3 From Import, choose **Import From File** and browse to locate the file that you have already exported from the Cisco ISE server.

The file format has to be in the format as specified so that the list of endpoints appears as follows: MAC, Endpoint Policy.

You can also use the Generate a Template link to create a template and save the file. When you use this link, a default template .csv file is created with the following values: 00:22:5e:4d:fe:01, Unknown. You must update the MAC address of endpoints and their profiles and save the file with a different file name. You can use this saved file for importing endpoints. The Microsoft Office Excel application is the default application to open the .csv files.

Note Please format the file so that your list of endpoints appears as follows: MAC, Endpoint Policy. For example, 00:22:5e:4d:fe:01, Unknown.

Step 4 Perform one of the following tasks:

- Click **Submit**, and the endpoints that are imported appear on the Endpoints page.
- Click **Cancel** to return to the Endpoints page.
- Click the **Endpoint List** link from the Import Endpoints page to return to the Endpoints page.

Importing Endpoints from an LDAP Server

Prerequisite:

Before you import from an LDAP sever, ensure that you have installed the LDAP server.

To import endpoints from an LDAP server, complete the following tasks:

Step 1 Deploy the Cisco ISE for your network.

Step 2 Start the LDAP server.

Step 3 Configure the following connection settings:

a. Choose **Administration > Identity Management > Identities > Endpoints > Import > Import From LDAP**.

b. Enter the value for the fields for the connection settings, as shown in Table 4-9 on page 4-24.

- Host
- Port
- Enable Secure Connection
- Root CA Certificate Name
- Anonymous Bind
- Admin DN
- Password
- Base DN

Note You enable either the Anonymous Bind check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.

c. Enter the value for the fields for the query settings, as shown in Table 4-9 on page 4-24.

- MAC Address objectClass
- MAC Address Attribute Name
- Profile Attribute Name
- Time Out

The Lightweight Directory Access Protocol (LDAP) is an application protocol that uses an LDAP directory to query and import data from the LDAP directory. LDAP is an external identity store in Cisco ISE. A directory is a set of objects with attributes that are organized in a logical and hierarchical manner. It is a tree of directory entries that contains a set of attributes. An attribute has a name, and one or more values that are defined in the schema and stored in an LDAP Data Interchange Format (LDIF) file that you use to import the attribute.

Cisco ISE allows you to import MAC addresses and the associated profiles of endpoints securely from an LDAP server. You can use an LDAP server to import endpoints and the associated profiles, by using either the default port 389 or securely over SSL, by using the default port 636.

You have to configure the connection settings and query settings to import from an LDAP server. If the connection settings or query settings are configured incorrectly in Cisco ISE, then the “LDAP import failed:” error message appears.

Root CA Certificate Name

The root certificate authority (CA) certificate name refers to the trusted CA certificate that is required to connect to an LDAP server. You can add (import), edit, delete, and export trusted CA certificates.

Configuring Importing of Endpoints from an LDAP server over SSL

You can import MAC addresses and the associated profiles of endpoints securely from an LDAP server.

To import endpoints from an LDAP server over SSL, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

Step 2 From the Endpoints page, choose **Import**.

Step 3 From Import, choose **Import From LDAP**.

Step 4 Modify the values on the Import Endpoints from LDAP page, as shown in Table 4-9.

Step 5 Perform one of the following tasks:

a. Click **Submit** and the endpoints, which are imported from an LDAP server, appear on the Endpoints page.

b. Click **Cancel** to return to the Endpoints page.

c. Click the **Endpoint List** link from the Import Endpoints from LDAP page to return to the Endpoints page.

Table 4-9 describes the fields that allow you to import endpoints from an LDAP server on the Endpoints page.

Table 4-9 Importing from LDAP

Field Name	Description
Host	Enter the hostname, or the IP address of an LDAP server.
Port	Enter the port number of an LDAP server. You can use the default port 389 to import from an LDAP server, and the default port 636 to import from an LDAP server over SSL. **Note** Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.
Enable Secure Connection	To import from an LDAP server over SSL, check the Enable Secure Connection check box.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates.
Anonymous Bind	To enable the anonymous bind, check the Anonymous Bind check box.
Admin DN	Enter the distinquished name (DN) configured for the LDAP administrator in the slapd.conf configuration file. Admin DN format example: cn=Admin, dc=cisco.com, dc=com
Password	Enter the password configured for the LDAP administrator in the slapd.conf configuration file.
Base DN	Enter the distinguished name of the parent entry. Base DN format example: dc=cisco.com, dc=com.
MAC Address objectClass	Enter the query filter, which is used for importing the MAC address. For example, ieee802Device.

Table 4-9 Importing from LDAP (continued)

Field Name	Description
MAC Address Attribute Name	Enter the returned attribute name for import. For example, macAddress.
Profile Attribute Name	(Optional). Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server. When you configure the Profile Attribute Name field, consider the following: • If you do not specify this LDAP attribute in the Profile Attribute Name field or configure this attribute incorrectly, then endpoints are marked "Unknown" during an import operation, and these endpoints are profiled separately to the matching endpoint profiling policies. • If you configure this LDAP attribute in the Profile Attribute Name field, the attribute values are validated to ensure that the endpoint policy matches with an existing policy in Cisco ISE, and endpoints are imported. If the endpoint policy does not match with an existing policy, then those endpoints will not be imported.
Time Out [seconds]	Enter the time in seconds between 1 and 60 seconds.

Exporting Endpoints

You can export selected or all the endpoints from the Cisco ISE server to different Cisco ISE servers.

To export endpoints on the Endpoints page to a CSV file, do the following:

Step 1 Choose **Administration > Identity Management > Identities > Endpoints**.

The Endpoints page appears.

Step 2 Choose one or more endpoints, and choose **Export**.

The Export Selected and Export All options appear.

Step 3 Choose an option to export selected endpoints, or export all the endpoints from the Endpoints list page. If endpoints are filtered on the Endpoints page, only those filtered endpoints are exported when you are using the **Export All** option.

Step 4 Choose the **Open with** option.

By default, the profiler_endpoints.csv is a Microsoft Office Excel CSV file. For example, the Opening profiler_endpoints.csv dialog box appears, which allows you to open or save the profiler_endpoints.csv file. The Microsoft Office Excel application is the default application to open the .csv files.

Step 5 From the Opening profiler_endpoints.csv dialog box, click **OK**.

The exported list of endpoints appears in the profiler_endpoints.csv file, which opens in the Microsoft Office Excel application. The CSV file displays the header information in two separate columns such as the MAC address and Endpoint Policy. You can save this CSV file locally on your system, as well as use it for importing endpoints.

Step 6 From the Opening profiler_endpoints.csv dialog box, choose **Cancel** to return to the Endpoints page.

of

Latest Network Scan Results

The most recent network scan results are stored in **Administration > Identity Management > Identities > Latest Network Scan Results.**

The Latest Network Scan Results Endpoints page displays only the most recent endpoints that are detected, along with their associated endpoint profiles, their MAC addresses, and their static assignment status, when you perform a manual network scan on any subnet. This page allows you to edit endpoints that are detected from the subnet for better classification, if required.

For more information on how to edit endpoints on the Latest Network Scan Results Endpoints page, see Editing an Endpoint, page 4-19.

Cisco ISE allows you to perform the manual network scan from the Policy Service nodes that are enabled to run the profiling service. You must choose the Policy Service node from the primary Administration ISE node user interface in your deployment, and run the manual network scan from the Policy Service node. During the manual network scan on any subnet, the Network Scan probe detects endpoints on the specified subnet, their operating systems, and check UDP ports 161 and 162 for an SNMP service.

For more information on the manual network scan, see Chapter 18, “Configuring the Network Scan (NMAP) Probe.”

Understanding Admin Access Terminology

Table 4-10 defines and describes some basic admin access terminology that applies to role-based access policies, administrators, admin groups, permissions, and settings in Cisco ISE.

Table 4-10 Cisco ISE Admin Access Terminology

Term	Description
Policies	Role-based access policies (known as Admin access) are access control policies that you define that allow you to restrict the network access privileges for any user or group. Role-based access policies are defined when you configure specific access control policies and permissions. These admin access policies allow you to customize the amount and type of access on a per-user or per-group basis using specified role-based access permission settings that apply to a group or an individual user.
Administrators	An individual who manages or performs a specific type of administrative task using the Cisco ISE user interface is considered an admin (or administrator). Administrators are dependent upon the admin role assigned to them, which limits the network access or tasks they can perform (a role-based access approach). Using the Cisco ISE user interface, administrator roles can perform the following tasks: • Change admin or user passwords • Manage deployments, helpdesk operations, monitoring and troubleshooting nodes, and network devices • Manage Cisco ISE services policies and admin access, Cisco ISE administrator accounts and roles, Cisco ISE administrative functions, and Cisco ISE system configuration and operations

Table 4-10 Cisco ISE Admin Access Terminology (continued)

Term	Description
Admin Groups	These are groups that contain a number of users that all belong to the same administrative group. Each user that belongs to an administrative group is listed in the Member User table for that group, which includes information about each member, such as user status (Enabled or Disabled), email address, user name, First Name, and Last Name. Cisco ISE allows you to filter entries in a group, and add or remove entries from the Member User table. Applying role-based access information to groups directly maps these limits to any individual user who belongs to that group, because all group members share a common identity and the privileges assigned to that role (for example, users with the Network Device Admin role). A user's identity as a member of a specific administrative group can also be used as a condition in authorization policies. The supported Cisco ISE admin group roles and the tasks each role type can manage are listed and described in Table 4-11 on page 4-28.
Permissions	Cisco ISE uses this process to control permissions or access rights to specific users or groups of users. Permissions allow you to control the ability of an individual user or group to access or manage any network service or resource. The Cisco ISE user interface provides two options: menu access and data access. Cisco ISE allows you to create, modify, duplicate, or delete permission privilege settings that limit access to Cisco ISE menus and Cisco ISE data.
Settings	Cisco ISE uses this process to configure three key settings that affect admin access: • Access • Password Policy • Session Timeout The Access settings allow you to configure access connection restrictions with two options (allow all IP addresses or allow only listed IP addresses). This option allows you to configure a list of IP addresses with a subnet mask that you configure for access. You can also edit or delete any IP addresses with a subnet mask in the configured list. The Password Policy settings consist of two tabs (Password Policy and Advanced) that you can use to create an admin access password policy. Under the Password Policy tab, you can choose from eight check boxes and two text fields to configure a password policy. **Note** For passwords with UTF-8 characters, it is important to uncheck the following password policy options: Lowercase alphabetic characters, Uppercase alphabetic characters. Under the Advanced tab, you can define a password history setting in a text field or use two check boxes and text fields to define the lifetime of an admin access password. The Session Timeout setting allows you to define a session idle timeout period in minutes. After this period elapses, the session times out and access is no longer possible during this session.

Administrative users are users of Cisco ISE that can be assigned to one or more admin-level groups. You can create an administrative user when you first configure Cisco ISE users or you can promote an existing user to this role. Administrative users can also be demoted to simple network user status by disabling the corresponding administrative privileges.

Note Administrators can be considered users that have local privileges to configure and operate the Cisco ISE system.

Table 4-11 Cisco ISE Admin Group Roles and Responsibilities

Admin Group Role	Description
Helpdesk Admin	This role provides access for querying all monitoring and troubleshooting operations and within the Cisco ISE administrative console, and can perform the following tasks: • Run all reports • Run all troubleshooting flows • View the Cisco ISE dashboard and livelogs • View alarms This role cannot create, update, or delete reports, troubleshooting flows, live authentications, or alarms.
Identity Admin	This role provides access for managing all of the internal user identities that use the Cisco ISE administrative console across the Cisco ISE network. This role has read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups).
Monitoring Admin	This role provides access to all monitoring and troubleshooting operations within the Cisco ISE administrative console, and can perform the following tasks: • Manage all reports (run, create, and delete) • Run all troubleshooting flows • View the Cisco ISE dashboard and livelogs • Manage alarms (create, update, view, and delete)
Network Device Admin	This role provides access for Cisco ISE administrators that manage only the Cisco ISE network device repository and perform tasks such as adding, updating, or deleting devices. This role has the following permissions: • Read and write permissions on network devices • Read and write permissions on NDGs and all network resources object types
Policy Admin	This role provides access for Cisco ISE policy administrators who are responsible for creating and managing the policies for all Cisco ISE services across the network that are related to authentication, authorization, posture, profiler, and client provisioning. This role has the following permissions: • Read and write permissions on all the elements used in policies, such as authorization profiles, NDGs, and conditions • Read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups) • Read and write permissions on services policies

Table 4-11 Cisco ISE Admin Group Roles and Responsibilities (continued)

Admin Group Role	Description
RBAC Admin	This role provides full access (read and write permissions) to perform all activities under the Operations tab and partial access to some menu items under the Administration tab. This role has the following permissions: • View the authentication details • Enable or disable endpoint protection service • Create, edit, and delete alarms; generate and view reports; and use ISE to troubleshoot problems in your network • Read permissions on administrator account settings and admin group settings • View permissions on admin access and data access permissions along with the RBAC policy screen.
Super Admin	This role provides access to every Cisco ISE administrative function. This role is assigned to the default administrator account, and has create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources. **Note** The super admin user cannot modify the default system-generated RBAC policies and permissions. To do this, you must create new RBAC policies with the necessary permissions based on your needs, and map these policies to any admin group.
System Admin	This role provides access for Cisco ISE administrators who are responsible for Cisco ISE configuration and operations. This role provides full access (read and write permissions) to perform all activities under the Operations tab and partial access to some menu items under the Administration tab. This role has the following permissions: • Read permissions on administrator account settings and administrator group settings • Read permissions on admin access and data access permissions along with the RBAC policy screen. • Read and write permissions for all options under the Administration > System menu. • View the authentication details • Enable or disable endpoint protection service • Create, edit, and delete alarms; generate and view reports; and use ISE to troubleshoot problems in your network

Managing Admin Access Types Using the User Interface

Use the Cisco ISE dashboard as your starting point for displaying and performing admin access management operations that allow you to manage policies, administrators, admin groups, permissions, and settings. You perform management operations by using the controls, tabs, and navigation pane options to perform the following tasks:

- Configure RBAC policies—Choose **Administration > System > Admin Access > Authorization > Policy**
- Configure administrators—Choose **Administration > System > Admin Access > Administrators > Local Administrators**

- Configure admin groups—Choose **Administration > System > Admin Access > Administrators > Admin Groups**
- Configure permissions—Choose **Administration > System > Admin Access > Authorization > Permissions**
- Configure settings—Choose **Administration > System > Admin Access > Settings**

Table 4-12 lists the admin access types and configurable values you can set using the Admin Access tab.

Table 4-12 Cisco ISE Admin Access Types and Values

Tab: Sub Tab	User Interface Page Functions	Panel	Values
Admin Access: Policies			
Your starting point for managing RBAC policies and values	Create role-based admin access policies	RBAC	• Rule • RBAC Groups • Permissions
Admin Access: Local Administrators			
Your starting point for managing Administrators	• Add • Edit • Change Status • Delete • Duplicate • Filter	New Administrator (or Edit)	Admin User • Name • Email • Status (Enabled or Disabled) Password • Password* • Re-Enter Password* User Information • First Name • Last Name Account Options • Description Admin Groups

Table 4-12 Cisco ISE Admin Access Types and Values (continued)

Tab: Sub Tab	User Interface Page Functions	Panel	Values
Admin Access: Admin Groups			
Your starting point for managing Admin Groups	• Add • Edit • Duplicate • Delete • Filter	Admin Groups	Admin Group • Name* • Description
			Member User • Status • Email • Username • First Name • Last Name **Note** In the Member Users page, you can add, remove, or search for member users having a specific attribute (or attributes) using either the Quick Filter or Advanced Filter search function.
Admin Access: Permissions			
Your starting point for managing Permissions	Menu Access • Add • Edit • Duplicate • Delete Data Access • Add • Edit • Duplicate • Delete	Menu Access	Create Menu Access Permission • Name* • Description
			Menu Access Privileges • Show or Hide • Menu Access Permission for: – Operations – Policy – Administration
		Data Access	Create Data Access Permission • Name* • Description
			Data Access Privileges • Full Access or No Access • Data Access Permission for: – Admin Groups – User Identity Groups – Endpoint Identity Groups – All Locations – All Device Types

Table 4-12 Cisco ISE Admin Access Types and Values (continued)

Tab: Sub Tab	User Interface Page Functions	Panel	Values
Admin Access: Settings			
Your starting point for managing Settings	Access	Configure Access Restriction	• Allow all IP addresses to connect • Allow only listed IP addresses to connect
		Configure IP List for Access Restriction	• Add • Edit • Delete
	Password Policy	Password Policy tab	Password check boxes and text fields requirements: • Minimum length* • Non-allowed characters or reverse order • Lowercase alphabetic characters • Uppercase alphabetic characters • Numeric characters • Non-numeric characters **Note** For passwords with UTF-8 characters, it is important to uncheck the following password policy options: Lowercase alphabetic characters, Uppercase alphabetic characters.
		Advanced tab	• Password history setting • Password lifetime settings – Disable Account – Disable Reminder
	Session Timeout	Session Timeout tab	• Session Idle Timeout* (in minutes)

Note Configurable values marked with an asterisk (*) are required.

For more information:

- For more information about managing RBAC policies—See Configuring RBAC Policies, page 4-56 and Configuring RBAC Permissions, page 4-49.
- For more information about managing administrators—See Configuring Cisco ISE Administrators, page 4-33 and Administrator Access Settings, page 4-60.

- For more information about managing administrator Groups—See Configuring Admin Groups, page 4-37.
- For more information about Configuring Cisco ISE to allow for administrator authentication using credentials that are stored on an external identity source—See Configuring Cisco ISE for Administrator Access Using an External Identity Store, page 4-44.
- For more information about managing user identity groups—See Configuring User Identity Groups, page 4-40.
- For more information about managing endpoint identity groups—See Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-71 and Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-71.

Configuring Cisco ISE Administrators

Use the Admin Users window to display, create, modify, delete, change the status, duplicate, or search for attributes of Cisco ISE administrators. The following topics are covered in this section:

- Displaying Existing Cisco ISE Administrators, page 4-33
- Creating a New Cisco ISE Administrator, page 4-33
- Modifying an Existing Cisco ISE Administrator, page 4-34
- Deleting an Existing Cisco ISE Administrator, page 4-34
- Changing the Status of an Existing Cisco ISE Administrator, page 4-35
- Duplicating an Existing Cisco ISE Administrator, page 4-35
- Searching for Specific Attributes in an Existing Cisco ISE Administrator, page 4-35

Displaying Existing Cisco ISE Administrators

Use this procedure to display the list of currently configured Cisco ISE administrators.

To display existing Cisco ISE administrators, choose **Administration > System > Admin Access > Administrators > Local Administrators**.

The Administrators window appears, listing all existing locally defined administrators.

Creating a New Cisco ISE Administrator

Use this procedure to create a new Cisco ISE administrator.

To create a new Cisco ISE administrator, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Local Administrators**.

The Administrators window appears, listing all existing locally defined administrators.

Step 2 Click **Add (+)**, and do one of the following:

- **Create New User**

  If you choose Create New User, a blank Admin User page appears that you must configure.

- **Select from Network Access Users**

  If you choose Select from Network Access Users, a list of current users appears from which you can click to choose a user, and the corresponding Admin User page appears.

Step 3 Enter values for the following Administrator fields (for details, see Administrators in Table 4-12 on page 4-30).

- Admin User and Status
- Password (if you click the **External** option, the Password and Re-Enter Password fields are not used)
- User Information
- Account Options
- Admin Groups

Step 4 Click **Submit** to create the new Administrator in the Cisco ISE database.

Modifying an Existing Cisco ISE Administrator

Use this procedure to modify an existing Cisco ISE administrator configuration.

To modify an existing Cisco ISE administrator, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Local Administrators**.

The Administrators window appears.

Step 2 Check the check box that corresponds to the administrator that you want to modify, and click **Edit**.

The corresponding Admin User page appears.

Step 3 Modify the values in the following Admin User fields that you want to change.

- Admin User and Status
- Password (if you click the **External** option, the Password and Re-Enter Password fields are not used)
- User Information
- Account Options
- Admin Groups

Step 4 Click **Save** to save the modified administrator in the Cisco ISE database.

Deleting an Existing Cisco ISE Administrator

Use this procedure to delete an existing Cisco ISE administrator.

To delete an existing Cisco ISE administrator, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Local Administrators**.

The Administrators window appears.

Step 2 Check the check box that corresponds to the administrator that you want to delete, click **Delete**, and do one of the following:

- Click **Remove from Administrator List.** The selected Administrator is removed from the list.
  - This action removes the selected Administrator from the list, but does not delete the user account.
- Click **Delete Admin User**, then click **OK**.

– This action deletes the selected administrator from the Cisco ISE database.

Changing the Status of an Existing Cisco ISE Administrator

Use this procedure to change the status of an existing Cisco ISE administrator.

To change the status of an existing Cisco ISE administrator, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Local Administrators**.

The Administrators window appears.

Step 2 Check the check box that corresponds to the administrator whose status you want to change, and click **Change Status**.

Step 3 Click **OK** in the confirmation dialog box to change the status of the selected administrator.

The Administrators window appears with this modified status.

Duplicating an Existing Cisco ISE Administrator

Use this procedure to duplicate an existing Cisco ISE administrator.

To duplicate an existing Cisco ISE administrator, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Local Administrators**.

The Administrators window appears.

Step 2 Check the check box that corresponds to the administrator who you want to duplicate, and click **Duplicate**.

The Administrators window appears with the duplicated status.

Step 3 Modify the duplicated administrator as necessary.

Step 4 Click **Submit** to save this new administrator.

Searching for Specific Attributes in an Existing Cisco ISE Administrator

Use this procedure to search for an existing Cisco ISE administrator based on specific attributes.

To search for an existing Cisco ISE administrator using specific attributes, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Local Administrators**.

The Administrators window appears.

Step 2 Click **Filter** and choose one of the following options:

- Quick Filter (see Step 3)
- Advanced Filter (see Step 4)

Step 3 To perform a Quick Filter, perform the following:

a. Enter search criteria in one or more of the following attribute fields:
   - Status
   - Name
   - Description
   - First Name
   - Last Name
   - Admin Groups

b. To filter, click the **Go** button in each field.

   Cisco ISE administrator entries that match the specified attribute(s) are displayed in the Cisco ISE Administrators page.

Step 4 To perform an Advanced Filter, create a matching rule by performing the following:

a. Choose one of the following options from the Filter drop-down list:
   - Admin Groups
   - Description
   - First Name
   - Last Name
   - Name
   - Status

b. Choose one of the following options from the second drop-down list:
   - Contains
   - Does not contain
   - Does not equal
   - Ends with
   - Is empty
   - Is exactly (or equals)
   - Is greater than
   - Is greater than or equal to
   - Is less than
   - Is less than or equal to
   - Is not empty
   - Starts with

c. In the text box, enter your desired search value.

d. Click **Go** to launch the filter process, or click plus (**+**) to add additional search criteria.

e. Click **Clear Filter** to reset the filter process.

Configuring Admin Groups

The Admin Groups window lets you display, create, modify, delete, duplicate, or filter Cisco ISE network admin groups. The following topics are covered in this section:

- Displaying Existing Admin Groups, page 4-37
- Creating an Admin Group, page 4-37
- Modifying an Existing Admin Group, page 4-38
- Deleting an Existing Admin Group, page 4-38
- Duplicating an Existing Admin Group, page 4-39
- Searching for Specific Attributes in an Existing Admin Group, page 4-39

Prerequisite

To configure an external administrator group type, you must have already specified one or more external identity stores according to the guidelines that are found in these sections:

- Microsoft Active Directory, page 5-4
- LDAP, page 5-17
- RADIUS Token Identity Sources, page 5-32
- RSA Identity Sources, page 5-39

Displaying Existing Admin Groups

Use this procedure to display existing admin groups.

To display existing admin groups, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Admin Groups**.

The Admin Groups window appears.

Creating an Admin Group

Use this procedure to create an admin group (and create or delete users within that admin group).

To create an admin group, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Admin Groups > Add**.

The Admin Groups window appears.

Step 2 Enter the values for the following Admin Group fields.

- Name
- Description

Step 3 Specify the **Type** of administrator group you are configuring:

- Internal—Administrators assigned to this group type will authenticate against the credentials that are specified in the Cisco ISE internal database.

- External—Administrators that you assign to this group will authenticate against the credentials that are contained in the external identity store that you specify in the attribute selector. After choosing **External**, specify the identity store from which Cisco ISE should import the external group information.

Note To configure an external administrator group type, you must have already specified one or more external identity stores according to the guidelines in the applicable sections of Chapter 5, "Managing External Identity Sources."

Step 4 To add users to the Admin Group Users table, click **Add**. From the Users page, select the users to be added to the admin group.

Step 5 To delete users from the Admin Group Users table, check the check box corresponding to the user that you want to delete and click **Remove**.

Step 6 Click **Submit** to save any changes made to the admin group that you created in the Cisco ISE database.

Modifying an Existing Admin Group

Use this procedure to modify the configuration values for an existing locally configured admin group.

To modify an existing admin group, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Admin Groups**.

The Admin Groups window appears.

Step 2 Check the check box that corresponds to the admin group that you want to modify, and click **Edit**.

The corresponding Admin Group page appears.

Step 3 Modify the member users that are part of this admin group as follows:

- Click **Add** to add new member.
- Check the check box corresponding to existing members, and click **Remove** to delete users.
- Click **Quick Filter** or **Advanced Filter** and search on specific attributes for admin group users.

Step 4 Click **Save** to save your modified network access user in the Cisco ISE database.

Deleting an Existing Admin Group

Use this procedure to delete an existing admin group (and by doing so, delete the users within that admin group).

To delete an existing admin group, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Admin Groups**.

The Admin Groups window appears.

Step 2 Check the check box that corresponds to the admin group that you want to delete, and click **Delete**.

A Delete Confirmation dialog box appears.

Step 3 Click **OK** to confirm the deletion of the selected admin group.

Duplicating an Existing Admin Group

Use this procedure to duplicate an existing admin group.

To duplicate an existing admin group, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Admin Groups**.

The Admin Groups window appears.

Step 2 Check the check box that corresponds to the admin group you want to duplicate, and click **Duplicate**.

The Admin Group window appears with the duplicated status.

Step 3 Modify the duplicated admin group as necessary.

Step 4 Click **Submit** to save this new admin group.

Searching for Specific Attributes in an Existing Admin Group

Use this procedure to search for an existing admin group based on specific attributes.

To search for an existing admin group using specific attributes, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Admin Groups**.

The Admin Groups window appears.

Step 2 Click **Filter** and select from one of the following options:

- Quick Filter
- Advanced Filter

To perform a Quick Filter, enter search criteria in one or more of the following attribute fields:

- Name
- Description

a. To perform an Advanced Filter, create a matching rule by choosing one of the following option in the **Filter** drop-down list:

- Description
- Name

b. In the second drop-down list, choose one of the following options:

- Contains
- Does not contain
- Does not equal

- Ends with
- Is empty
- Is exactly (or equals)
- Is greater than
- Is greater than or equal to
- Is less than
- Is less than or equal to
- Is not empty
- Starts with

c. In the text box, enter your desired search value.

d. Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.

e. Click **Clear Filter** to reset the filter process.

Configuring User Identity Groups

The Identity Groups window lets you display, create, modify, delete, duplicate, or filter Cisco ISE user identity groups. The following topics are covered in this section:

- Displaying a User Identity Group, page 4-40
- Creating a User Identity Group, page 4-41
- Modifying an Existing User Identity Group, page 4-41
- Deleting an Existing User Identity Group, page 4-42
- Importing or Exporting an Existing User Identity Group, page 4-42
- Searching for Specific Attributes in an Existing User Identity Group, page 4-43

Displaying a User Identity Group

Use this procedure to display a Cisco ISE user identity group.

To display existing user identity groups, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > User Identity Groups**.

The User Identity Groups window appears.

Creating a User Identity Group

Use this procedure to create a user identity group (and create or delete users within this local user identity group.

To create a user identity group, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > User Identity Groups**.

The User Identity Groups window appears.

Step 2 In the Identity Groups navigation pane, click **User Identity Groups**, click **Action**, and click **Create Top User Identity Group**.

The User Identity Groups page appears with two panels: Identity Group and Member Users.

Step 3 In the Identity Group panel, enter values in the following fields.

- Name*
- Description

Note Use the best practice to include no spaces when creating the name for a user identity group.

Step 4 To add users to the Member Users table, click **Add** in the Member Users panel.

A Users dialog box appears.

Step 5 Click users listed in the Users dialog box to add them to this identity group.

Step 6 To delete users from the Member Users table, check the check box corresponding to the user that you want to delete, and click **Delete**.

A Delete confirmation dialog box appears. Click **OK** to confirm your user deletion choice.

Step 7 Click **Submit** to save any changes made to the identity group in the Cisco ISE database.

Modifying an Existing User Identity Group

Use this procedure to modify an existing user identity group (and by doing so, modify the users within this local user identity group).

To modify an existing user identity group, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > User Identity Groups**.

The User Identity Groups window appears.

Step 2 In the Identity Groups navigation pane, click **User Identity Groups**.

The User Identity Groups page appears.

Step 3 Check the check box corresponding to the user identity group that you want to modify, and click **Edit**.

The User Identity Groups page appears with two panels: Identity Group and Member Users.

Step 4 Modify the settings in the Identity Group and Member Users panels as necessary (including adding or deleting group members).

Step 5 Click **Submit** to save any changes made to the identity group in the Cisco ISE database.

Deleting an Existing User Identity Group

Use this procedure to delete an existing user identity group (and by doing so, delete the users within this local user identity group).

To delete an existing user identity group, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > User Identity Groups**.

The User Identity Groups window appears.

Step 2 In the Identity Groups navigation pane, click **User Identity Groups**.

The User Identity Groups page appears.

Step 3 Check the check box next to the user identity group that you want to delete, and click **Delete**.

A Delete Confirmation dialog box appears. Click **OK** to confirm your user identity group deletion choice.

Importing or Exporting an Existing User Identity Group

Use this procedure to import or export locally configured user identity groups.

To import or export existing user identity groups, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > User Identity Groups**.

The User Identity Groups window appears.

Step 2 In the Identity Groups navigation pane, click **User Identity Groups**.

The User Identity Groups page appears.

Step 3 Click **Import** to import network access users from a comma-delimited text file.

The Import User Identity Groups from File page appears.

- In the **File** field, enter the filename that contains the user identity group that you want to import, or click **Browse** and navigate to the location where this file resides.
- Check the **Overwrite existing data with new data** check box if you want to both add a new user identity group and update existing user identity groups.
- If this check box option is not selected during the import process, only a new user identity group is created and existing user identity groups are not affected by any updates.

Step 4 (Optional) If you do not have a comma-delimited text file, click **Generate a Template** to create this type of file, which includes the following data fields:

- Identity Group Name
- Identity Group Description

Step 5 (Optional) Click **Go Back** to return to the previous window if you decide not to perform an import operation.

Step 6 Click **Import**.

Step 7 To export a user identity group, you must first check the check box that corresponds to the user identity group that you want to export, and click **Export**.

The "Opening users.csv" window is displayed, and is where you can click **Save File** and click **OK** to create a users.csv file with the network access users that you selected to export.

Step 8 Click **Save** to save your changes to the Cisco ISE database.

Searching for Specific Attributes in an Existing User Identity Group

Use this procedure to search for an existing user identity group based on specific attributes.

To search for an existing user identity group using specific attributes, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > User Identity Groups**.

The User Identity Groups window appears.

Step 2 In the Identity Groups navigation pane, click **User Identity Groups**.

The User Identity Groups page appears.

Step 3 Click **Filter** and choose one of the following options:

- Quick Filter
- Advanced Filter

a. To perform a Quick Filter, enter search criteria in one or more of the following attribute fields:

- Name
- Description

b. To perform an Advanced Filter, create a matching rule by choosing one of the following options in the **Filter** drop-down list:

- Description
- Name

c. In the second drop-down list, choose one of the following options:

- Contains
- Does not contain
- Does not equal
- Ends with
- Is empty
- Is exactly (or equals)
- Is greater than
- Is greater than or equal to
- Is less than
- Is less than or equal to

  - Is not empty
  - Starts with

d. In the text box, enter your desired search value.

e. Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.

f. Click **Clear Filter** to reset the filter process.

Configuring Cisco ISE for Administrator Access Using an External Identity Store

In Cisco ISE you can provide administrator user authentication via an external identity store like Active Directory, LDAP, or RSA SecureID. There are two models you can use to provide authentication via an external identity store:

- External Authentication + External Authorization—There are no credentials that are specified on the local Cisco ISE database for the administrator ID in question, and authorization is based on external identity store group membership only. This is used for Active Directory and LDAP authentication.
- External Authentication + Internal Authorization—There administrator's authentication credentials come from the external identity source, and authorization and administrator role assignment takes place using the local Cisco ISE database. This is used for RSA SecurID authentication. (This method requires you to configure the same username in both the external identity store and the local Cisco ISE database.)

During operation, Cisco ISE is designed to "fall back" and attempt to perform authentication from the internal identity database, if communication with the external identity store has not been established or if it fails. In addition, whenever an administrator for whom you have set up external authentication launches a browser and initiates a login session, the administrator still has the option to request authentication via the Cisco ISE local database by choosing "Internal" from the **Identity Store** drop-down selector in the login dialog.

Note You can configure this method of providing external administrator authentication only via the administrator user interface. The Cisco ISE Command Line Interface (CLI) does not feature these functions.

Prerequisites

- If your network does not already have one or more existing external identity stores, ensure that you have installed the necessary external identity stores and configured Cisco ISE to access those identity stores. See the following sections for guidelines:
  - Microsoft Active Directory, page 5-4
  - LDAP, page 5-17
  - RADIUS Token Identity Sources, page 5-32
  - RSA Identity Sources, page 5-39

External Authentication + External Authorization

By default, Cisco ISE is set up to provide internal administrator authentication. Therefore, to set up external authentication, you need to create a password policy for the external administrator accounts that you define on the external identity stores. You can then apply this policy to the external administrator groups that eventually become a part of the external administrator RBAC policy. For more details on setting up the password policy, see Configuring a Password Policy for Administrator Accounts, page 4-62.

In addition to providing authentication via an external identity store, your network may also require you to use a Common Access Card (CAC) authentication device. If your external network access method requires a CAC, see Configuring Cisco ISE for Administrator CAC Authentication, page 8-4.

To create an external administrator authentication password policy, complete the following steps:

Step 1 Navigate to **Administration > System > Admin Access > Authentication**.

Step 2 On the Authentication Method tab, select **Password Based** and choose one of the external identity sources you should have already configured according to the Prerequisites, which are outlined on page 4-44.

Step 3 Configure any other specific password policy settings according to the guidelines in Configuring a Password Policy for Administrator Accounts, page 4-62.

Step 4 Click **Save**.

Next, you will need to create an external Active Directory or LDAP administrator group. This ensures that Cisco ISE uses the username that is defined in the external Active Directory or LDAP identity store to validate the administrator username and password that you entered upon login. For details, see Creating an Admin Group, page 4-37.

Cisco ISE imports the Active Directory or LDAP group information from the external resource and stores it as a dictionary attribute. You can then specify that attribute as one of the policy elements when it is time to configure the RBAC policy for this external administrator authentication method.

To create an internal administrator group to which you will map the external Active Directory or LDAP identity group, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Admin Groups > Add**.

The Admin Groups window appears.

Step 2 Follow the guidelines that are described in Creating an Admin Group, page 4-37 to create a new external administrator group.

Step 3 Click **Save**.

To specify menu access and data access permissions for the new external administrator group, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and then click the following:

- **Menu Access**
- **Data Access**

The Menu Access or Data Access page appears, listing all existing default and user-defined access permissions.

Step 3 Specify access permissions according to the guidelines in Configuring Menu Access Permissions, page 4-49 and Configuring Data Access Permissions, page 4-53.

Step 4 Click **Save**.

In order to configure Cisco ISE to authenticate the administrator using an external identity store and to specify custom menu and data access permissions at the same time, you must configure a new RBAC policy. This policy must have the *external* administrator group for authentication and the *internal* administrator group with menu and data access permissions to manage administrator external authentication and authorization.

Note You cannot modify an existing (system-preset) RBAC policy to specify these new external attributes. If you have an existing policy that you would like to use as a "template," be sure to duplicate that policy, rename it, and then assign the new attributes. See Duplicating RBAC Policy, page 4-59 for details.

To create a new RBAC policy for external administrator authentication:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.

The RBAC Policies page appears. This page contains a set of ready-to-use predefined policies for default admin groups.

Step 2 Specify the necessary external administrator authentication RBAC policy elements (group, permissions, and so on.) according to the guidelines in Creating Custom RBAC Policy, page 4-57.

Step 3 Click **Save**.

Note Remember that the appropriate external administrator group must be assigned to the correct administrator user IDs. Ensure that the administrator in question is associated with the correct external administrator group, as described in the subsections under Configuring Cisco ISE Administrators, page 4-33.

Figure 4-1 shows an example of the login dialog that is presented to the administrator when an external identity store has been set up in Cisco ISE to provide authentication. Upon logging in, administrators see only the menu and data access items that are specified in the RBAC policy.

Figure 4-1 Administrator Login—External Identity Store Available



Note If you log in as an administrator, and the Cisco ISE RBAC policy is not able to authenticate your administrator identity, Cisco ISE displays an "unauthenticated" message, and you cannot access the Cisco ISE administrator user interface.

External Authentication + Internal Authorization

When configuring Cisco ISE to provide administrator authentication using an external RSA SecurID identity store, administrator credential authentication is performed by the RSA identity store. However, authorization (policy application) is still done according to the Cisco ISE internal database. In addition, there are two important factors to remember that are different from External Authentication + External Authorization:

- You do not need to specify any particular external administrator groups for the administrator.
- You must configure the same username in both the external identity store and the local Cisco ISE database.

To create a new Cisco ISE administrator that authenticates via the external identity store, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Administrators > Local Administrators**.

The Administrators window appears, listing all existing locally defined administrators.

Step 2 Follow the guidelines at Creating a New Cisco ISE Administrator, page 4-33 to ensure that the administrator username on the external RSA identity store is also present in Cisco ISE. Be sure to click the **External** option under Password.

Note Remember: you do not need to specify a password for this external administrator user ID, nor are you required to apply any specially configured external administrator group to the associated RBAC policy.

Step 3 Click **Save**.

When the administrator logs in, the login session passes through the following general steps in the process:

1. The administrator sends a RSA SecurID challenge.
2. RSA SecurID returns a challenge response.
3. The administrator enters a user name and the RSA SecurID challenge response in the Cisco ISE login dialog, as if entering the user ID and password.
4. The administrator ensures that the specified **Identity Store** is the external RSA SecurID resource.
5. The administrator clicks **Login**.

Figure 4-2 shows an example of the login dialog that is presented to the administrator when RSA SecurID is the external identity store. Upon logging in, the administrator sees only the menu and data access items that are specified in the RBAC policy.

Figure 4-2 Administrator Login—RSA SecurID External Identity Store



Managing Admin Access (RBAC) Policies

In Cisco ISE, RBAC policies are simple access control policies that use RBAC concepts to manage admin access. These RBAC policies are formulated to grant permissions to a set of administrators that belong to one or more admin group(s) that restrict or enable access to perform various administrative functions using the user interface menus and admin group data elements.

RBAC policies determine if an admin user can be granted a specific type of access to a menu item or other identity group data elements. You can grant or deny access to a menu item or identity group data element to an admin user based on the admin group by using effective RBAC policies. When admin users log into the Cisco ISE user interface, they can access menus and data that are based on the policies and permissions defined for the admin groups with which they are associated.

For example, you can prevent a network administrator from viewing the Admin Access operations menu and the policy data elements. This can be achieved by creating a custom RBAC policy for the admin group with which the network administrator is associated.

For more information:

- To understand admin access terminologies, see Understanding Admin Access Terminology, page 4-26
- To manage admin access types and values, see Managing Admin Access Types Using the User Interface, page 4-29
- For detailed procedures for creating RBAC permissions, see Configuring RBAC Permissions, page 4-49.
- For detailed procedures for creating RBAC policies, see Configuring RBAC Policies, page 4-56.

Configuring RBAC Permissions

Cisco ISE provides an out of the box set of permissions that are associated with a set of predefined admin groups. Having pre-defined admin group permissions allow you to set permissions so that a member of any admin group can have full or limited access to the menu items within the administrative interface (known as menu access) and to delegate an admin group to use the data access elements of other admin groups (known as data access). These permissions are reusable entities that can be further used to formulate RBAC policies for various admin groups.

The following permissions are available in Cisco ISE:

- Menu Access—See Configuring Menu Access Permissions, page 4-49 for more information.
- Data Access—See Configuring Data Access Permissions, page 4-53 for more information.

Configuring Menu Access Permissions

In Cisco ISE, the menu access permissions allow you to show or hide the menu items of the Cisco ISE administrative interface to an admin group. This feature lets you create permissions for the admin group so that you can restrict or enable access to an administrator belonging to that group at the menu level. The following topics are covered in this section:

- Viewing Predefined Menu Access Permissions, page 4-50
- Creating Custom Menu Access Permissions, page 4-51
- Updating Menu Access Permissions, page 4-52

- Duplicating Menu Access Permissions, page 4-52
- Deleting Menu Access Permissions, page 4-53

Viewing Predefined Menu Access Permissions

Cisco ISE provides a set of system defined menu access permissions that are already used in the default RBAC policies.

To view the default menu access for an admin group, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Menu Access**.

The Menu Access page appears listing all existing menu access permissions, both default and user-defined.

Table 4-13 lists the default menu access permissions.

Table 4-13 Default Menu Access Permissions

Menu Access Name	RBAC Group	Permissible Set of Menu Items [1]
Super Admin Menu Access	Super Admin	• Operations > All menu items • Policy > All menu items • Administration > All menu items
Policy Admin Menu Access	Policy Admin	• Operations > All menu items • Policy > All menu items • Administration > – Identity Management > All menu items – System > Settings
Helpdesk Admin Menu Access	Helpdesk Admin	• Operations > All menu items
Identity Admin Menu Access	Identity Admin	• Operations > All menu items • Administration > – Identity Management > All menu items
Network Admin Menu Access	Network Device Admin	• Operations > All menu items • Administration > – Network Resources > All menu items
System Admin Menu Access	System Admin	• Operations > Authentications, Alarms, Reports, and Troubleshoot • Administration > – System > All menu items

Table 4-13 Default Menu Access Permissions

Menu Access Name	RBAC Group	Permissible Set of Menu Items [1]
RBAC Admin Menu Access	RBAC Admin	• Operations > All menu items • Administration > – Admin Access > All menu items
MnT Admin Menu Access	MnT Admin	• Operations > All menu items

1. **For Super Admin User, all the menu items are available. For other Admin Users, all the Menu Items in this column are available for Standalone deployment and Primary Node in Distributed Deployment. For Secondary Node in Distributed Deployment, the Menu Items under the Administration tab are not available.**

Creating Custom Menu Access Permissions

This section describes how you create custom menu access permissions.

To add a menu access permissions for an admin group, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Menu Access**.

The Menu Access page appears listing all existing menu access permissions, both default and user-defined.

Step 3 Click **Add** and enter the following field values on the Create Menu Access Permission page:

- Name—Enter the name of the menu access permissions.
- Description—Enter a brief description of the menu access permissions.

Step 4 Go to the Menu Access Privileges section, which contains two sections:

- Cisco ISE Navigation Structure displays a list of selectable menu items in a tree structure starting from top-level menu items, such as Operations, Policy, and Administration.
- Permission For Menu Access contains two radio buttons:
  - Show—Shows the selected menu items to the member of the admin group upon login to the Cisco ISE user interface.
  - Hide—Hides the selected menu items.

By default, all menu items are shown with **Hide** status.

Step 5 To create menu access permissions for a menu item, complete the following steps:

a. Click to expand the menu item up to the desired level, and click the menu item(s) on which you want to create permissions.

b. In the Permission area, click **Show**.

Step 6 Click **Save**.

Updating Menu Access Permissions

You can edit only the custom menu access permissions and not the predefined menu access permissions.

To edit menu access permissions for an admin group, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Menu Access**.

The Menu Access page appears listing all existing menu access permissions, both default and user-defined.

Step 3 Check the check box next to the menu access permissions that you want to delete and click **Edit**.

The Edit Menu Access Permission page appears.

Step 4 Modify the following field values:

- Name
- Description

Step 5 Do the following to add or remove menu items from the existing permissions:

- To add a new menu item to the permissions, select the menu items from the Menu Access Privileges section and click the **Show** radio button.
- To remove an existing menu item from the permissions, select the menu items from the Menu Access Privileges section and click the **Hide** radio button.

Step 6 Click **Save** to save the menu access permissions.

Duplicating Menu Access Permissions

Duplicating menu access permissions is a process that reuses the same set of menu items that were used by the original menu access.

To add a duplicate menu access permissions for an admin group, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Menu Access**.

The Menu Access page appears listing all existing menu access permissions, both default and user-defined.

Step 3 Check the check box next to the menu access permissions that you want to duplicate and click **Duplicate**.

New menu access permissions are added to the list with the word "_copy" affixed to the name of the selected permissions. For example, if you want to create a duplicate of *MnT Admin Menu Access*, the duplicate is created with the name of *MnT Admin Menu Access_copy*.

Step 4 Modify the duplicate permissions as necessary.

Step 5 Click **Save** to save the duplicate menu access permissions.

Deleting Menu Access Permissions

You can delete only the custom menu access permissions and not the predefined menu access permissions.

To delete a menu access permissions for an admin group, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Menu Access**.

The Menu Access page appears listing all existing menu access permissions, both default and user-defined.

Step 3 Check the check box next to the menu access permissions that you want to delete and click **Delete**.

Step 4 Click **OK** in the confirmation dialog box to confirm that you want to delete the menu access permissions.

Configuring Data Access Permissions

In Cisco ISE, the data access permissions enable multiple administrators to have the data access permissions within the same user population. You can enable or restrict the use of data access permissions to one or more admin groups. This process allows autonomous delegated control to administrators of one admin group to reuse data access permissions of the chosen admin groups through selective association. Data access permissions range from full access to no access for viewing selected admin groups or the network device groups.The following topics are covered in this section:

- Viewing Predefined Data Access Permissions, page 4-53
- Creating Custom Data Access Permissions, page 4-54
- Updating Data Access Permissions, page 4-55
- Duplicating Data Access Permissions, page 4-55
- Deleting Data Access Permissions, page 4-56

Viewing Predefined Data Access Permissions

To view data access permissions, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Data Access**.

The Data Access page appears listing all existing data access permissions, both default and user-defined.

Table 4-14 lists the default data access permissions.

Table 4-14 Default Data Access Permissions

Data Access Name	RBAC Group	Permissible Admin Groups	Permissible Network Device Groups
Super Admin Data Access	Super Admin	• Admin Groups • User Identity Groups • Endpoint Identity Groups	• All Locations • All Device Types
Policy Admin Data Access	Policy Admin	• User Identity Groups • Endpoint Identity Groups	None
Identity Admin Data Access	Identity Admin	• User Identity Groups • Endpoint Identity Groups	None
Network Admin Data Access	Network Device Admin	None	• All Locations • All Device Types
System Admin Data Access	System Admin	• Admin Groups	None
RBAC Admin Data Access	RBAC Admin	• Admin Groups	None

Creating Custom Data Access Permissions

This section describes how you create custom data access permissions.

To create custom data access permissions, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Data Access**.

The Data Access page appears listing all existing data access permissions, both default and user-defined.

Step 3 Click **Add** and then enter the name of the data access permissions.

The Create Data Access Permission page appears.

Step 4 Enter a brief description of the data access permissions, then go to the Data Access Privileges area, which contains the following two sections:

- Hierarchy list that contains admin groups, user identity groups, and endpoint identity groups.
- Permission for data access, such as Full Access and No Access. By default, all groups are shown in No Access mode.

Step 5 To create a data access permissions that provide full access to an admin group, do the following:

a. Click to expand the admin group and select the desired admin group.

b. Click **Full Access**.

Step 6 Click **Save**.

This creates the required data access permissions.

Updating Data Access Permissions

You can edit only the custom data access permissions and not the predefined data access permissions.

To update a data access permissions, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Data Access**.

The Data Access page appears listing all existing data access permissions, both default and user-defined.

Step 3 Click **Edit** and modify the following values on the Edit Data Access Permission page:

- Name
- Description

Step 4 Complete the following steps to add or remove admin groups from the existing permissions:

- To add a new admin group to the permissions, select the group from the Admin Group Hierarchy and click the **Full Access** radio button.
- To remove an existing admin group from the permissions, select the admin group from the Admin Group and click **No Access**.

Step 5 Click **Save** to save the data access permissions.

Duplicating Data Access Permissions

Duplicating data access permissions is a process that reuses the same set of admin groups as the original data access is having.

To add a duplicate data access permissions for an admin group, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Data Access**.

The Data Access page appears listing all existing data access permissions, both default and user-defined.

Step 3 Check the check box next to the data access permissions that you want to duplicate and click **Duplicate**.

New data access permissions are added to the list with the word "_copy" affixed to the name of the selected permission. For example, if you want to create a duplicate of *Policy Admin Data Access*, the duplicate will be created with the name *Policy Admin Data Access_copy*.

Step 4 Modify the duplicate permissions as necessary.

Step 5 Click **Save** to save the duplicate data access permissions.

Deleting Data Access Permissions

You can delete only the custom data access permissions and not the predefined data access permissions.

To delete a data access permissions for an admin group, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Permissions**.

Step 2 From the Admin Access navigation pane, click to expand **Permissions** and click **Data Access**.

The Data Access page appears listing all existing data access permissions, both default and user-defined.

Step 3 Check the check box next to the data access permissions that you want to delete and click **Delete**.

Step 4 Click **OK** in the confirmation dialog box to confirm that you want to delete the data access permissions.

Configuring RBAC Policies

In Cisco ISE, an RBAC policy is represented in an *if-then* format, where *if* is the RBAC Admin Group value and *then* is the RBAC Permissions value.

From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**, which displays all default RBAC policies. These default policies cannot be modified or deleted. This page also provides the interfaces to create custom RBAC policies for an admin group.

The following topics provide procedures for performing these tasks:

- Using Predefined RBAC Policies, page 4-56
- Creating Custom RBAC Policy, page 4-57
- Updating RBAC Policy, page 4-59
- Duplicating RBAC Policy, page 4-59
- Deleting RBAC Policy, page 4-60

Using Predefined RBAC Policies

Cisco ISE provides a set of system-defined RBAC policies to perform various Cisco ISE administrative functions. You can use these policies as is unless you plan for more granular access policies.

To create a custom RBAC policy, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.

The RBAC Policies page appears. This page contains a set of ready-to-use predefined policies for default admin groups.

Table 4-15 lists the predefined policies, the associated admin groups, and the permissions.

Table 4-15 Predefined RBAC Policies

Policy Name	RBAC Group[1]	Permissions (Menu Access and/or Data Access)[2]
Helpdesk Admin Policy	Helpdesk Admin	• Helpdesk Admin Menu Access
Identity Admin Policy	Identity Admin	• Identity Admin Menu Access • Identity Admin Data Access
MnT Admin Policy	MnT Admin	• MnT Admin Menu Access
Network Device Policy	Network Device Admin	• Network Device Menu Access • Network Device Data Access
Policy Admin Policy	Policy Admin	• Policy Admin Menu Access • Policy Admin Data Access
RBAC Admin Policy	RBAC Admin	• RBAC Admin Menu Access • RBAC Admin Data Access
Super Admin Policy	Super Admin	• Super Admin Menu Access • Super Admin Data Access
System Admin Policy	System Admin	• System Admin Menu Access • System Admin Data Access

1. See Understanding Admin Access Terminology, page 4-26, for more information on the default admin groups.
2. See Table 4-13 for the list of predefined menu access permissions and Table 4-14 for the list of predefined data access permissions.

Creating Custom RBAC Policy

Besides the default policies, you can create as many custom RBAC policies that you can then apply to personalized admin groups designed specifically for your work place.

Prerequisites:

- Ensure that you have created all admin groups for which you want to define the RBAC policies. See Configuring Admin Groups, page 4-37, for more information on how to create admin groups.
- Ensure that these admin groups are mapped to the individual admin users. See Configuring Cisco ISE Administrators, page 4-33, for more information on how to create admin users.
- Ensure that you have configured the RBAC permissions, such as menu access and data access permissions. See Configuring RBAC Permissions, page 4-49, for more information on how to create RBAC permissions.

To create a custom RBAC policy, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.

The RBAC Policies page appears. This page contains a set of ready-to-use predefined policies for default admin groups.

Step 2 Click the drop-down arrow for the **Action** icon next to a policy.

A drop-down list is displayed with the policy-based choices.

Table 4-16 lists the RBAC policy object selector options.

Table 4-16 RBAC Policy Object Selector Options

Action Name	Result
Duplicate	Adds a copy of the selected policy on the PBAC policies page, along with the word copy in the RBAC policy name. Save the policy with an appropriate name.
Insert New Policy.	Adds a new policy row.
Delete	Deletes the selected policy. This option is disabled for default policies.

Step 3 Click the appropriate action from the drop-down menu.

RBAC policies appear in an alphabetical order according to their rule names after you save the RBAC policy on the RBAC Policies page.

Step 4 Enter values for the following RBAC policy fields:

- Rule Name—Enter a name for the new policy.
- RBAC Group(s)—Choose a name for the RBAC group that is associated with the policy.
  - Click the plus sign (+) next to RBAC Groups to display a drop-down list of group choices. This list shows all existing RBAC groups, including the default groups and user-defined internal and external groups.
  - Click the plus sign (+) next to RBAC Groups to add multiple RBAC groups.
- Permissions—Choose the permissions, which include menu access and data access permissions.

  To add permissions:
  - Click the plus sign (+) next to Permissions to enter the menu access permissions name.
  - Click the button next to Enter Menu Access Permission to display a drop-down list of menu access permission choices.
  - Click the necessary Menu Access Permission in the list to add it to the policy.
  - Click the plus sign (+) next to the selected Menu Access Permission name to add data access permissions.
  - Select the button next to Enter Data Access Permission to display a drop-down list of data access permission choices.
  - Click the necessary Data Access Permission in the list to add it to the policy.

Note You cannot select multiple menu access and data access permissions when creating an RBAC policy.

- Click **Submit**.

RBAC policy creation is now complete.

Updating RBAC Policy

In Cisco ISE Administration dashboard, there is no specific button or control available to edit a policy. You can update only the custom RBAC policies and not the default RBAC policies. You can update all or any RBAC Policy fields by modifying the field values that you want to change.

To edit a custom RBAC policy, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.

The RBAC Policies page appears.

Step 2 Modify the values of following fields, as necessary:

- Rule Name
- RBAC Group
- Permissions
  - Menu Access Permission
  - Data Access Permission

Step 3 Click **Save** to save the modified RBAC Policy.

Duplicating RBAC Policy

Use this procedure to add a duplicate RBAC policy.

To duplicate a policy, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.

The RBAC Policies page appears.

Step 2 Click the drop-down arrow for the **Action** icon next to the policy that you want to duplicate.

Step 3 Select **Duplicate**.

A duplicate policy row is added in the desired location with the word "_copy" affixed to the selected policy name.

Step 4 Modify values of the policy fields, as necessary.

Step 5 Click **Save** to save the duplicate policy.

Deleting RBAC Policy

You can delete only the custom RBAC policies and not the default RBAC policies.

To delete a policy, complete the following steps:

Step 1 From the Cisco ISE Administration dashboard, choose **Administration > System > Admin Access > Authorization > Policy**.

The RBAC Policies page appears.

Step 2 Click the drop-down arrow for the **Action** icon next to the policy of which you want to delete.

Step 3 Click **Delete**.

Step 4 Click **Save** to delete the policy from the Cisco ISE database.

Configuring Settings for Accounts

This section describes how to configure general settings for different Cisco ISE accounts and covers the following topics:

- Administrator Access Settings, page 4-60
- Configuring Network Access for User Accounts, page 4-65

Administrator Access Settings

Cisco ISE allows you to define some rules for administrator accounts to enhance security. You can restrict access to the management interfaces, force administrators to use strong passwords, regularly change their passwords, and so on. The password policy that you define under the Administrator Account Settings in Cisco ISE applies to all administrator accounts.

Note For passwords with UTF-8 characters, it is important to uncheck the following password policy options: Lowercase alphabetic characters, Uppercase alphabetic characters.

This section describes how to define rules for administrator accounts:

- Restricting Administrative Access to the Management Interfaces, page 4-61
- Configuring a Password Policy for Administrator Accounts, page 4-62
- Configuring Session Timeout for Administrators, page 4-64

For more information:

Refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1* for a list of ports that must be open for specific services.

The username and password that you configure using Setup is intended only for administrative access to the Cisco ISE command-line interface (CLI), and this role is considered to be the CLI-admin user. By default, the username for the CLI-admin user is “admin” and the password is user-defined during Setup (there is no default password).

As the CLI-admin user, you can start and stop the Cisco ISE application, apply software patches and upgrades, reload or shut down the Cisco ISE appliance, and view all system and application logs. Because of the special privileges of the CLI-admin user, we recommend that you protect the CLI-admin user credentials and create web-based admin users for configuring and managing your Cisco ISE deployment.

For more information:

- For information about web-based admin users, see the "Configuring Cisco ISE Administrators" section on page 4-33.
- For details about the differences between the CLI-admin users and web-based admin users, refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

Restricting Administrative Access to the Management Interfaces

Cisco ISE allows you to restrict administrative access to the management interfaces based on the IP address of the remote client. You can choose to do one of the following:

- Allow all IP addresses to connect
- Allow only listed IP addresses to connect

If you choose the Allow only listed IP addresses to connect option, you must add a list of IP addresses.

Note The administrator access control settings are only applicable for Cisco ISE nodes that assume the Administration, Policy Service, or Monitoring personas. These restrictions are replicated from the primary to the secondary nodes. These restrictions are not applicable for the Cisco ISE nodes that assume the Inline Posture node type.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or System Admin. See Table 4-11 for more information on the various administrative roles and the privileges associated with each of them.

To add a range of IP addresses to the IP List area, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Settings > Access**.

The Configure Access Restriction page appears.

Step 2 Do one of the following:

- Click the **Allow all IP addresses to connect** radio button and proceed to Step 4.
- Click the **Allow only listed IP addresses to connect** radio button, and complete the following steps:

a. From the Configure IP List for Access Restriction area, click **Add**.

The Add IP CIDR page appears.

b. Enter IP addresses in the classless interdomain routing (CIDR) format in the IP address field.

Enter the subnet mask in the Netmask in CIDR format field.

c. Click **OK** to add the range of IP addresses to the IP List area.

d. Repeat the process to add more IP address ranges to this list.

Administrative access to Cisco ISE will now be restricted to the IP address ranges that are specified in this list after you click the Submit button.

Step 3 Click **Submit** to save the changes.

Related Topics

- Configuring Cisco ISE Administrators, page 4-33
- Configuring Admin Groups, page 4-37

Configuring a Password Policy for Administrator Accounts

You can create a password policy for administrator accounts to enhance security. The policy that you define here is applied to all administrator accounts in Cisco ISE.

Note For passwords with UTF-8 characters, it is important to uncheck the following password policy options: Lowercase alphabetic characters, Uppercase alphabetic characters.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: RBAC Admin, Super Admin, or System Admin. See Table 4-11 for more information on the various administrative roles and the privileges that are associated with each of them.

Specifying Password-Based or Client Certificate-Based Authentication

To enable either password-based or client certificate-based administrator authentication:

Step 1 Navigate to **Administration > System > Admin Access > Authentication**.

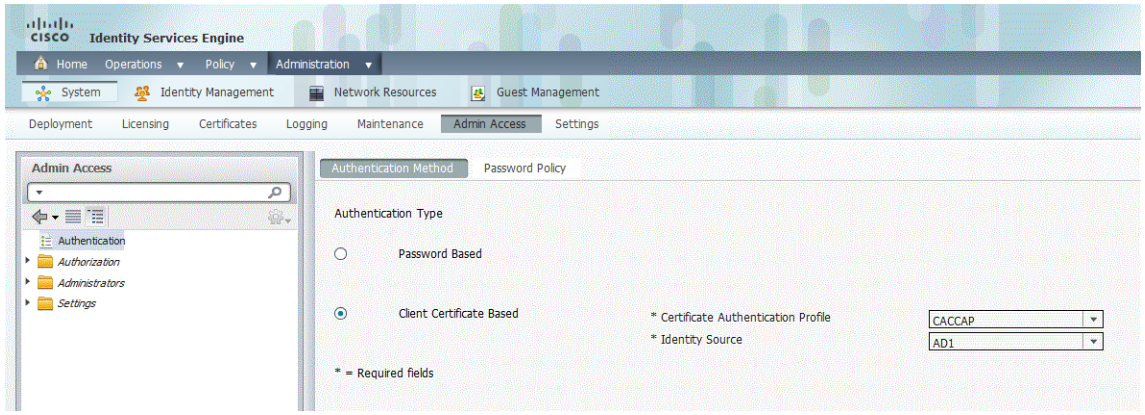
Step 2 On the Authentication Method tab, select either the **Password Based** or the **Client Certificate Based** option.

- If you want to use standard user ID and password credentials for administrator login, choose the **Password Based** option and specify either the “Internal” or “External” authentication type. The default setting is “Internal.”

Note If you have configured an external identity source such as LDAP and want to use that as your authentication source to grant access to the admin user, you must select that particular identity source from the Identity Source list box.

- If you want to specify a certificate-based policy, choose the **Client Certificate Based** option, and select an existing Certificate Authentication Profile.

Figure 4-3 Administrator > System > Admin Access > Authentication > Authentication Method



Specifying the Administrator Password Policy

To create the password policy for administrators, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Authentication**.

Step 2 Click the **Password Policy** tab.

Step 3 In the Password Policy tab, enter the following information:

Note For passwords with UTF-8 characters, it is important to uncheck the following password policy options: Lowercase alphabetic characters, Uppercase alphabetic characters.

- Minimum Length—(Required) Specifies the minimum length of the password (in characters). The default is six characters.
- Password may not contain the admin name or its characters in reversed order—Check this check box to restrict the use of the administrator username or its characters in reverse order.
- Password may not contain ‘cisco’ or its characters in reversed order—Check this check box to restrict the use of the word “cisco” or its characters in reverse order.
- Password may not contain *variable* or its characters in reversed order—Check this check box to restrict the use of any word that you define or these characters in reverse order.
- Password may not contain repeated characters four or more times consecutively—Check this check box to restrict the use of repeated characters four or more times consecutively.
- Password must contain at least one character of each of the selected types—Specifies that the administrator password must contain at least one character of the type that you choose from the following choices:
  - Lowercase alphabetic characters
  - Uppercase alphabetic characters
  - Numeric characters
  - Non-alphanumeric characters

- Password History—Specifies the number of previous passwords from which the new password must be different to prevent the repeated use of the same password.
- Password Lifetime—Specifies the following options to force users to change passwords after a specified time period:
  - Time (in days) before the administrator account is disabled if the password is not changed. (The allowable range is 0 to 2,147,483,647 days.)
  - Reminder (in days) before the administrator account is disabled.
- Incorrect Password Attempts—Specifies the number of times Cisco ISE records incorrect administrator passwords before locking the administrator out of Cisco ISE and disabling account credentials:
  - The number of failed attempts Cisco ISE logs before the administrator account is disabled based on incorrect password entry. (The minimum and default number of attempts is 5, and the maximum number of allowed attempts is 20.)
  - Text that is displayed notifying the user of the administrator account deactivation.

Note If you are using external identity stores to authenticate administrators at login, remember that even if this setting is configured for the password policy applied to the administrator profile, the external identity store will still validate the administrator's username and password. For information on administrator login via external identity stores, see Configuring Cisco ISE for Administrator Access Using an External Identity Store, page 4-44.

Step 4 Click **Save** to save the administrator password policy.

Related Topics

- Configuring Cisco ISE Administrators, page 4-33
- Configuring Admin Groups, page 4-37
- Configuring Cisco ISE for Administrator Access Using an External Identity Store, page 4-44

Configuring Session Timeout for Administrators

Cisco ISE allows you to determine the length of time an administration GUI session can be inactive and still remain connected. You can specify a time in minutes after which Cisco ISE logs out the administrator. After a session timeout, the administrator must log in again to access the Cisco ISE administrative user interface.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or System Admin. See Table 4-11 for more information on the various administrative roles and the privileges associated with each of them.

To configure session timeout, complete the following steps:

Step 1 Choose **Administration > System > Admin Access > Settings > Session Timeout**.

The Session Timeout page appears.

Step 2 Enter the amount of time in minutes that you want Cisco ISE to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.

Step 3 Click **Save** to save the administrator session timeout settings.

Related Topics

- Configuring Cisco ISE Administrators, page 4-33
- Configuring Admin Groups, page 4-37

Changing Administrator Name

Cisco ISE allows the name of the internal administrator account to be changed to help prevent security breaches of the system. Since ISE supports role-based access control, this is applicable not only to the default Cisco ISE Administrator but to all the internal administrators.

All administrators can change their own name in two ways:

- From the respective Edit screens, based on their privilege level
- From the *logged in user's* link that is available on the left of the **Logout** button. This link appears in the logged in user's name. For example, if you have logged in as *Smith*, the link is displayed as *Smith*. Figure 4-4 shows *admin* as the logged in user.

Figure 4-4 Logged in User Link



When administrators edit their own name, they are redirected to the login screen. A Super admin can change the name of all other admin roles, including system/default administrators.

The administrator name can be changed in the following ways:

- A Super/System/RBAC admin can change the administrator name from the **Administration > System > Admin Access > Administrators > Local Administrators > Edit** screen or from the *logged in user's* link.
- An Identity or Policy admin can change the administrator name from the *logged in user's* link only.
- A network access user who is promoted to Identity or Policy admin can change the administrator name from the **Administration > Identity Management > Identities > Users > Edit** screen or from the *logged in user's* link.

Configuring Network Access for User Accounts

Cisco ISE allows you to restrict network access for user accounts that are based on authentication settings that you configure for attributes and passwords associated with the user accounts. When defining user accounts, you can manage network access in the following ways:

- Use pre-defined system attributes or create custom attributes
- Define authentication settings that form a password policy

There are two options for configuring network access for user accounts:

- User Custom Attributes Policy, page 4-66
- User Password Policy, page 4-66

For information about configuring network access user accounts, see Configuring Network Access User Accounts, page 4-67.

User Custom Attributes Policy

When you choose User Custom Attributes Policy, the page displays two panes with the following options that you can use to define user account attributes:

- Pre-defined Attributes
- Custom Attributes

The Cisco ISE provides the following predefined and nonconfigurable attributes that help define a user account:

- CredentialPassword—A string defining the credential password
- OlderGenerationPasswordList—A string list defining previous account passwords
- Description—A string representing the account password
- isSystemData—An integer representing system data for the account
- DatePasswordLastUpdatedOn—A string defining the last date the account password was updated
- EmailAddress—A string defining the email address for the account
- EnableFlag—A string defining the account as enabled
- isAdmin—A string defining whether the account role is an admin or user
- AllowPasswordChangeAfterLogin—A string that defines a password change after logging in

The Cisco ISE also allows you to define custom attributes to help further define a user account by configuring the following:

- Attribute Name—Enter a name for the custom attribute you create
- Data Type—Choose one of the following from a drop-down list for the custom attribute:
  - String
  - Integer
  - Enum
  - Float
  - Password

User Password Policy

If you choose User Password Policy, the page displays the following two tabs where you can set options:

- Password Policy
- Advanced

When you select the Password Policy tab, the Cisco ISE provides the following configurable options that you set by entering values in text boxes or selecting check boxes. Your choice of values creates a password policy for managing network access per user account:

- ***Minimum Length**—Sets minimum length of password (in characters)
- Username—Restricts the use of the username or its characters in reversed order

- Cisco—Restricts the use of “cisco” or its characters in reverse order
- Special characters—Restricts the use of special characters that you define in reverse order
- Repeated characters—Restricts the use of characters repeated four or more times consecutively
- Required characters—Requires that the password include at least one of each of the following types:
  - Lowercase alphabetic characters
  - Uppercase alphabetic characters
  - Numeric characters
  - Non-alphanumeric characters

Note Options marked by an asterisk (*) are required settings that must have a value configured.

When you select the Advanced tab, Cisco ISE provides the following configurable options that you set by entering values in text boxes or selecting check boxes. Your choice of values creates an “advanced” password policy setting for managing network access per user account.

- **Password History**—Sets the number of previous versions from which the password must be different to prevent the repeated use of the same password.
- **Password Lifetime**—Sets the following options to force users to change passwords after a specified time period:
  - **Time** (in days) before the user account is disabled if the password is not changed
  - **Reminder** (in days) before the user account is disabled

Configuring Network Access User Accounts

The following topics describe how to configure or manage a network access user account:

- Configuring a User Password Policy for the Network Access User Account, page 4-67
- Filtering the Predefined Attributes, page 4-68
- Configuring Custom Attributes for the Network Access User Account, page 4-69

Configuring a User Password Policy for the Network Access User Account

Use this procedure to configure a password policy for any network access user account.

To configure a user password policy for a network access user account, complete the following steps:

Step 1 Choose **Administration > Identity Management > Settings > User Password Policy**.

The Password Policy page appears.

Step 2 Click the **Password Policy** tab and configure the password policy for the user account by entering the desired values in the text boxes or selecting specific check boxes.

Note For more information about the values and corresponding text boxes and check boxes, see User Password Policy, page 4-66.

For example, to create a password policy that requires a strong password, enter the following values or check the following check boxes:

- Enter 10 or greater in the **Minimum Length:** text box.
- Check the **Password may not contain repeated characters four or more times consecutively** check box.
- Under **Password must contain at least one character of each of the following types**, check the following check boxes:
  - Lowercase alphabetic characters
  - Uppercase alphabetic characters
  - Numeric characters
  - Non-alphanumeric characters

Step 3 The **Password may not contain the username or its characters in reversed order** check box is checked by default. You may uncheck it if you require.

Step 4 Click the **Advanced** tab and configure the advanced password settings by entering values or selecting check boxes to define the Password History and Password Lifetime.

For example, to define unique passwords, enter the following values or check the following check boxes:

- Under Password History, enter 5 or greater in the **Password must be different from the previous versions** text box.
- Under Password Lifetime, check the following check boxes:
  - **Disable user account after__ days if password was not changed**, and enter **30** in the text box (to represent 30 days).
  - **Display reminder after __ days**, and enter **15** in the text box (to represent 15 days).

Step 5 After you make your selections, click **Save** to save this user password policy locally.

Filtering the Predefined Attributes

Predefined attributes are system-configured and cannot be modified. However, you can filter the list of predefined attributes and search for specific attributes. Use this procedure to filter and search for specific attributes of interest.

To search for specific predefined attributes, complete the following steps:

Step 1 Choose **Administration > Identity Management > Settings > User Custom Attributes**.

The Pre-defined Attributes page appears with a list of all predefined attributes.

Step 2 Click **Filter** and choose one of the following options:

- Quick Filter
- Advanced Filter

a. To perform a Quick Filter, enter search criteria in one of the following attribute fields:

- Required
- Attribute Name
- Data Type

- Parameter

Note By default, all four search fields are displayed. To customize your search to one or more fields, click **Action** and choose **Columns**. Unmark any of the selected search fields that you do not wish to use in a search.

b. To perform an Advanced Filter, create a matching rule by choosing one of the following options in the **Filter** drop-down list:
   - Attribute Name
   - Data Type
   - Parameters
   - Required

c. In the second drop-down list, choose one of the following options:
   - Contains
   - Does not contain
   - Does not equal
   - Ends with
   - Is empty
   - Is exactly (or equals)
   - Is not empty
   - Starts with

d. In the text box, enter your desired search value.

e. Click **Go** to launch the filter process, or click plus (**+**) to add additional search criteria.

f. Click **Clear Filter** to reset the filter process.

Configuring Custom Attributes for the Network Access User Account

The Pre-defined Attributes page allows you to configure custom attributes as part of the authentication settings for the network access user account. The network access user account already contains a set of predefined attributes. You can configure custom attributes using the following process.

To configure custom attributes for a network access user account, complete the following steps:

Step 1 Choose **Administration > Identity Management > Settings > User Custom Attributes**.

The Pre-defined Attributes page appears

Step 2 In the Custom Attributes pane, do the following:

- Enter the name for the custom attribute in the **Attribute Name** text box.
- In the Data Type drop-down list, choose the data type from the these choices:
  - String
  - Integer

  - Enum
  - Float
  - Password
- To add parameters, click plus (+) under Parameters and add the desired attribute names and data types.

Step 3 After making your selections, click **Save** to save these user custom attributes locally.

Endpoint Identity Groups

An endpoint identity group is used to group all the identified endpoints on your network according to their profiles. Cisco ISE creates the following three identity groups in the system: Blacklist, Profiled, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group.

You can create an endpoint identity group and associate the group to one of the system-created identity groups. You can also assign an endpoint that you create directly (statically) to any one of the identity group that exists in the system, and the profiling service cannot reassign the identity group.

In addition, you can map an endpoint profile where you match the endpoint profile with an existing profile and group it to a matching identity group. If you have an endpoint profile that matches an existing profile, then the profiling service can create a matching identity group.

This identity group becomes the child of the Profiled identity group. When you create an endpoint profiling policy, you can check the Create matching identity group check box in the Endpoint Policies page to create a matching identity group. You cannot delete the matching identity group unless the mapping of the profile is removed.

When an endpoint is mapped to an existing profile, the profiling service searches the hierarchy of profiles for the closest parent profile that has a matching group of profiles and assigns the endpoint to the appropriate profile.

Parent Group

By default, a Cisco ISE deployment creates the following three endpoint identity groups: Blacklist, Profiled, and Unknown. A parent group is the default identity group that exists in the system. The profiling service includes the following endpoint identity groups:

- Blacklist—This endpoint identity group includes endpoints that are statically assigned to endpoints identities in Cisco ISE and grouped within the Blacklist identity group. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.
- Profiled—This endpoint identity group includes endpoints that are profiled by Cisco ISE and grouped within the Profiled endpoint identity group.
- Unknown—Endpoints that do not match any profile are grouped within the Unknown endpoint identity group.

In addition, the profiling service includes the following endpoint identity groups, which are associated to the Profiled identity group:

- Cisco-IP-Phone—An identity group that contains all the profiled Cisco IP phones on your network.

Note An authorization rule for all types of Cisco IP Phones is available in Cisco ISE in the following location: **Policy > Authorization > Standard**.

- Workstation—An identity group that contains all the profiled workstations on your network.

Using Endpoint Identity Groups in Authorization Policies

The profiling service discovers endpoints and classifies them now into their corresponding endpoint profiling policies based on the attributes that are collected and existing endpoint profiling policies in Cisco ISE. The Cisco ISE application moves these discovered endpoints to the corresponding endpoint identity groups based on the endpoint profiling policies.

The endpoint identity groups can be effectively used in the authorization policies to provide appropriate network access privileges to the discovered endpoints. To use the endpoint identity groups more effectively in the authorization policies, you need to ensure that the endpoint profiling policies are either standalone policies (no parent to the policies), or their parent policies of the endpoint profiling policies are disabled.

This section includes the following topic, which describe the procedures for managing endpoint identity groups:

- Filtering, Creating, Editing, and Deleting Endpoint Identity Groups, page 4-71

Note For more information on endpoint profiling in Cisco ISE networks, see Chapter 18, “Configuring Endpoint Profiling Policies”.

Filtering, Creating, Editing, and Deleting Endpoint Identity Groups

The Endpoint Identity Groups page allows you to manage endpoint identity groups, and provides an option to filter the groups by their group names and description.This section describes the basic operations that allow you to group all the identified endpoints on your network and manage the identity groups.

The procedures for managing endpoint identity groups include the following tasks:

- Filtering Endpoint Identity Groups, page 4-71
- Creating, Editing, and Deleting an Endpoint Identity Group, page 4-73

Filtering Endpoint Identity Groups

You can use the Show drop-down list or the filter icon to both invoke a quick filter and close it on the Endpoint Identity Groups page. A quick filter is a simple filter that you can use to filter identity groups on the Endpoint Identity Groups page. The quick filter filters identity groups based on field descriptions, such as the name of the identity group and the description on the Endpoint Identity Groups page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use and retrieve later, along with the filtering results, on the Endpoint Identity Groups page. The advanced filter filters based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option, which lists all the preset filters. This option allows you to manage preset filters. Once you have created and saved a preset filter, you can choose a preset filter from the list of filtered results on the Endpoint Identity Groups page.You can also edit preset filters and remove them from the preset filters list.

To filter identity groups on the Endpoint Identity Groups page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups**.

The Groups menu window appears.

Step 2 From the Groups menu window, choose **Endpoint Identity Groups** (menu).

The Endpoint Identity Groups page appears, which lists all the identity groups.

Step 3 From the Endpoint Identity Groups page, click the Show drop-down arrow to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 4-17.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 4-72 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 4-72.

Note To return to the endpoint identity groups list, choose **All** from the Show drop-down list to display all the endpoint identity groups without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters identity groups based on each field description on the Endpoint Identity Groups page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the result on the Endpoint Identity Groups page. If you clear the field, it displays the list of all the endpoint identity groups on the Endpoint Identity Groups page.

Step 1 To filter, click the **Go** button within each field to refresh the page with the results that are displayed on the Endpoint Identity Groups page.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter identity groups by using variables that are more complex. It contains one or more filters that filter identity groups based on the values that match the field descriptions. A filter on a single row filters identity groups based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter identity groups by using any one or all of the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove a filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save Preset Filter dialog appears. Enter a file name to save the filter and click **Save**. Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Note Any preset filter that you create and save is browser-based only and is only accessible using the same browser type (preset filters are not saved in the Cisco ISE database). For example, any preset filter you create and save using a Firefox version 3.6.x browser will not be accessible by a Microsoft Internet Explorer (IE8) browser (or vice versa).

Table 4-17 describes the fields on the Endpoint Identity Groups page that allow you to filter the endpoint identity groups.

Table 4-17 Filtering Endpoint Identity Groups

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter identity groups by the name of the endpoint identity group.
	Description	This field enables you to filter identity groups by the description of the endpoint identity group.
Advanced Filter	Choose the field description from the following: • Name • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter identity groups.
	Value	From the Value field, choose the value for the field description that you selected against which the endpoint identity groups are filtered.

Creating, Editing, and Deleting an Endpoint Identity Group

You can create, edit, or delete an endpoint identity group on the Endpoint Identity Groups page.

To create an endpoint identity group on the Endpoint Identity Groups page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**.

The Endpoint Identity Groups page appears, which lists all the identity groups.

Step 2 From the Endpoint Identity Groups page, choose **Create**.

Step 3 Modify the values on the New Endpoint Group page, as shown in Table 4-18.

Step 4 Perform one of the following tasks:

a. Click **Submit** to create the endpoint, which appears on the Endpoint Identity Groups page.

b. Click **Cancel** to terminate the action without creating the endpoint.

Step 5 Click the **Endpoint Group List** link from the New Endpoint Group page to return to the Endpoint Identity Groups page.

Table 4-18 describes the fields on the Endpoint Identity Groups page that allow you to create an endpoint identity group:

Table 4-18 Creating Endpoint Identity Groups

Field Name	Description
Name	In the Name field, enter the name of the endpoint identity group that you want to create. **Note** Use the best practice to include no spaces when creating the name for an endpoint identity group.
Description	In the Description field, enter the description of the endpoint identity group that you want to create.
Parent Group	Cisco ISE creates the following three endpoint identity groups on your deployment: Blacklist, Profiled, and Unknown. From the Parent Group field, choose an endpoint identity group. Click the drop-down arrow to view the endpoint identity groups, which are created on your Cisco ISE deployment.

To edit an endpoint identity group on the Endpoint Identity Groups page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**.

The Endpoint Identity Groups page appears, which lists all the identity groups.

Step 2 From the Endpoint Identity Groups page, choose an identity group, then choose **Edit**.

Note You can only edit the name and description of the identity groups that you create in the system. The name of the endpoint identity groups are not editable but their description are editable that are created by Cisco ISE in the system.

Step 3 Perform one of the following tasks:

a. Click **Reset** to revert to the previous data.

b. Verify if you want to reset the data and lose any current data, or click **Cancel** to continue with the current input data.

c. Click **Save** to save the current input data on the edit page.

Step 4 Click the **Endpoint Group List** to return to the Endpoint Identity Groups page after editing an endpoint identity group.

To delete an endpoint identity group on the Endpoint Identity Groups page, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**.

The Endpoint Identity Groups page appears, which lists all the identity groups.

Step 2 Choose an endpoint identity group from the Endpoint Identity Groups page, then choose **Delete**.

Note You can only delete the identity groups that you create in the system. You cannot delete the endpoint identity groups that are created by Cisco ISE in the system.

Step 3 Click **OK** in the confirmation dialog to delete an endpoint identity group.

Click **Cancel** to return to the Endpoint Identity Groups page without deleting the endpoint identity group.

Related Topics

Adding and Removing Endpoints in an Endpoint Identity Group, page 4-75

Adding and Removing Endpoints in an Endpoint Identity Group

This section describes the basic operations that allow you to manage endpoints in an endpoint identity group. The MAC address is used in all the basic operations.

You can filter, add, or remove statically added endpoints in any endpoint identity group. If an endpoint identity group assignment is not static, then endpoints are reprofiled after adding, or removing from any endpoint identity group. Endpoints that are identified dynamically by the profiler appear in appropriate endpoint identity groups. If you remove dynamically added endpoints from an endpoint identity group, Cisco ISE displays a message that you have successfully removed endpoints from the identity group but reprofiles them back in the endpoint identity group. You can only add endpoints from the Endpoints widget to a specific identity group. If you add an endpoint to the specific endpoint identity group, then the endpoint is moved from the endpoint identity group where it was dynamically grouped earlier. Upon removal from the endpoint identity group where you recently added an endpoint, the endpoint is reprofiled back to the appropriate identity group. Here, you do not delete endpoints from the endpoint identity group but only remove them from the endpoint identity group.

The Endpoint Identity Group page displays the name and description of all the endpoint identity groups. You can use the Edit menu on the Endpoint Identity Groups page to filter, add, or remove endpoints in an endpoint identity group.

The procedure for managing endpoints in the endpoint identity groups include the following tasks:

- Adding Endpoints in an Endpoint Identity Group, page 4-76
- Removing Endpoints in an Endpoint Identity Group, page 4-76

Adding Endpoints in an Endpoint Identity Group

You can add endpoints to an identity group from the Endpoints widget, or remove endpoints from the identity group. You cannot remove an endpoint from the identity group that has a matching profile with an existing profile.

To add endpoints to an endpoint identity group, complete the following steps:

Step 1 Choose **Administration > Identity Management > Groups > Endpoint Identity Groups**.

The Endpoint Identity Groups page appears, which lists all the identity groups.

Step 2 From the Endpoint Identity Groups page, choose an identity group.

Step 3 From the Endpoint Identity Groups page, choose **Edit**.

Step 4 Click the arrow in front of Endpoints to display or hide the Identity Group Endpoints list, which displays the list of endpoints for the selected endpoint identity group.

Step 5 Click **Add**.

The Endpoints widget appears.

Step 6 Choose an endpoint from the Endpoints widget.

The endpoint appears in the endpoint identity group.

Step 7 Click the **Endpoint Group List** link on the edit page to return to the Endpoint Identity Groups page.

Removing Endpoints in an Endpoint Identity Group

You can remove one or more endpoints in an endpoint identity group. If endpoints are filtered on the Identity Group Endpoints list page, only those filtered endpoints are removed from the endpoint identity group when you are using the Removing All option.

To remove endpoints from an endpoint identity group, complete the following steps:

Step 1 Choose an endpoint from the Identity Group Endpoints list, and choose **Edit**.

Step 2 Click the arrow in front of Endpoints to display or hide the Identity Group Endpoints list, which displays the list of endpoints for the selected endpoint identity group.

Step 3 Choose **Remove**.

Remove Selected and Remove All options appear. You can choose to remove one or more endpoints that you select or remove all the endpoints in an endpoint identity group.

Note Here, you can remove one or more endpoints from the endpoint identity group.

Step 4 Click the **Endpoint Group List** link on the edit page to return to the Endpoint Identity Groups page.



CHAPTER 5

Managing External Identity Sources

The Cisco Identity Services Engine (ISE) integrates with external identity sources to validate credentials in user authentication functions, and to retrieve group information and other attributes that are associated with the user for use in authorization policies. You must configure the external identity source that contains your user information in ISE. External identity sources also include certificate information for the ISE server and certificate authentication profiles.

Both internal and external identity sources can be used as the authentication source for sponsor authentication and also for authentication of remote guest users.

Table 5-1 lists the identity sources and the protocols that they support.

Table 5-1 Protocol Versus Database Support

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP[1]	RADIUS Token Server or RSA
EAP-GTC[2], PAP[3] (plain text password)	Yes	Yes	Yes	Yes
MS-CHAP[4] password hash: MSCHAPv1/v2[5] EAP-MSCHAPv2[6] LEAP[7]	Yes	Yes	No	No
EAP-MD5[8] CHAP[9]	Yes	No	No	No
EAP-TLS[10] PEAP-TLS[11] (certificate retrieval) **Note** For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required, but are optional and can be added for authorization policy conditions.	No	Yes	Yes	No

1. LDAP = Lightweight Directory Access Protocol.
2. EAP-GTC = Extensible Authentication Protocol-Generic Token Card
3. PAP = Password Authentication Protocol
4. MS-CHAP = Microsoft Challenge Handshake Authentication Protocol

5. MS-CHAPv1/v2 = Microsoft Challenge Handshake Authentication Protocol Version 1/Version 2
6. EAP-MSCHAPv2 = Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol Version 2
7. LEAP = Lightweight Extensible Authentication Protocol
8. EAP-MD5 = Extensible Authentication Protocol-Message Digest 5
9. CHAP = Challenge-Handshake Authentication Protocol
10. EAP-TLS = Extensible Authentication Protocol-Transport Layer Security
11. PEAP-TLS = Protected Extensible Authentication Protocol-Transport Layer Security

This chapter describes how you can configure the following identity sources and certificate authentication profiles in ISE and contains the following topics:

- Certificate Authentication Profiles, page 5-2
- Microsoft Active Directory, page 5-4
- LDAP, page 5-17
- RADIUS Token Identity Sources, page 5-32
- RSA Identity Sources, page 5-39
- Identity Source Sequences, page 5-51
- Viewing and Monitoring the Identity Sources, page 5-54

Certificate Authentication Profiles

Certificate authentication profiles are used in authentication policies for certificate-based authentications in place of identity sources to verify the authenticity of the user. The certificate authentication profiles allow you to specify the following items:

- The certificate field that should be used as the principal username
- Whether a binary comparison of the certificate should be performed

The Certificate Authentication Profiles page lists the certificate authentication profiles that you have added.

For more information:

Adding or Editing a Certificate Authentication Profile, page 5-2

Adding or Editing a Certificate Authentication Profile

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To add or edit a certificate authentication profile, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Certificate Authentication Profile**.

The Certificate Authentication Profile page appears.

Step 3 Do one of the following:

- To add a new certificate authentication profile, click **Add**.
- To edit an existing certificate authentication profile, choose the profile that you want to edit and click **Edit**.
- To create a duplicate of an existing certificate authentication profile, choose the profile that you want to duplicate and click **Duplicate**.

Step 4 Enter the following details:

- Name—(Required) Enter the name of the certificate authentication profile.
- Description—Enter a description of the certificate authentication profile.
- Principal Username X509 Attribute—The available list of principal username attributes for X.509 certificate includes the following selections:
  - Common Name
  - Subject Alternative Name
  - Subject Serial Number
  - Subject
  - Subject Alternative Name—Other Name
  - Subject Alternative Name—Email
  - Subject Alternative Name—DNS
- Perform Binary Certificate Comparison with Certificate Retrieved from LDAP or Active Directory—Check this check box if you want to validate certificate information for authentication against a selected LDAP or Active Directory identity source.

  If you check this check box, you must choose the LDAP or Active Directory identity source from the available list.
- LDAP/Active Directory Instance Name—Choose the LDAP or Active Directory identity source against which you want to validate the certificate information for authentication.

Step 5 Click **Submit** to add the certificate authentication profile or save the changes.

Next Steps:

1. See Chapter 16, “Managing Authentication Policies” for information on how to create authentication policies.
2. See Chapter 17, “Managing Authorization Policies and Profiles” for information on how to create authorization profiles and policies.

Microsoft Active Directory

ISE uses Active Directory as an external identity source to access resources such as users, machines, groups, and attributes. You can configure ISE to authenticate users and machines. This section contains the following topics:

- Key Features of the Integration of ISE and Active Directory, page 5-4
- Integrating ISE with Active Directory, page 5-6
- Enabling Active Directory Debug Logs, page 5-15
- Supplemental Information, page 5-16

Note ISE does not support Microsoft Active Directory Servers that reside behind a network address translator and have a Network Address Translation (NAT) address.

Key Features of the Integration of ISE and Active Directory

Supported Authentication Protocols

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) and Protected Extensible Authentication Protocol (PEAP)—ISE supports user and machine authentication and change password against Active Directory using EAP-FAST and PEAP with an inner method of Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) and Extensible Authentication Protocol-Generic Token Card (EAP-GTC).
- Password Authentication Protocol (PAP)—ISE supports authenticating against Active Directory using PAP and also allows you to change Active Directory user passwords.
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)—ISE supports user and machine authentication against Active Directory using MS-CHAPv1.
- MS-CHAPv2—ISE supports user and machine authentication against Active Directory using EAP-MSCHAPv2.
- EAP-GTC—ISE supports user and machine authentication against Active Directory using EAP-GTC.
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)—ISE uses the certificate retrieval option to support user and machine authentication against Active Directory using EAP-TLS.
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)—ISE supports user and machine authentication against Active Directory using PEAP-TLS.
- LEAP—ISE supports user authentication against Active Directory using LEAP.

Refer to the *Release Notes for Cisco Identity Services Engine, Release 1.1* for a list of Windows Server Operating Systems that support Active Directory services.

Directory Service

Active Directory is a directory service that allows for central administration and management of user accounts, clients, and servers. Active Directory can interoperate with other directory services such as Lightweight Directory Access Protocol (LDAP) and is mostly used in distributed networking environments.

User Authentication

User authentication provides network access to only those users who are listed in Active Directory.

Machine Authentication

Machine authentication provides access to network services to only those devices that are listed in Active Directory.

Attribute Retrieval for Authorization

You can configure ISE to retrieve user or machine Active Directory attributes to be used in authorization rules. The attributes are mapped to the ISE policy results and determine the authorization level for the user or machine. ISE retrieves user and machine Active Directory attributes after a successful user or machine authentication and can also retrieve the attributes for an authorization that is independent of authentication.

Group Retrieval for Authorization

ISE can retrieve user or machine groups from Active Directory after a successful authentication. ISE can also retrieve the user or machine group that is independent of authentication for authorization. You can use the Active Directory group data for authorization and introduce special conditions to match them against the retrieved groups.

Certificate Retrieval for EAP-TLS Authentication

ISE supports certificate retrieval for user or machine authentication that uses the EAP-TLS protocol. The user or machine record on Active Directory includes a certificate attribute of the binary data type. This certificate attribute can contain one or more certificates. ISE identifies this attribute as userCertificate and does not allow you to configure any other name for this attribute. ISE retrieves this certificate and uses it to verify the identity of the user or machine. The certificate authentication profile determines the field to be used for retrieving the certificates. For example, Subject Alternative Name (SAN), Common Name, or Social Security Number (SSN). After ISE retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, ISE compares the certificates to check for one that matches. When a match is found, ISE grants the user or machine access to the network.

User Access Restriction

While authenticating or querying a user, ISE checks for the following:

- Is the user account disabled?
- Is the user locked out?
- Has the user account expired?
- Is the query run outside of the specified login hours?

If the user has one of these limitations, the *Active Directory Identifier*::IdentityAccessRestricted attribute on the Active Directory dictionary is set to indicate that the user has restricted access. You can use this attribute in all policy rules.

Active Directory identifier is the name that you enter for the Active Directory identity source.

Support for Multidomain Forests

ISE supports multidomain forests. ISE connects to a single domain, but can access resources from the other domains in the Active Directory forest if trust relationships are established between the domain to which ISE is connected and the other domains.

For more information:

- Dictionaries and Dictionary Attributes, page 7-1
- Integrating ISE with Active Directory, page 5-6

Integrating ISE with Active Directory

Prerequisites:

Before you connect your ISE server with the Active Directory domain, you must check the following:

- Ensure that Cisco ISE hostnames are only 15 characters or less in length. Active Directory does not validate hostnames larger than 15 characters, which can cause a problem if you have multiple ISE hosts in your deployment whose hostnames are identical through the first 15 characters and only distinguished from one another by trailing digits or other identifiers.
- Ensure that your ISE server and Active Directory are time synchronized. Time in the ISE is set according to the Network Time Protocol (NTP) server. It is recommended that you use the NTP to synchronize time between the ISE and Active Directory. For more information on NTP server settings, see the "System Time and NTP Server Settings" section on page 8-18.

  Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for information on how to configure the NTP server settings from the CLI.
- If there is a firewall between ISE and Active Directory, certain ports need to be opened to allow ISE to communicate with Active Directory. Ensure that the following default ports are open:

Protocol	Port Number
LDAP	389 (UDP)
SMB[1]	445 (TCP)
KDC[2]	88 (TCP)
Global Catalog	3268 (TCP), 3269
KPASS	464 (TCP)
NTP	123 (UDP)
LDAP	389 (TCP)
LDAPS[3]	636 (TCP)

1. SMB = Server Message Block
2. KDC = Kerberos Key Distribution Center
3. LDAPS = Lightweight Directory Access Protocol over TLS/SSL

- If your Active Directory source has a multidomain forest, ensure that trust relationships exist between the domain to which ISE is connected and the other domains with resources to which you need access. For more information on establishing trust relationships, refer to the *Microsoft Active Directory documentation*.

- The DNS server that is configured in ISE using the **ip name-server** command should be able to resolve the domain names in your Active Directory identity source. Typically, the DNS server that is part of the Active Directory deployment is configured in ISE. If you have to configure multiple DNS servers you can use the **application configure ise** command to do so. See the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on usage of the command.
- There must be at least one global catalog server operational in the domain to which ISE is to be joined.
- The Active Directory username that you provide while joining to an Active Directory domain should be predefined in Active Directory and should have the permission to create and update for computer account objects and change password in the domain you are joining.

Note If your Active Directory domain has subdomains and the user belongs to one of the subdomains, then, the username should also include the subdomain name. For example, for a domain abc.com, if there are two subdomains sub1 and sub2, and the user belongs to sub1, then the username should be sub1\user1.

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations that are described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges that are associated with each role.
- Ensure that your Microsoft Active Directory Server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.

Note Sometimes, the status is indicated as "Connected" when ISE is joined and has a connection established to Active Directory. However, even when ISE is connected, there may still be issues in operation. To identify such issues, refer to the Authentication Report under **Operations > Reports**.

This section contains the following topics:

- Connecting to the Active Directory Domain, page 5-7
- Configuring Active Directory Advanced Settings, page 5-10
- Configuring Active Directory Groups, page 5-11
- Leaving the Active Directory Domain, page 5-13
- Deleting Active Directory Configuration, page 5-14

Connecting to the Active Directory Domain

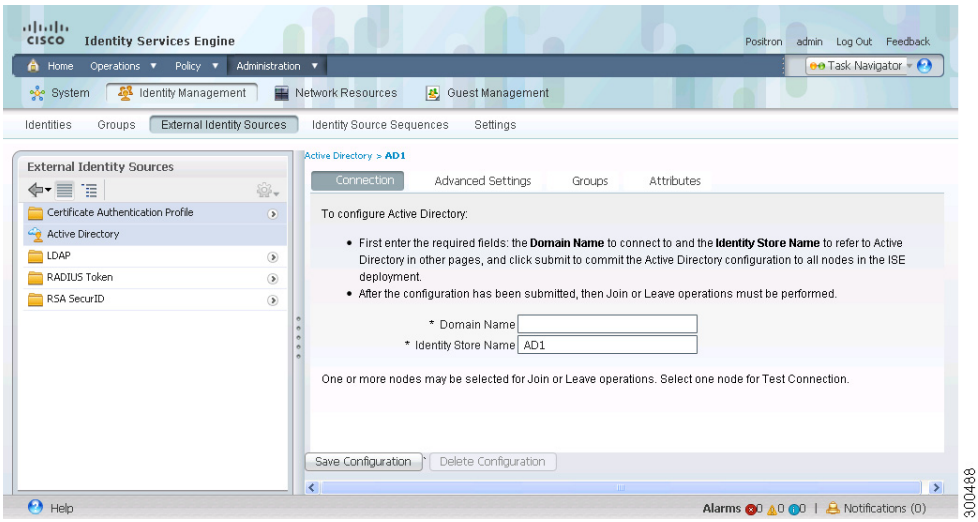
To connect to an Active Directory domain, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

The Active Directory pages appear as shown in Figure 5-1.

Figure 5-1 Active Directory Connections Page



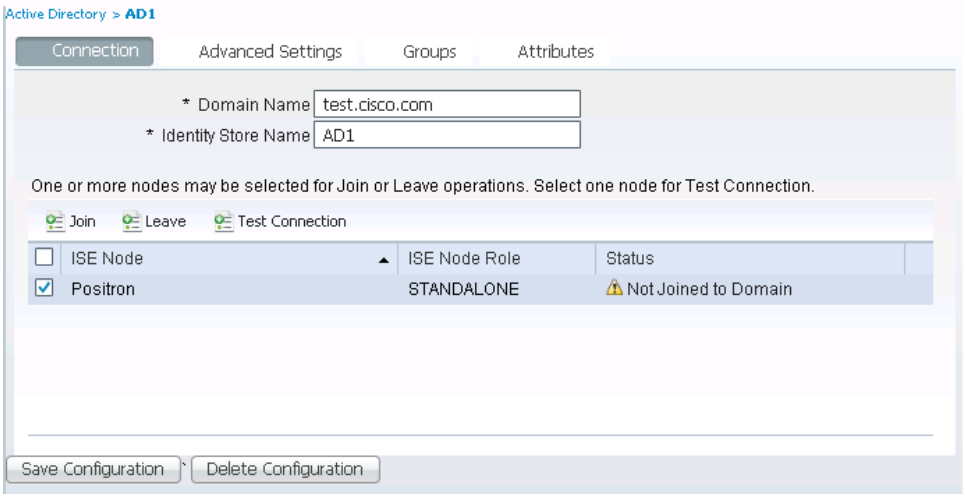
Step 3 Enter the domain name in the Domain Name text box.

Step 4 Enter a friendly name in the Identity Store Name text box for your Active Directory identity source (by default, this value will be AD1).

Step 5 Click **Save Configuration**.

After you successfully submit with a domain name, the deployment join/leave table is displayed with all the ISE nodes, node roles, and their status, as shown in Figure 5-2.

Figure 5-2 Active Directory Nodes Table



Saving the configuration saves the Active Directory domain configuration globally (in the primary as well as the secondary policy service nodes), but none of the ISE nodes are joined to the domain.

Note Even though you submitted the configuration in Step 4, you have to explicitly click Join to connect your ISE node to the Active Directory domain. You must manually perform the join operation for each of the secondary policy service nodes in your deployment for them to be connected to the Active Directory domain.

Step 6 To verify if your ISE node can be connected to the Active Directory domain, check the check box next to the ISE node and click **Test Connection**. A dialog box appears and prompts you to enter the Active Directory username and password.

Step 7 Enter the Active Directory username and password and click **OK**.

Note If your Active Directory domain has subdomains and the user belongs to one of the subdomains, then, the username should also include the subdomain name. For example, for a domain abc.com, if there are two subdomains sub1 and sub2, and the user belongs to sub1, then the username should be sub1\user1.

A dialog box appears with the status of the test connection operation.

Step 8 Click **OK**.

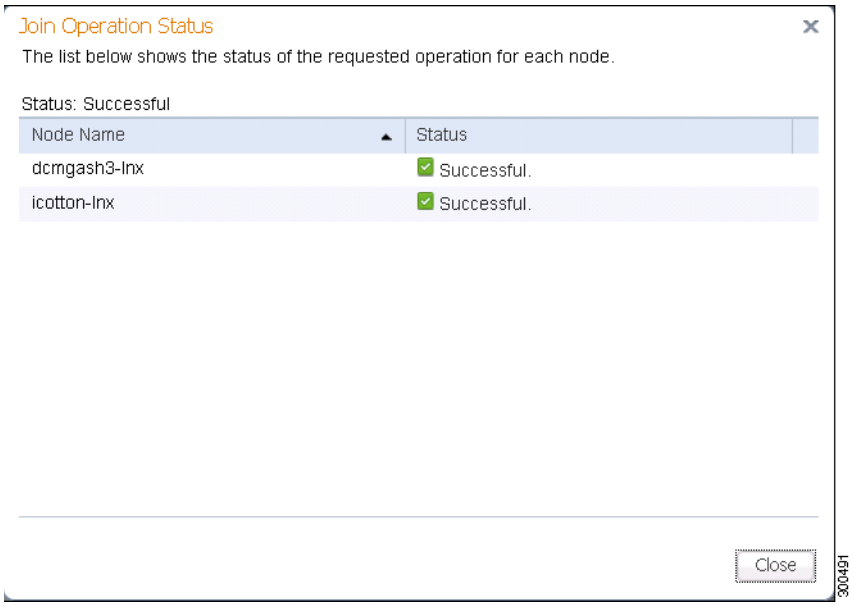
Step 9 To join the ISE node to the Active Directory domain, check the check box next to the ISE node and click **Join**.

The Join Domain dialog box appears.

Step 10 Enter your Active Directory username and password, and click **OK**.

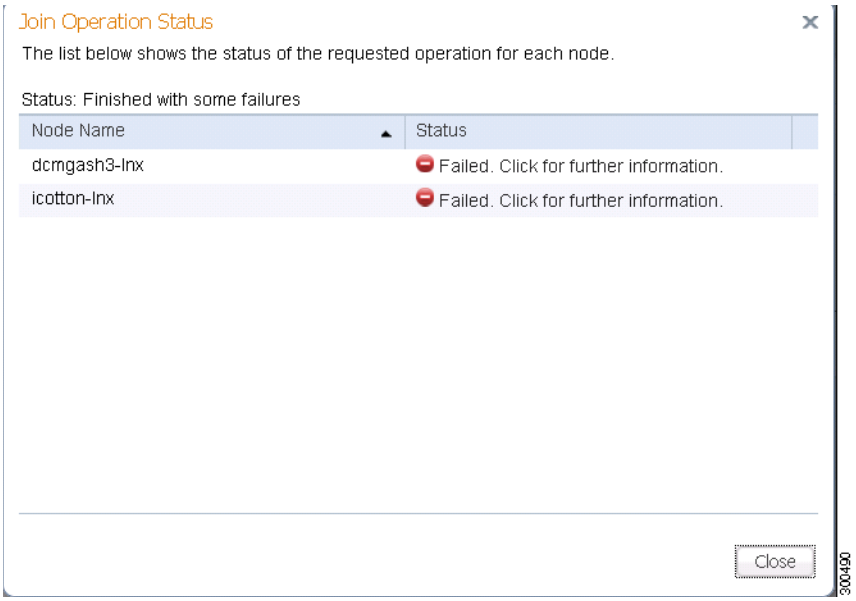
You can select more than one node to join to the Active Directory domain. After you join, a pop-up list is displayed showing the progress of the request for each node. After the operation is completed successfully, each node is marked as such. (Figure 5-3)

Figure 5-3 Success Message Displayed After Active Directory Domain Join



If the join operation is not successful, the failure message is displayed in the pop-up list as shown in Figure 5-4. You can click the failure message for each node to view detailed logs for that node (Figure 5-4).

Figure 5-4 Failure Message Displayed for Active Directory Domain Join



Step 11 Click **Close**.

Configuring Active Directory Advanced Settings

To configure Active Directory Advanced Settings, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

Step 3 Click the **Advanced Settings** tab.

Step 4 Check the **Enable Password Change** check box to allow the user to change the password.

Step 5 Check the **Enable Machine Authentication** check box to allow machine authentication.

Step 6 Check the **Enable Machine Access Restrictions (MARs)** check box to ensure that the machine authentication results are tied to the user authentication and authorization results. If you check this check box, you must enter the Aging Time in hours.

Step 7 Enter the **Aging Time** in hours if you have enabled MARs.

This value specifies the expiration time for machine authentication. If the time expires, the user authentication fails. For example, if you have enabled MARs and enter a value of 2 hours, the user authentication fails if the user tries to authenticate after 2 hours.

Step 8 Click **Save Configuration**.

Next Steps:

1. Configuring Active Directory Groups, page 5-11
2. Configuring Active Directory Attributes, page 5-12

Configuring Active Directory Groups

To configure Active Directory groups that will be available for use in authorization policy conditions, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

Step 3 Ensure that your ISE server is joined to the Active Directory domain. See the "Connecting to the Active Directory Domain" section on page 5-7 for information.

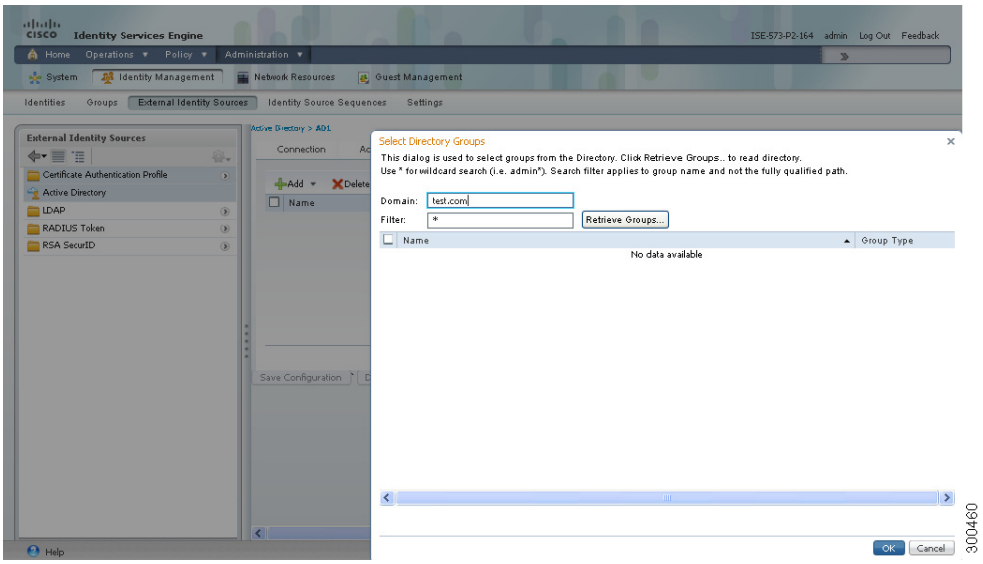
Step 4 Click the **Groups** tab.

The Groups page appears. The groups that you configure in this page will be available for use in policy conditions.

Step 5 Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to choose an existing group.

- If you choose to add groups, enter a name for a new group.
- If you want to choose groups from the directory, the Select Directory Groups page appears. You can refine your search using the filter. For example, enter **cn=users** as the filter criteria and click **Retrieve Groups** to narrow down user groups that begin with cn=users as shown in Figure 5-5. You can also enter the asterisk (*) wildcard character to filter the results.

Figure 5-5 Active Directory Groups Page



Step 6 Check the check boxes next to the groups that you want to use in policy conditions and rules and click **OK**.

You will return to the Groups page. The groups that you have selected appear in the Groups page.

a. To remove the group that you do not want to use in your policy conditions and rules, click the radio button next to that group and click **Delete Group**.

   The following message appears:

   "Are you sure you want to delete?"

b. Click **OK** to delete the group.

Next Step:

Configuring Active Directory Attributes, page 5-12

Configuring Active Directory Attributes

To configure Active Directory attributes that will be available for use in authorization policy conditions, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

Step 3 Ensure that your ISE server is joined to the Active Directory domain. See the "Connecting to the Active Directory Domain" section on page 5-7 for information.

Step 4 Click the **Attributes** tab to choose the attributes that you want to use in policy conditions.

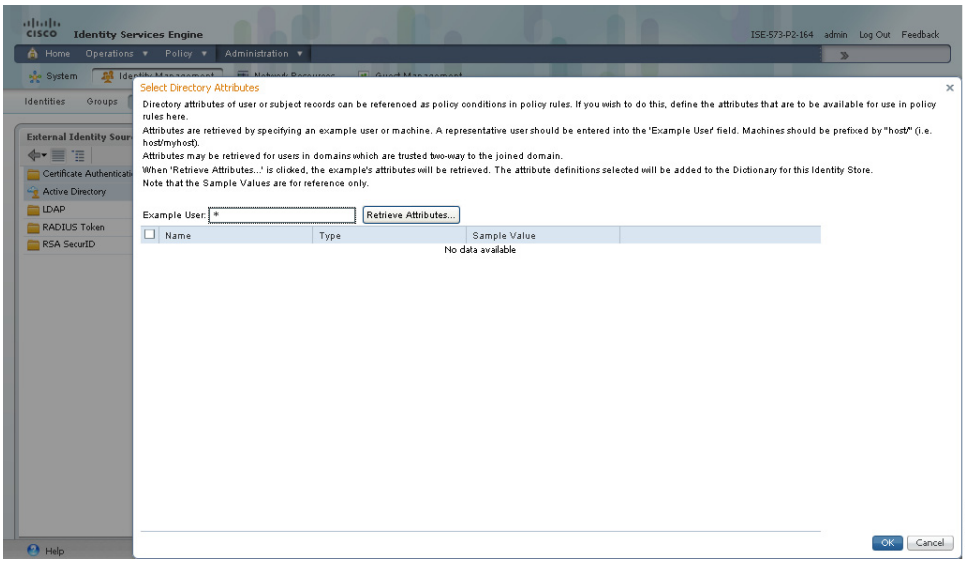
Step 5 Choose **Add > Add Attribute** to add attributes that you want to use in policy conditions or choose **Add > Select Attributes From Directory** to choose a list of attributes from the directory.

- If you choose to add an attribute, enter a name for a new attribute.
- If you want to choose attributes from directory, the Select Directory Attributes page appears. In the Select Directory Attributes page, enter the name of a user in the Example User field and click **Retrieve Attributes** to obtain a list of attributes for the user as shown in Figure 5-6. For example, enter **admin** in the Example User field to obtain the list of attributes for administrators. You can also enter the asterisk (*) wildcard character to filter the results.

Note

- When you choose an example user for obtaining user attributes, ensure that you choose a user from the Active Directory domain to which the Cisco ISE is connected.
- When you choose an example machine to obtain machine attributes, be sure to prefix the machine name with "host/." For example, you might use host/myhost.

Figure 5-6 Active Directory Attributes Page



Step 6 Check the check boxes next to the attributes from the Active Directory that you want ISE to use in policy conditions and click **OK**.

The Attributes page appears. The attributes that you have selected will appear in this page.

To remove any attribute that you do not want to use in policy conditions, click the radio button next to the attribute and click **Delete Attribute**.

Next Steps:

1. See Chapter 16, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 17, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

Leaving the Active Directory Domain

Note Before you leave the Active Directory domain, ensure that you are not using Active Directory as an identity source in your authentication policies either directly or as part of an identity source sequence. If you leave the Active Domain, but still use Active Directory as an identity source for authentication (either directly or as part of an identity source sequence), it might cause authentications to fail.

To leave the Active Directory domain, complete the following steps:

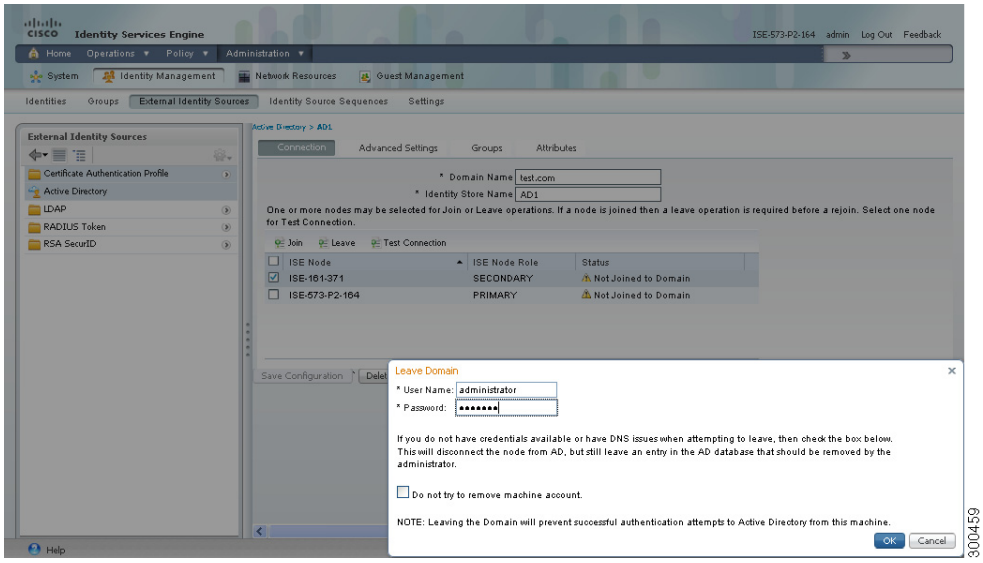
Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

Step 3 To leave an Active Directory domain, check the check box next to the ISE node and click **Leave**.

Step 4 The Leave Domain dialog box appears as shown in Figure 5-7.

Figure 5-7 Leave Domain Dialog Box



Step 5 Enter the Active Directory username and password, and click **OK** to leave the domain and remove the configuration from the ISE database.

Step 6 If you do not have the Active Directory credentials, check the **No Credentials Available** check box and click **OK**.

If you have checked the **No Credentials Available** check box, the primary ISE node will leave the Active Directory domain. The Active Directory administrator has to manually remove the entry that is made in the Active Directory database that was created during the join.

If you have entered the Active Directory credentials, the Cisco ISE will leave the Active Directory domain and delete the configuration from the Active Directory database.

Note The Active Directory credentials must have Create Computer Objects or Delete Computer Objects permission on the computer where the ISE account was created.

Deleting Active Directory Configuration

Prerequisites:

1. Before you delete the Active Directory configuration, ensure that you no longer need to connect to Active Directory and that you have left the Active Directory domain.
2. Do not delete the configuration if you want to join another Active Directory domain. You can leave the domain to which you are currently joined and join a new domain. See the "Leaving the Active Directory Domain" section on page 5-13 for more information.

To remove the Active Directory configuration from ISE, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **Active Directory**.

The Active Directory page appears.

Note Ensure that the Local Node Status is Not Joined to a domain.

Step 3 Click **Delete Configuration**.

You have removed the configuration from the Active Directory database. If you want to use Active Directory at a later point in time, you can resubmit a valid Active Directory configuration.

Enabling Active Directory Debug Logs

Active Directory debug logs are not logged by default. You must enable this option on the ISE node that has assumed the Policy Service persona in your deployment from which you want to obtain debug information.

To enable Active Directory debug logs, complete the following steps:

Step 1 Choose **Administration > System > Logging**.

Step 2 From the Logging navigation pane on the left, click **Debug Log Configuration**.

The Node List window displays a list of nodes in your deployment.

Step 3 Click the radio button next to the ISE Policy Service node from which you want to obtain Active Directory debug information and click **Edit**.

The Debug Level Configuration page appears.

Step 4 Click the **Active Directory** radio button and click **Edit**.

Step 5 From the drop-down list box next to Active Directory, choose DEBUG.

Step 6 Click **Save** to save the logging settings.

The log file is saved in the following location:

/opt/CSCOcpm/logs/ad_agent.log

To download the ad_agent.log file, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Download Logs**.

Step 2 From the Appliance node list navigation pane on the left, select the node from which you want to obtain the Active Directory debug log file.

Step 3 In the right pane, click the **Debug Logs** tab.

Step 4 Scroll down this page to locate the ad_agent.log file. Click this file to download it.

Supplemental Information

This section provides pointers to help you:

- Configure Group Policy in Active Directory, page 5-16
- Configure Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory, page 5-17
- Configure AnyConnect Agent for Machine Authentication, page 5-17

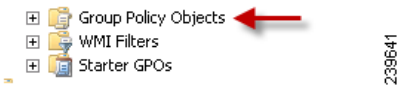
Configure Group Policy in Active Directory

This section provides pointers to set up a group policy for wired services. For more information about how to access the Group Policy management editor, refer to *Microsoft Active Directory Documentation*.

To configure group policy in Active Directory, complete the following steps:

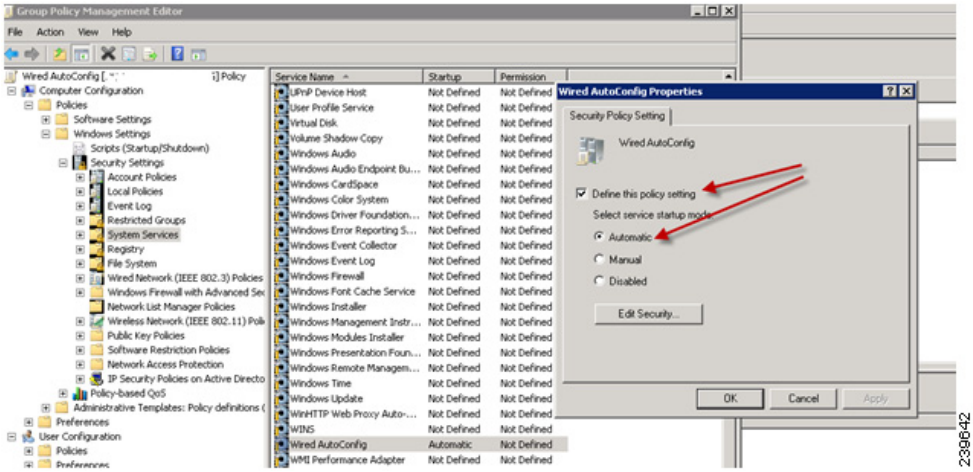
1. Open the Group Policy management editor as shown in Figure 5-8 and create a new policy object or add to an existing domain policy.

Figure 5-8 Group Policy Objects



2. Create a new policy and enter a descriptive name for it. For example, you might use Wired Autoconfiguration.
3. Check the **Define this policy setting** check box and click the **Automatic** radio button for the service startup mode as shown in Figure 5-9.

Figure 5-9 Policy Properties



4. Apply the policy at the desired organizational unit or domain Active Directory level. The computers will receive the policy when they reboot the next time, and this service will be turned on.

Configure Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory

If you are using the Odyssey 5.x supplicant for EAP-TLS machine authentications against Active Directory, you must configure the following in your Odyssey supplicant.

1. Start your Odyssey Access Client.
2. From the Tools menu, choose **Odyssey Access Client Administrator**.
3. Double-click the **Machine Account** icon.
4. From the Machine Account page, you must configure a profile for EAP-TLS authentications:
   a. Choose **Configuration > Profiles**.
   b. Enter a name for the EAP-TLS profile.
   c. In the Authentication tab, choose **EAP-TLS** as the authentication method.
   d. In the Certificate tab, check the **Permit login using my certificate** check box and choose a certificate for the supplicant machine.
   e. In the User Info tab, check the **Use machine credentials** check box.

If this option is enabled, the Odyssey supplicant sends the machine name in the format host\<*machine_name*> and Active Directory identifies the request as coming from a machine and will look up computer objects to perform authentication. If this option is disabled, the Odyssey supplicant sends the machine name without the host\ prefix and Active Directory will look up user objects and the authentication will fail.

Configure AnyConnect Agent for Machine Authentication

When you configure AnyConnect Agent for machine authentication, you can do one of the following:

- Use the default machine hostname, which includes the prefix “host/.”
- Configure a new profile, in which case you must include the prefix “host/” and then the machine name.

LDAP

Lightweight Directory Access Protocol (LDAP), is a networking protocol defined by RFC 2251 for querying and modifying directory services that run on TCP/IP. LDAP is a lightweight mechanism for accessing an X.500-based directory server.

ISE integrates with an LDAP external database, which is also called an identity source, by using the LDAP protocol. See the “Adding and Editing LDAP Identity Sources” section on page 5-22 for information about configuring an LDAP identity source.

This section contains the following topics:

- Key Features of Integration of ISE and LDAP, page 5-18
- Adding and Editing LDAP Identity Sources, page 5-22

Key Features of Integration of ISE and LDAP

This section contains the following:

- Directory Service, page 5-18
- Multiple LDAP Instances, page 5-18
- Failover, page 5-19
- LDAP Connection Management, page 5-19
- User Authentication, page 5-19
- Authentication Using LDAP, page 5-20
- Binding Errors, page 5-20
- User Lookup, page 5-21
- MAC Address Lookup, page 5-21
- Group Membership Information Retrieval, page 5-21
- Attributes Retrieval, page 5-21
- Certificate Retrieval, page 5-22

Directory Service

The directory service is a software application, or a set of applications, for storing and organizing information about the users and resources of a computer network. You can use the directory service to manage user access to these resources. The LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server, and sends operation requests to the server. The server then sends its responses. One or more LDAP servers contain data from the LDAP directory tree or the LDAP backend database.

The directory service manages the directory, which is the database that holds the information. Directory services use a distributed model for storing information, and that information is usually replicated between directory servers.

An LDAP directory is organized in a simple tree hierarchy and can be distributed among many servers. Each server can have a replicated version of the total directory, which is synchronized periodically.

An entry in the tree contains a set of attributes, where each attribute has a name (an attribute type or attribute description) and one or more values. The attributes are defined in a schema.

Each entry has a unique identifier: its distinguished name (DN). This name contains the relative distinguished name (RDN), which is constructed from attributes in the entry, followed by the DN of the parent entry. You can think of the DN as a full filename, and the RDN as a relative filename in a folder.

Multiple LDAP Instances

You can create more than one LDAP instance in ISE. By creating more than one LDAP instance with different IP addresses or port settings, you can configure ISE to authenticate by using different LDAP servers or different databases on the same LDAP server. Each primary server IP address and port configuration, along with the secondary server IP address and port configuration, forms an LDAP instance that corresponds to one ISE LDAP identity source instance.

ISE does not require that each LDAP instance correspond to a unique LDAP database. You can have more than one LDAP instance set to access the same database. This method is useful when your LDAP database contains more than one subtree for users or groups. Because each LDAP instance supports only

one subtree directory for users and one subtree directory for groups, you must configure separate LDAP instances for each user directory subtree and group directory subtree combination for which ISE should submit authentication requests.

Failover

ISE supports failover between a primary LDAP server and a secondary LDAP server. In the context of LDAP authentication with ISE, failover applies when an authentication request fails because ISE could not connect to an LDAP server. Failover can occur when the server is down or is otherwise unreachable by ISE. To use this feature, you must define the primary and secondary LDAP servers, and you must set failover settings.

If you establish failover settings and if the first LDAP server that ISE attempts to contact cannot be reached, ISE always attempts to contact the other LDAP server. The first server that ISE attempts to contact might not always be the primary LDAP server. Instead, the first LDAP server that ISE attempts to contact depends on the previous LDAP authentication attempts and on the value that you enter in the Failback Retry Delay box.

Note Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies from the user interface, so the primary LDAP server must be reachable when you configure these items. Cisco ISE uses the secondary LDAP server only for authentications and authorizations at runtime, according to your failover configuration.

LDAP Connection Management

ISE supports multiple concurrent LDAP connections. Connections are opened on demand at the time of the first LDAP authentication. The maximum number of connections is configured for each LDAP server. Opening connections in advance shortens the authentication time. You can set the maximum number of connections to use for concurrent binding connections. The number of opened connections can be different for each LDAP server (primary or secondary) and is determined based on the maximum number of administration connections configured for each server.

ISE retains a list of open LDAP connections (including the binding information) for each LDAP server that is configured in ISE. During the authentication process, the connection manager attempts to find an open connection from the pool. If an open connection does not exist, a new one is opened.

If the LDAP server closed the connection, the connection manager reports an error during the first call to search the directory, and tries to renew the connection. After the authentication process is complete, the connection manager releases the connection.

User Authentication

LDAP can be used as an external database against which Cisco ISE users authenticate. ISE supports plain password authentication of users. User authentication includes the following actions:

- Searching the LDAP server for an entry that matches the username in the request
- Checking the user password with the one that is found in the LDAP server
- Retrieving the group membership information of the user for use in policies
- Retrieving values for the attributes that you have specified for use in policies and authorization profiles

To authenticate a user, ISE sends a bind request to the LDAP server. The bind request contains the DN and password of the user in clear text. A user is authenticated when the DN and password of the user match the username and password in the LDAP directory.

Note We recommend that you protect the connection to the LDAP server using Secure Sockets Layer (SSL).

- Authentication Errors—ISE logs authentication errors in the ISE log files.
- Initialization Errors—Use the LDAP server timeout settings to configure the number of seconds that ISE waits for a response from an LDAP server before determining that the connection or authentication on that server has failed. Possible reasons for an LDAP server to return an initialization error are:
  - LDAP is not supported.
  - The server is down.
  - The server is out of memory.
  - The user has no privileges.
  - Administrator credentials are configured incorrectly.

Authentication Using LDAP

ISE can authenticate a subject (user or host) against an LDAP identity source by performing a bind operation on the directory server to find and authenticate the subject. After a successful authentication, ISE can retrieve groups and attributes that belong to the subject whenever they are required. You can configure the attributes to be retrieved in the ISE user interface by choosing **Administration > Identity Management > External Identity Sources > LDAP**. These groups and attributes can be used by ISE to authorize the subject.

To authenticate a user or query the LDAP identity source, ISE connects to the LDAP server and maintains a connection pool. See the "LDAP Connection Management" section on page 5-19.

Binding Errors

Possible reasons for an LDAP server to return binding (authentication) errors include the following:

- Parameter errors—Invalid parameters were entered
- User account is restricted (disabled, locked out, expired, password expired, and so on)

The following errors are logged as external resource errors, indicating a possible problem with the LDAP server:

- A connection error occurred
- The timeout expired
- The server is down
- The server is out of memory

The following error is logged as an Unknown User error:

- A user does not exist in the database

The following error is logged as an Invalid Password error, where the user exists, but the password sent is invalid:

- An invalid password was entered

User Lookup

ISE supports the user lookup feature with the LDAP server. This feature allows you to search for a user in the LDAP database and retrieve information without authentication. The user lookup process includes the following actions:

- Searching the LDAP server for an entry that matches the username in the request
- Retrieving the group membership information of the user for use in policies
- Retrieving values for the attributes that you have specified for use in policies and authorization profiles

MAC Address Lookup

ISE supports the MAC address lookup feature. This feature allows you to search for a MAC address in the LDAP database and retrieve information without authentication. The MAC address lookup process includes the following actions:

- Searching the LDAP server for an entry that matches the MAC address of the device
- Retrieving the group information for the device for use in policies
- Retrieving values for the attributes that you have specified for use in policies

Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, ISE must retrieve the group membership information from LDAP databases. LDAP servers represent the association between a subject (a user or a host) and a group in one of the following two ways:

- Groups Refer to Subjects—The group objects contain an attribute that specifies the subject. Identifiers for subjects can be sourced in the group as the following:
  - Distinguished names
  - Plain usernames
- Subjects Refer to Groups—The subject objects contain an attribute that specifies the group to which they belong.

LDAP identity sources contain the following parameters for group membership information retrieval:

- Reference Direction—This parameter specifies the method to use when determining group membership (either groups to subjects or subjects to groups).
- Group Map Attribute—This parameter indicates which attribute contains the group membership information.
- Group Object Class—This parameter determines that certain objects are recognized as groups.
- Group Search Subtree—This parameter indicates the search base for group searches.
- Member Type Option—This parameter specifies how members are sourced in the group member attribute (either as DNs or plain usernames).

Attributes Retrieval

For user authentication, user lookup, and MAC address lookup, ISE must retrieve the subject attributes from LDAP databases. For each instance of an LDAP identity source, an identity source dictionary is created. These dictionaries support attributes of the following data types:

- String

- Unsigned integer 32
- IPv4 address

For unsigned integers and IPv4 attributes, ISE converts the strings that it has retrieved to the corresponding data types. If conversion fails or if no values are retrieved for the attributes, ISE logs a debug message, but does not fail the authentication or the lookup process.

You can optionally configure default values for the attributes that ISE can use when the conversion fails or when ISE does not retrieve any values for the attributes.

Certificate Retrieval

If you have configured certificate retrieval as part of user lookup, then ISE must retrieve the value of the certificate attribute from LDAP. To retrieve the value of the certificate attribute from LDAP, you must have previously configured the certificate attribute in the list of attributes to be accessed while configuring an LDAP identity source.

For information on how to add LDAP identity sources, see the "Adding and Editing LDAP Identity Sources" section on page 5-22.

Adding and Editing LDAP Identity Sources

Prerequisites:

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies from the user interface, so the primary LDAP server must be reachable when you configure these items.

To create an LDAP identity source, complete the following steps:

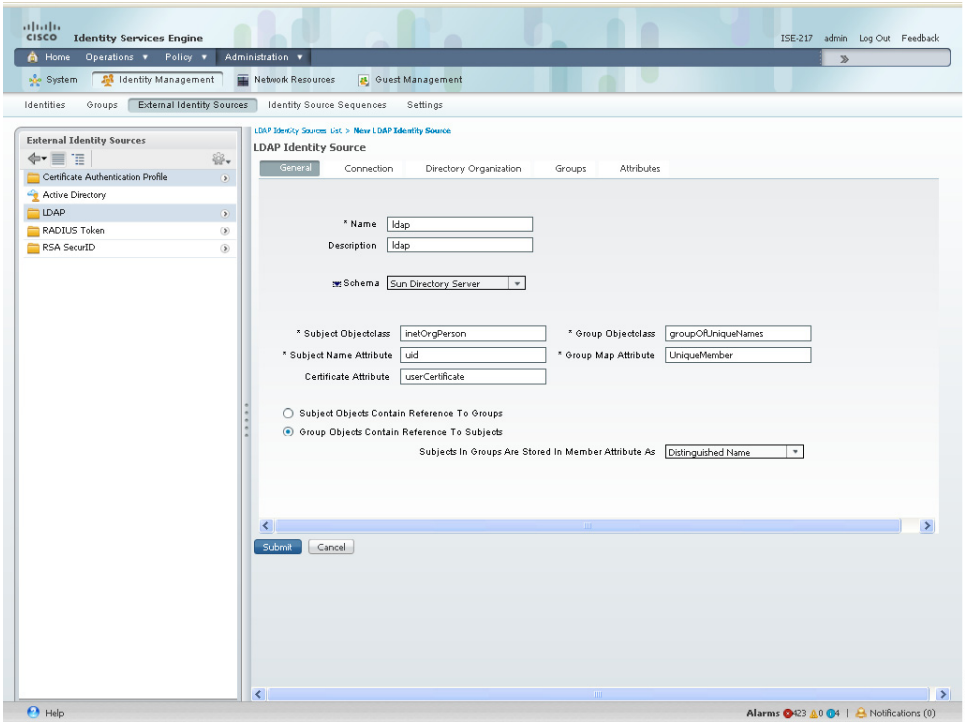
Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

Step 3 Click **Add** to add an LDAP identity source or check the check box next to an LDAP identity source and click **Edit** or **Duplicate** to edit or duplicate an existing LDAP identity source.

Step 4 A screen similar to the one shown in Figure 5-10 appears.

Figure 5-10 LDAP General Tab



Step 5 Enter the values as described in Table 5-2.

Step 6 Click **Submit** to create an LDAP instance.

LDAP General Information

Table 5-2 lists the fields in the LDAP general tab and their descriptions.

Table 5-2 LDAP General Tab

Option	Description
Name	(Required) This value is used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 64 characters.
Description	This description is optional, is of type string, and has a maximum length of 1024 characters.

Table 5-2 LDAP General Tab (continued)

Option	Description
Schema	If you choose any one of the following built-in schema types, the schema details will be prepopulated and are hidden: • Active Directory • Sun Directory Server • Novell eDirectory **Note** You can edit the details from the predefined schema, but ISE detects the change and relabels the Schema as Custom. You can click the Expand button next to Schema to view the schema details.
The following fields contain the schema details and will appear only if you choose the Custom schema.	
Subject Objectclass	(Required) This value is used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 256 characters.
Subject Name Attribute	(Required) This field is the name of the attribute containing the username from request. It is of type string and the maximum length is 256 characters.
Certificate Attribute	Enter the attribute that contains the certificate definitions. These definitions can optionally be used to validate certificates that are presented by clients when they are defined as part of a certificate authentication profile. In such cases, a binary comparison is performed between the client certificate and the certificate retrieved from the LDAP identity source.
Group Objectclass	(Required) This value is used in searches to specify the objects that are recognized as groups. The value is of type string and the maximum length is 256 characters.
Group Map Attribute	(Required) This field specifies the attribute that contains the mapping information. This attribute can be a user or group attribute based on the reference direction that is chosen.
Subject Objects Contain Reference To Groups	Click this radio button if the subject objects contain an attribute that specifies the group to which they belong.
Group Objects Contain Reference To Subjects	Click this radio button if the group objects contain an attribute that specifies the subject. This value is the default value.
Subjects in Groups Are Stored in Member Attribute As	This option is available only when you enable the Group Objects Contain Reference To Subjects radio button. This option specifies how members are sourced in the group member attribute and defaults to the DN.

You can edit an LDAP instance to accomplish the following tasks:

- Configure LDAP Connection Settings, page 5-25
- Configure Directory Organization Values, page 5-27
- Add LDAP Groups, page 5-30
- Select LDAP Attributes, page 5-31

Configure LDAP Connection Settings

To connect to the LDAP server, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

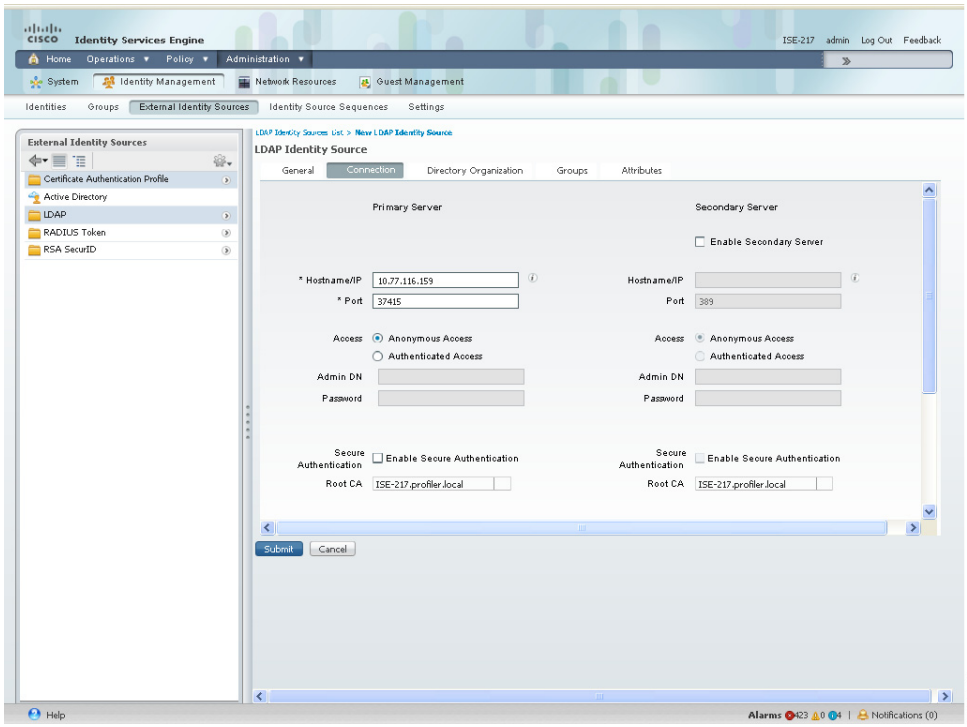
The LDAP page appears.

Step 3 Check the check box next to the LDAP instance that you want to edit, and then click **Edit**.

Step 4 Click the **Connection** tab to configure the primary and secondary servers.

A screen similar to the one shown in Figure 5-11 appears.

Figure 5-11 LDAP Connection Tab



Step 5 Enter the values as described in Table 5-3.

Step 6 Click **Submit** to save the connection parameters.

LDAP Connection Settings

Table 5-3 lists the fields in the LDAP connection tab and their descriptions.

Table 5-3 LDAP Connection Tab

Option	Description
Enable Secondary Server	Check this option to enable the secondary LDAP server to be used as a backup in the event that the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server.
Primary and Secondary Servers	
Hostname/IP	(Required) Enter the IP address or DNS name of the machine that is running the LDAP software. The hostname can contain from 1 to 256 characters or a valid IP address expressed as a string. The only valid characters for hostnames are alphanumeric characters (a to z, A to Z, 0 to 9), the dot (.), and the hyphen (-).
Port	(Required) Enter the TCP/IP port number on which the LDAP server is listening. Valid values are from 1 to 65,535. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information from the LDAP server administrator.
Access	(Required) Anonymous Access—Click to ensure that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client read access to any data that is configured as accessible to any unauthenticated client. In the absence of a specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection. Authenticated Access—Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields.
Admin DN	Enter the DN of the administrator. The Admin DN is the LDAP account that permits searching of all required users under the User Directory Subtree and permits searching groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users who are authenticated by that LDAP.
Password	Enter the LDAP administrator account password.
Secure Authentication	Click to use SSL to encrypt communication between ISE and the primary LDAP server. Verify that the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must choose a root CA.
Root CA	Choose a trusted root certificate authority from the drop-down list box to enable secure authentication with a certificate. See the "Certificate Authority Certificates" section on page 13-16 and "Adding a Certificate Authority Certificate" section on page 13-18 for information on CA certificates.
Server Timeout	Enter the number of seconds that ISE waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed. Valid values are 1 to 300. The default is 10.

Table 5-3 LDAP Connection Tab (continued)

Option	Description
Max. Admin Connections	Enter the maximum number of concurrent connections (greater than 0) with LDAP administrator account permissions that can run for a specific LDAP configuration. These connections are used to search the directory for users and groups under the User Directory Subtree and the Group Directory Subtree. Valid values are 1 to 99. The default is 20.
Test Bind to Server	Click to test and ensure that the LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.

Configure Directory Organization Values

To configure directory organization values, complete the following steps:

Note For LDAP identity source, the following three searches are applicable:

- Search for all groups in group subtree for administration
- Search for user in subject subtree to locate user
- Search for groups in which the user is a member

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

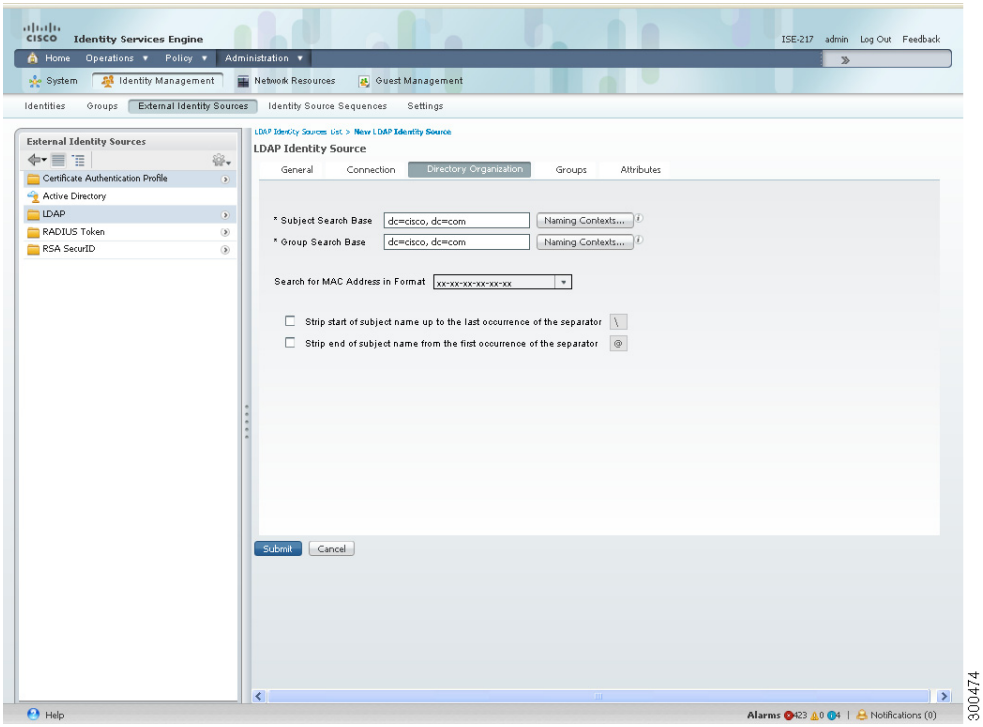
The LDAP page appears.

Step 3 Check the check box next to the LDAP instance that you want to edit, then click **Edit**.

Step 4 Click the **Directory Organization** tab.

A screen similar to the one shown in Figure 5-12 appears.

Figure 5-12 LDAP Directory Organization Tab



Step 5 Enter the values as described in Table 5-4.

Step 6 Click **Submit** to save the configuration.

LDAP Directory Organization Settings

Table 5-4 lists the fields in the LDAP directory organization tab and their descriptions.

Table 5-4 LDAP Directory Organization Tab

Option	Description
Subject Search Base	(Required) Enter the DN for the subtree that contains all subjects. For example: o=corporation.com If the tree containing subjects is the base DN, enter: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

Table 5-4 LDAP Directory Organization Tab (continued)

Option	Description
Group Search Base	(Required) Enter the DN for the subtree that contains all groups. For example: ou=organizational unit, ou=next organizational unit, o=corporation.com If the tree containing groups is the base DN, type: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.
Search for MAC Address in Format	MAC addresses in internal identity sources are sourced in the format xx-xx-xx-xx-xx-xx. MAC addresses in LDAP databases can be sourced in different formats. However, when ISE receives a host lookup request, ISE converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list box to enable searching for MAC addresses in a specific format, where <*format*> can be any one of the following: • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx The format you choose must match the format of the MAC address sourced in the LDAP server.
Strip Start of Subject Name Up To the Last Occurrence of the Separator	Enter the appropriate text to remove domain prefixes from usernames. If, in the username, ISE finds the delimiter character that is specified in this field, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the <start_string> box, ISE strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is DOMAIN\echamberlain, ISE submits echamberlain to an LDAP server. **Note** The <start_string> cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ISE does not allow these characters in usernames. If you provide any of these characters, stripping fails.

Table 5-4 LDAP Directory Organization Tab (continued)

Option	Description
Strip End of Subject Name from the First Occurrence of the Separator	Enter the appropriate text to remove domain suffixes from usernames. If, in the username, ISE finds the delimiter character that is specified in this field, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the characters that are specified in this field, ISE strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is the at symbol (@) and the username is *jwiedman@domain*, then ISE submits *jwiedman* to an LDAP server. **Note** The <*end_string*> box cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ISE does not allow these characters in usernames. If you provide any of these characters, stripping fails.

Add LDAP Groups

To add LDAP groups, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

The LDAP page appears.

Step 3 Check the check box next to the LDAP instance that you want to edit, then click **Edit**.

Step 4 Click the **Groups** tab.

The Groups page appears.

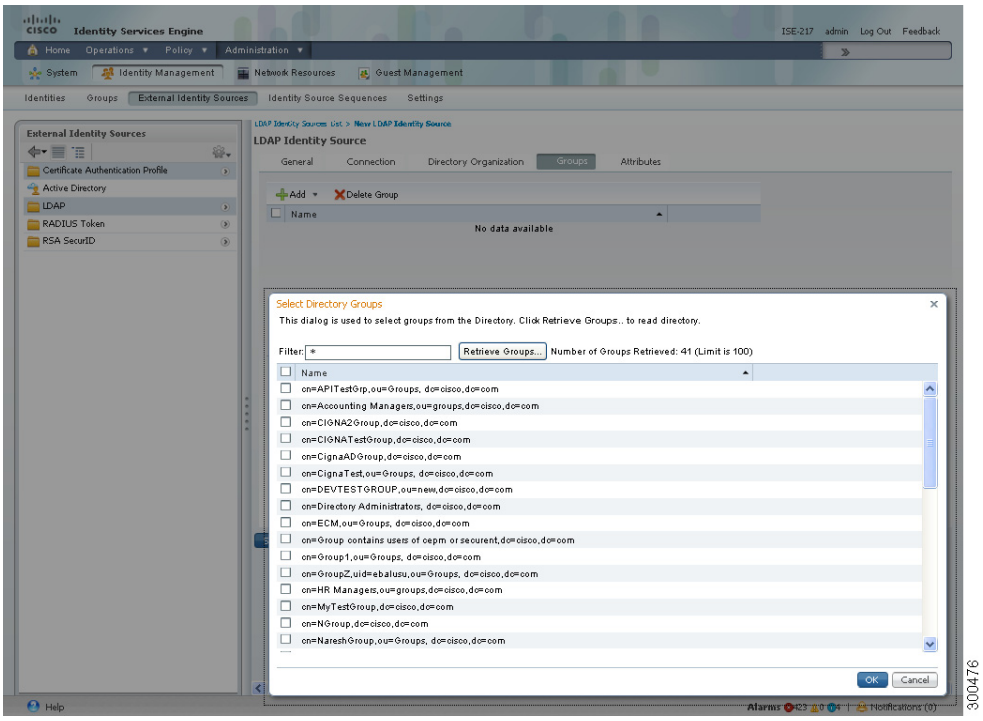
Step 5 Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to select the groups from the LDAP directory.

Step 6 If you choose to add a group, enter a name for the new group.

Step 7 If you are selecting from the directory, enter the filter criteria and click **Retrieve Groups**. Your search criteria can contain the asterisk (*) wildcard character.

A screen similar to the one shown in Figure 5-13 appears.

Figure 5-13 LDAP Select Groups Page



Step 8 Check the check boxes next to the groups that you want to select, then click **OK**.

The groups that you have selected will appear in the Groups page.

Step 9 Click **Submit** to save the group selection.

Select LDAP Attributes

To choose LDAP attributes, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **LDAP**.

The LDAP page appears.

Step 3 Check the check box next to the LDAP instance that you want to edit, then click **Edit**.

Step 4 Click the **Attributes** tab.

The Attributes page appears.

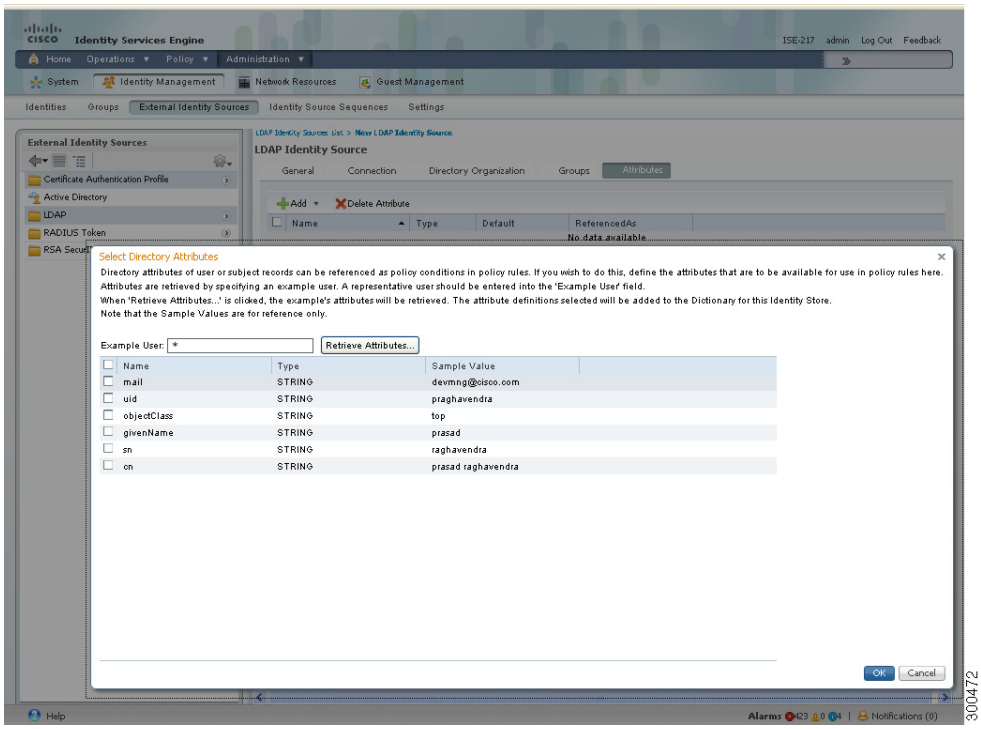
Step 5 Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to select attributes from the LDAP server.

Step 6 If you choose to add an attribute, enter a name for the new attribute.

Step 7 If you choose the Select from Directory option, the Select Directory Attributes page appears. Enter an example user and click **Retrieve Attributes** to retrieve the user's attributes. You can use the asterisk (*) wildcard character.

Step 8 A screen similar to the one shown in Figure 5-14 appears.

Figure 5-14 Select Directory Attributes Page



Step 9 Check the check boxes next to the attributes that you want to select, then click **OK**.

The attributes that you have selected appear in the Attributes page.

Step 10 Click **Submit** to save the attribute selections.

Next Steps:

1. See Chapter 16, "Managing Authentication Policies" for information on how to create authentication policies.
2. See Chapter 17, "Managing Authorization Policies and Profiles" for information on how to create authorization profiles and policies.

RADIUS Token Identity Sources

A server that supports the RADIUS protocol and provides authentication, authorization, and accounting (AAA) services to users and devices is called the RADIUS server. The RADIUS identity source is simply an external identity source that contains a collection of subjects and their credentials and uses the

RADIUS protocol for communication. For example, the Safeword token server is an identity source that can contain several users and their credentials as one-time passwords that provides an interface that you can query using the RADIUS protocol.

ISE supports any RADIUS RFC 2865-compliant server as an external identity source. ISE supports multiple RADIUS token server identities, for example, the RSA SecurID server and the SafeWord server. RADIUS identity sources can work with any RADIUS token server that is used to authenticate the user. RADIUS identity sources use the User Datagram Protocol (UDP) port for authentication sessions. The same UDP port is used for all RADIUS communication.

For ISE to successfully send RADIUS messages to a RADIUS-enabled server, you must ensure that the gateway devices between the RADIUS-enabled server and ISE allow communication over the UDP port. You can configure the UDP port through the ISE user interface.

This section contains the following topics:

- Key Features of the Integration of ISE and RADIUS Identity Source, page 5-33
- Adding or Editing a RADIUS Token Server, page 5-36

Key Features of the Integration of ISE and RADIUS Identity Source

Supported Authentication Protocols

ISE supports the following authentication protocols for RADIUS identity sources:

- RADIUS PAP
- PEAP with inner EAP-GTC
- EAP-FAST with inner EAP-GTC

Constraints

RADIUS token servers use the UDP port for authentication sessions. This port is used for all RADIUS communication. For ISE to send RADIUS one-time password (OTP) messages to a RADIUS-enabled token server, you must ensure that the gateway devices between ISE and the RADIUS-enabled token server allow communication over the UDP port.

RADIUS Shared Secret

You must provide a shared secret while configuring RADIUS identity sources in ISE. This shared secret should be the same as the shared secret that is configured on the RADIUS token server.

Failover

ISE allows you to configure multiple RADIUS identity sources. Each RADIUS identity source can have primary and secondary RADIUS servers. When ISE is unable to connect to the primary server, it uses the secondary server.

Password Prompt

RADIUS identity sources allow you to configure the password prompt. You can configure the password prompt through the ISE user interface.

User Authentication

ISE obtains the user credentials (username and passcode) and passes them to the RADIUS token server. ISE also relays the results of the RADIUS token server authentication processing to the user.

User Attribute Cache

RADIUS token servers, by default, do not support user lookups. However, the user lookup functionality is essential for the following ISE features:

- PEAP session resume—This feature allows the PEAP session to resume after successful authentication during EAP session establishment.
- EAP/FAST fast reconnect—This feature allows fast reconnection after successful authentication during EAP session establishment.

ISE caches the results of successful authentications to process user lookup requests for these features. For every successful authentication, the name of the authenticated user and the retrieved attributes are cached. Failed authentications are not written to the cache.

The cache is available in the memory at runtime and is not replicated between ISE nodes in a distributed deployment. You can configure the Time to Live (TTL) limit for the cache through the ISE user interface. You must enable the identity caching option and set the aging time in minutes. The cache is available in the memory for the specified amount of time.

RADIUS Identity Source in Identity Sequence

You can add the RADIUS identity source for authentication sequence in an identity source sequence. However, you cannot add the RADIUS identity source for attribute retrieval sequence because you cannot query the RADIUS identity source without authentication. ISE cannot distinguish among different error cases while authenticating with a RADIUS server. RADIUS servers return an Access-Reject message for all error cases. For example, when a user is not found in the RADIUS server, instead of returning a User Unknown status, the RADIUS server returns an Access-Reject message. You can, however, enable the Treat Rejects as Authentication Failed or User Not Found option, which is available in the RADIUS identity source pages of the ISE user interface.

Authentication Failure Messages

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. ISE provides the option to configure this message through the ISE user interface as either Authentication Failed or User Not Found. However, this option returns a User Not Found message not only for cases where the user is not known, but for all failure cases.

Table 5-5 lists the different failure cases that are possible with RADIUS identity servers.

Table 5-5 Error Handling

Cause of Authentication Failure	Failure Cases
Authentication Failed	• User is unknown. • User attempts to log in with an incorrect passcode. • User login hours expired.

Table 5-5 Error Handling (continued)

Cause of Authentication Failure	Failure Cases
Process Failed	• RADIUS server is configured incorrectly in ISE. • RADIUS server is unavailable. • RADIUS packet is detected as malformed. • Problem during sending or receiving a packet from the RADIUS server. • Timeout.
Unknown User	Authentication failed and the Fail on Reject option is set to false.

Username Special Format with SafeWord Server

The SafeWord token server supports authentication with the following username format:

Username—Username, OTP

As soon as ISE receives the authentication request, it parses the username and converts it to the following username:

Username—Username

The SafeWord token servers support both of these formats. ISE works with various token servers. While configuring a SafeWord server, you must check the SafeWord Server check box in the ISE user interface for ISE to parse the username and convert it to the specified format. This conversion is done in the RADIUS token server identity source before the request is sent to the RADIUS token server.

Authentication Request and Response

When ISE forwards an authentication request to a RADIUS-enabled token server, the RADIUS authentication request contains the following attributes:

- User-Name (RADIUS attribute 1)
- User-Password (RADIUS attribute 2)
- NAS-IP-Address (RADIUS attribute 4)

ISE expects to receive any one of the following responses:

- Access-Accept—No attributes are required, however, the response can contain a variety of attributes based on the RADIUS token server configuration.
- Access-Reject—No attributes are required.
- Access-Challenge—The attributes that are required per RADIUS RFC are the following:
  - State (RADIUS attribute 24)
  - Reply-Message (RADIUS attribute 18)
  - One or more of the following attributes: Vendor-Specific, Idle-Timeout (RADIUS attribute 28), Session-Timeout (RADIUS attribute 27), Proxy-State (RADIUS attribute 33)

No other attributes are allowed in Access-Challenge.

For information on how to add RADIUS token servers, see the "Adding or Editing a RADIUS Token Server" section on page 5-36.

For information on how to delete RADIUS token servers, see the "Deleting a RADIUS Token Server" section on page 5-39.

Adding or Editing a RADIUS Token Server

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create or edit a RADIUS identity source, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

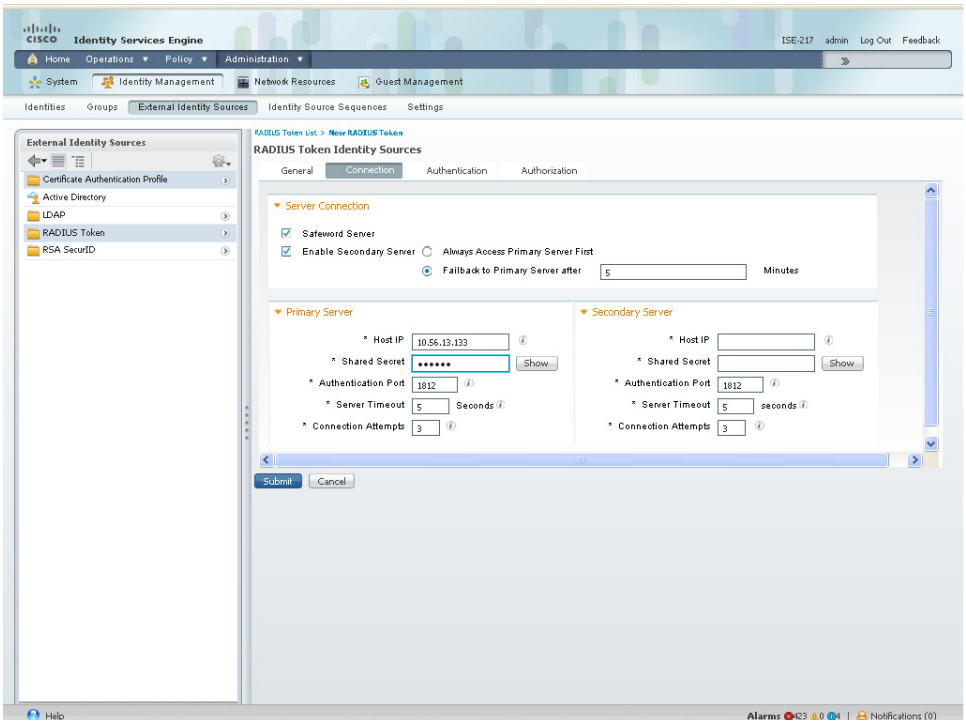
Step 2 From the External Identity Sources navigation pane on the left, click **RADIUS Token**.

The RADIUS Token Identity Sources page appears.

Step 3 Click **Add** to add a new RADIUS identity source or check the check box next to the RADIUS token server that you want to edit, then click **Edit** or click **Duplicate** to create a duplicate RADIUS token server definition.

A screen similar to the one shown in Figure 5-15 appears.

Figure 5-15 RADIUS Token Server Prompts Tab



Step 4 In the General and Connection tabs, enter the values as described in Table 5-6.

Step 5 Click the **Authentication** tab.

This tab allows you to control the responses to an Access-Reject message from the RADIUS token server. This response could either mean that the credentials are invalid or that the user is not known. ISE accepts either one of the following responses: Failed authentication or User not found. This tab also allows you to enable identity caching and to set the aging time for the cache. You can also configure a prompt to request the password.

Step 6 Select the following:

- Click the Treat Rejects as 'authentication failed' radio button if you want the Access-Reject response from the RADIUS token server to be treated as a failed authentication.
- Click the Treat Rejects as 'user not found' radio button if you want the Access-Reject response from the RADIUS token server to be treated as an unknown user failure.
- Enter a prompt for requesting the password.

Step 7 Click the **Authorization** tab.

This tab allows you to configure a name that will appear for this single attribute that is returned by the RADIUS token server while sending an Access-Accept response to ISE. This attribute can be used in authorization policy conditions. Enter a name for this attribute in the Attribute Name ACS field. The default value is CiscoSecure-Group-Id.

Step 8 Click **Submit** to save the RADIUS Token identity source.

RADIUS Token Server Connections

Table 5-6 lists the fields in the RADIUS Token Server Connections tab and their default values.

Table 5-6 RADIUS Token Server Prompts Tab

Option	Description
Name	(Required) This field is the name of the RADIUS token server. The maximum number of characters allowed is 64.
Description	This field is an optional description. The maximum number of characters is 1024.
SafeWord Server	Check this check box if your RADIUS identity source is a SafeWord server.
Enable Secondary Server	Check this check box to enable the secondary RADIUS token server for ISE to be used as a backup in case the primary fails. If you check this check box, you must configure a secondary RADIUS token server.
Always Access Primary Server First	Click this radio button if you want ISE to always access the primary server first.
Fallback to Primary Server after	Click this radio button to specify the amount of time in minutes that ISE can authenticate using the secondary RADIUS token server if the primary server cannot be reached. After this time elapses, ISE reattempts to authenticate against the primary server.

Table 5-6 RADIUS Token Server Prompts Tab (continued)

Option	Description
Primary Server	
Host IP	Enter the IP address of the primary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret that is configured on the primary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the primary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that ISE should wait for a response from the primary RADIUS token server before it determines that the primary server is down. Valid values are 1 to 300. The default is 5.
Connection Attempts	Specify the number of attempts that ISE should make to reconnect to the primary server before moving on to the secondary server (if defined) or dropping the request if a secondary server is not defined. Valid values are 1 to 9. The default is 3.
Secondary Server	
Host IP	Enter the IP address of the secondary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret configured on the secondary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the secondary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that ISE should wait for a response from the secondary RADIUS token server before it determines that the secondary server is down. Valid values are 1 to 300. The default is 5.
Connection Attempts	Specify the number of attempts that ISE should make to reconnect to the secondary server before dropping the request. Valid values are 1 to 9. The default is 3.

Next Steps:

1. See Chapter 16, “Managing Authentication Policies” for information on how to create authentication policies.
2. See Chapter 17, “Managing Authorization Policies and Profiles” for information on how to create authorization profiles and policies.

Deleting a RADIUS Token Server

Prerequisites:

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- Ensure that you do not select the RADIUS token servers that are part of an identity source sequence. If you select a RADIUS token server that is part of an identity source sequence for deletion, the delete operation will fail.

To delete a RADIUS identity source, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **RADIUS Token**.

The RADIUS Token Identity Sources page appears with a list of configured RADIUS token servers.

Step 3 Check the check box next to the RADIUS token server or servers that you want to delete, then click **Delete**.

ISE prompts you with the following message:

Are you sure you want to delete?

Step 4 Click **OK** to delete the RADIUS token server or servers that you have selected.

Note If you select multiple RADIUS token servers for deleting, and one of them is used in an identity source sequence, the delete operation fails and none of the RADIUS token servers are deleted.

RSA Identity Sources

ISE supports the RSA SecurID server as an external database. RSA SecurID two-factor authentication consists of the PIN of the user and an individually registered RSA SecurID token that generates single-use token codes based on a time code algorithm. A different token code is generated at fixed intervals (usually each at 30 or 60 seconds). The RSA SecurID server validates this dynamic authentication code. Each RSA SecurID token is unique, and it is not possible to predict the value of a future token based on past tokens. Thus, when a correct token code is supplied together with a PIN, there is a high degree of certainty that the person is a valid user. Therefore, RSA SecurID servers provide a more reliable authentication mechanism than conventional reusable passwords.

ISE supports the following RSA identity sources:

- RSA ACE/Server 6.x series
- RSA Authentication Manager 7.x series

You can integrate with RSA SecurID authentication technology in any one of the following ways:

- Using the RSA SecurID agent—Users are authenticated with their username and passcode through the RSA native protocol.

- Using the RADIUS protocol—Users are authenticated with their username and passcode through the RADIUS protocol.

The RSA SecurID token server in ISE integrates with the RSA SecurID authentication technology by using the RSA SecurID Agent.

Cisco ISE Release 1.1 supports only one RSA realm.

This section contains the following topics:

- Integrating ISE with RSA SecurID Server, page 5-40
- Configuring RSA Prompts, page 5-48
- Configuring RSA Messages, page 5-49

Integrating ISE with RSA SecurID Server

These are the two administrative roles involved in integrating ISE with an RSA SecurID server:

- RSA Server Administrator—Configuring and maintaining RSA systems and integration
- ISE Administrator—Configuring ISE to integrate with the RSA SecurID server and maintaining the configuration.

This section describes the processes that are involved in integrating ISE with the RSA SecurID server as an external identity source. For more information on RSA servers, please refer to the RSA documentation.

Configuring RSA in ISE

The RSA administrative system generates an sdconf.rec file, which the RSA system administrator will provide to you. This file allows you to add ISE servers as RSA SecurID agents in the realm. You have to browse and add this file to ISE. By the process of replication, the primary ISE server distributes this file to all the secondary servers.

Authenticating RSA Agents in ISE Against the RSA SecurID Server

After the sdconf.rec file is installed on all ISE servers, the RSA agent module initializes, and authentication with RSA-generated credentials proceeds on each of the ISE servers. After the agent on each of the ISE servers in a deployment has successfully authenticated, the RSA server and the agent module together download the securid file. This file resides in the ISE file system and is in a well-known place defined by the RSA agent.

Maintaining RSA Servers in ISE Deployment

After you have added the sdconf.rec file in ISE, the RSA SecurID administrator might have to update the sdconf.rec file in case of decommissioning an RSA server or adding a new RSA secondary server. The RSA SecurID administrator will provide you with an updated file. You can then reconfigure ISE with the updated file. The replication process in ISE distributes the updated file to the secondary ISE servers in the deployment. ISE first updates the file in the file system and coordinates with the RSA agent module to phase the restart process appropriately. When the sdconf.rec file is updated, the sdstatus.12 and securid files are reset (deleted).

Overriding Automatic RSA Routing

You can have more than one RSA server in a realm. The sdopts.rec file performs the role of a load balancer. ISE servers and RSA SecurID servers operate through the agent module. The agent module that resides on ISE maintains a cost-based routing table to make the best use of the RSA servers in the realm. You can, however, choose to override this routing with a manual configuration. You can override with a manual configuration for each ISE server for the realm using a text file called sdopts.rec through the ISE user interface. Refer to the RSA documentation for information on how to create this file.

Resetting an RSA Node Secret

The securid file is a secret node key file. When RSA is initially set up, it uses a secret to validate the agents. When the RSA agent that resides in ISE successfully authenticates against the RSA server for the first time, it creates a file on the client machine called securid and uses it to ensure that the data exchanged between the machines is valid. At times, you may have to delete the securid file from a specific ISE server or a group of servers in your deployment (for example, after a key reset on the RSA server). You can use the ISE user interface to delete this file from an ISE server for the realm. When the RSA agent in ISE authenticates successfully the next time, it creates a new securid file.

Resetting an RSA Automatic Availability

The sdstatus.12 file provides information about the availability of RSA servers in the realm. For example, it provides information on which servers are active and which are down. The agent module works with the RSA servers in the realm to maintain this availability status. This information is serially listed in the sdstatus.12 file, which is sourced in a well-known location in the ISE file system. Sometimes this file becomes old and the current status is not reflected in this file. You must remove this file so that the current status can be re-created. You can use the Cisco ISE user interface to delete the file from a specific Cisco ISE server for a specific realm. ISE coordinates with the RSA agent and ensures correct restart phasing.

The availability file sdstatus.12 will be deleted whenever the securid file is reset, or the sdconf.rec or sdopts.rec files are updated.

Distributed Environment Considerations

Managing RSA identity sources in a distributed ISE environment involves the following:

- Distributing the sdconf.rec and sdopts.rec files from the primary server to the secondary servers.
- Deleting the securid and sdstatus.12 files.

For more information, see the following topics:

- Importing the RSA Configuration File, page 5-42
- Configuring the Options File for a ISE Server and Resetting SecurID and sdstatus.12 Files, page 5-43
- Adding and Editing RSA Identity Sources, page 5-42

Adding and Editing RSA Identity Sources

To create or edit an RSA identity source, you must import the RSA configuration file (sdconf.rec). See the "Importing the RSA Configuration File" section on page 5-42 for more information.

Prerequisites:

1. You must obtain the sdconf.rec file from your RSA administrator.
2. Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Importing the RSA Configuration File

To configure general RSA settings, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

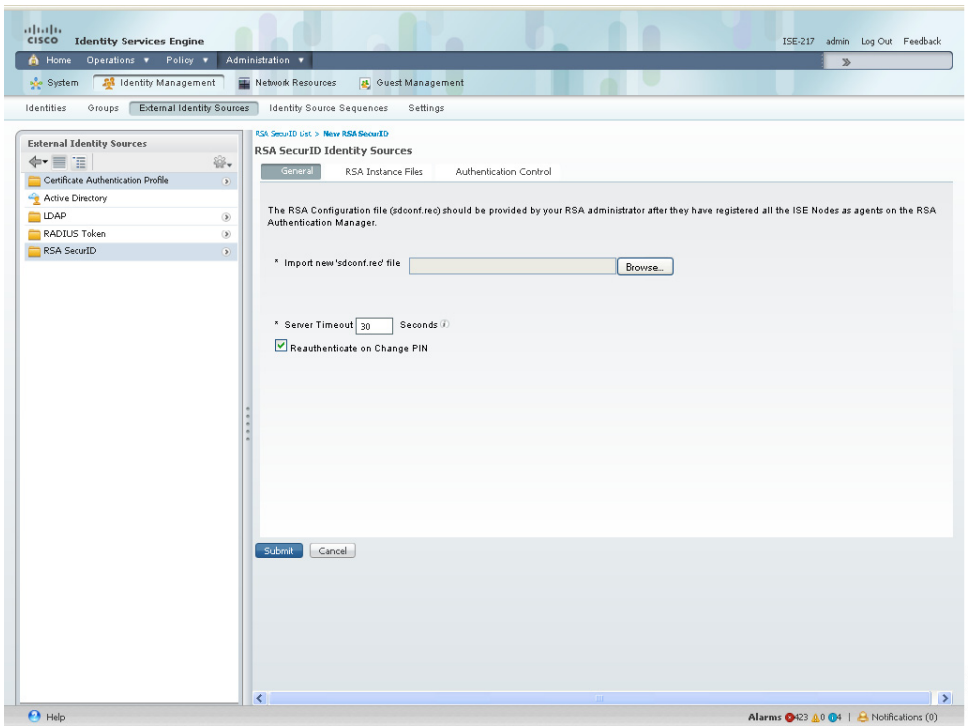
Step 2 From the External Identity Sources navigation pane on the left, click **RSA SecurID**.

The RSA SecurID Identity Sources page appears.

Step 3 Click **Add** to add an RSA identity source or check the check box next to the RSA identity source that you want to edit, and then click **Edit** or click **Duplicate** to create a duplicate entry of the RSA identity source.

The RSA General tab appears as shown in Figure 5-16.

Figure 5-16 RSA General Tab



Step 4 Click **Browse** to choose the new or updated sdconf.rec file from the system that is running your client browser.

When you create the RSA identity source for the first time, the Import new sdconf.rec file field will be a mandatory field. From then on, you can replace the existing sdconf.rec file with an updated one, but replacing the existing file is optional.

Step 5 (Required) Enter the server timeout value in seconds. ISE will wait for a response from the RSA server for the amount of time specified before it times out. This value can be any integer from 1 through 199. The default value is 30 seconds.

Step 6 Check the Reauthenticate on Change PIN check box to force a reauthentication when the PIN is changed.

Step 7 Click **Save** to save the configuration.

ISE also supports the following scenarios:

- Configuring the Options File for a ISE Server and Resetting SecurID and sdstatus.12 Files, page 5-43
- Configuring Authentication Control Options, page 5-46

Configuring the Options File for a ISE Server and Resetting SecurID and sdstatus.12 Files

To configure the sdopts.rec file, and to reset the securid and sdstatus.12 files, complete the following steps:

Step 1 Log into your ISE server.

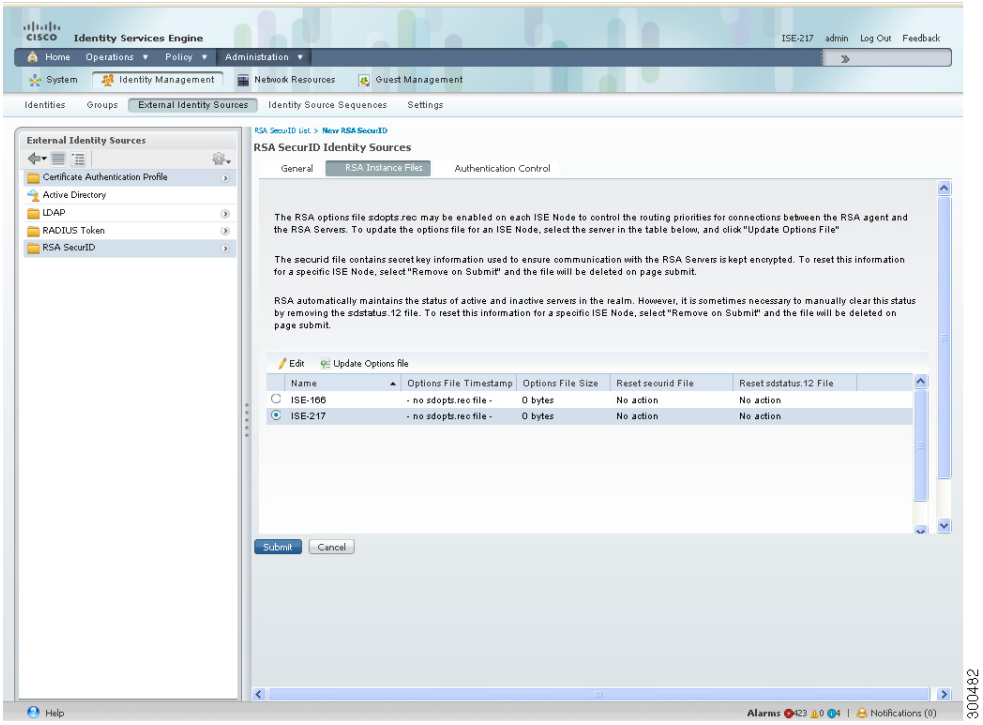
Step 2 Choose **Administration > Identity Management > External Identity Sources**.

Step 3 Click **Add** to add an RSA identity source or check the check box next to the RSA identity source that you want to edit, and then click **Edit** or click **Duplicate** to create a duplicate RSA identity source entry.

Step 4 Click the **RSA Instance Files** tab.

Step 5 A screen similar to the one shown in Figure 5-17 appears:

Figure 5-17 RSA Instance Files Tab

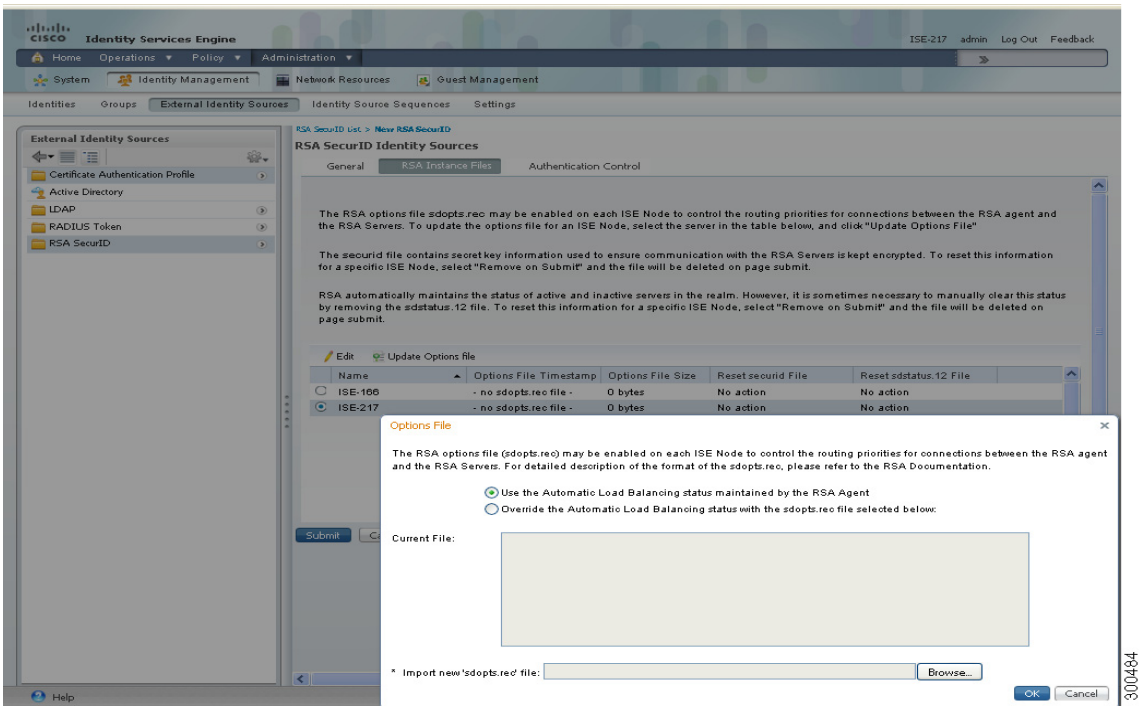


This page lists the sdopts.rec files for all the ISE servers in your deployment.

Step 6 Click the radio button next to the sdopts.rec file for a particular ISE server and click **Update Options File**.

A screen similar to the one shown in Figure 5-18 appears.

Figure 5-18 RSA Options File



The existing file is displayed in the Current File region (display only).

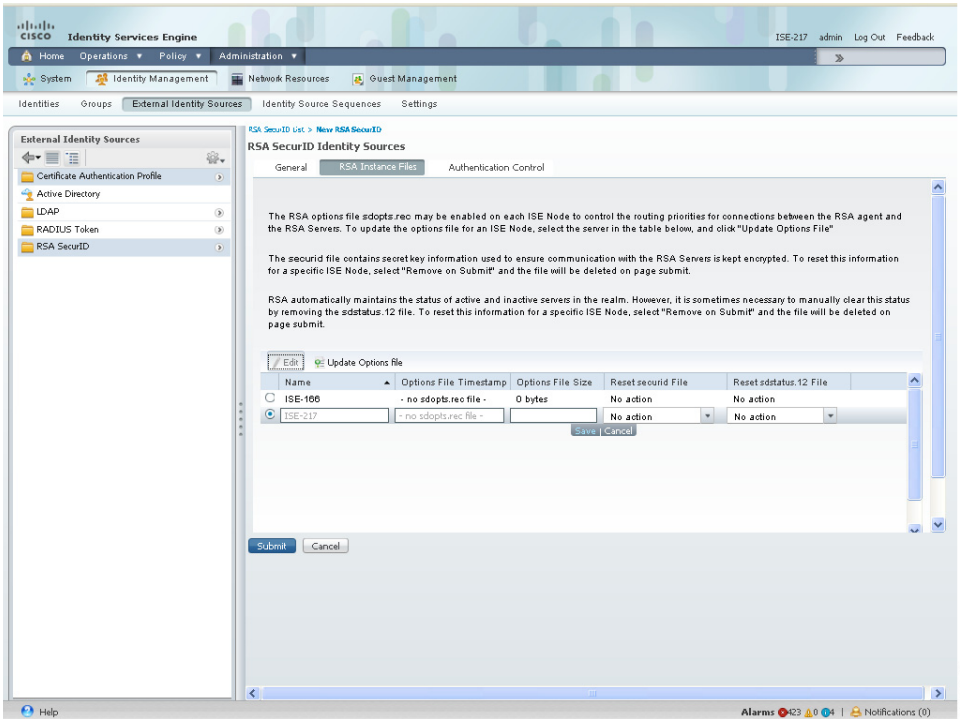
Step 7 Choose one of the following:

- Use the Automatic Load Balancing status maintained by the RSA agent—Choose this option if you want the RSA agent to automatically manage load balancing.
- Override the Automatic Load Balancing status with the sdopts.rec file selected below—Choose this option if you want to manually configure load balancing based on your specific needs. If you choose this option, you must click **Browse** and choose the new sdopts.rec file from the system that is running your client browser.

Step 8 Click **OK**.

Step 9 To reset the securid and sdstatus.12 files for an ISE server, click the row that corresponds to the ISE server. A screen similar to the one shown in Figure 5-19 appears.

Figure 5-19 Resetting securid and sdstatus.12 Files



Step 10 Click the drop-down arrow and choose **Remove on Submit** in the Reset securid File and Reset sdstatus.12 File columns.

Note The Reset sdstatus.12 File field is hidden from your view. Using the vertical and horizontal scroll bars in the innermost frame, scroll down and then to your right to view this field.

Step 11 Click **Save** in this row to save the changes.

Step 12 Click **Save** to save the configuration.

Configuring Authentication Control Options

You can use this page to specify how ISE defines authentication failures and to enable identity caching. The RSA identity source does not differentiate between “Authentication failed” and “User not found” errors and sends an Access-Reject response.

You can define how such failures should be handled by ISE for processing requests and for reporting failures. Identity caching enables ISE to process requests that fail to authenticate against the ISE server a second time. The results and the attributes retrieved from the previous authentication are available in the cache.

To configure authentication control options, complete the following steps:

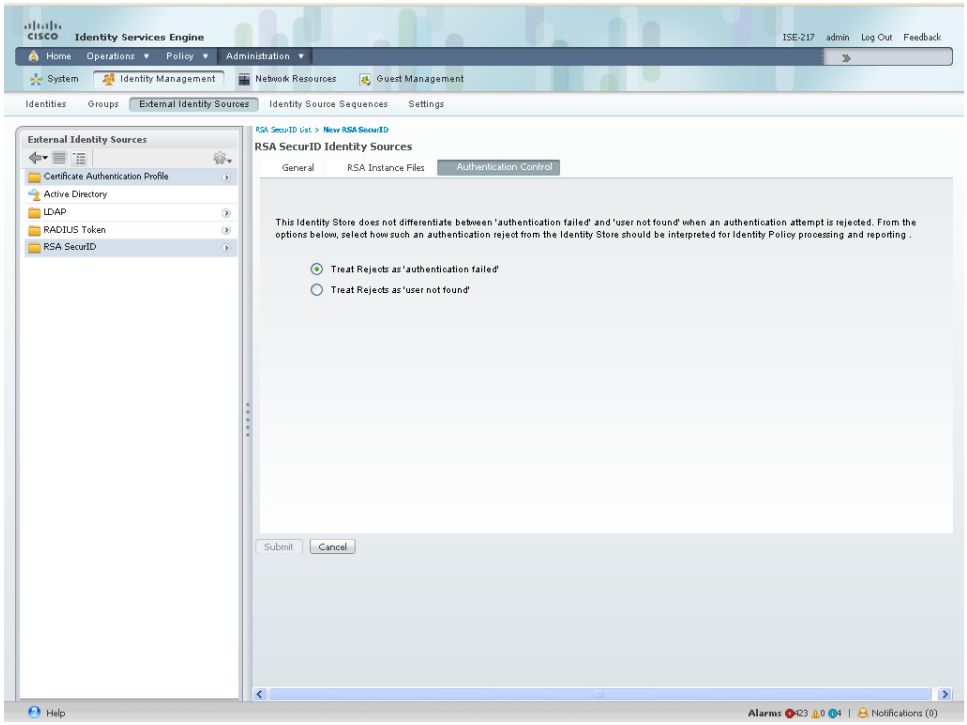
Step 1 Choose **Administration > Identity Management > External Identity Sources > RSA SecurID**.

Step 2 Click **Add** to add an RSA identity source or check the check box next to the RSA identity source that you want to edit, and then click **Edit** or click **Duplicate** to duplicate an existing RSA identity source entry.

Step 3 Click the **Authentication Control** tab.

The Authentication Control tab appears as shown in Figure 5-20.

Figure 5-20 Authentication Control Tab



Step 4 Choose one of the following:

- Treat Rejects as “authentication failed”—Choose this option if you want the rejected requests to be treated as failed authentications.
- Treat Rejects as “user not found”—Choose this option if you want the rejected requests to be treated as user not found errors.

Step 5 Click **Save** to save the configuration.

Next Steps:

1. See Chapter 16, “Managing Authentication Policies” for information on how to create authentication policies.
2. See Chapter 17, “Managing Authorization Policies and Profiles” for information on how to create authorization profiles and policies.

For more information:

- RSA Identity Sources, page 5-39
- Configuring RSA Prompts, page 5-48
- Configuring RSA Messages, page 5-49

Configuring RSA Prompts

ISE allows you to configure RSA prompts that will be presented to the user while processing requests to the RSA SecurID server.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure the RSA prompts, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

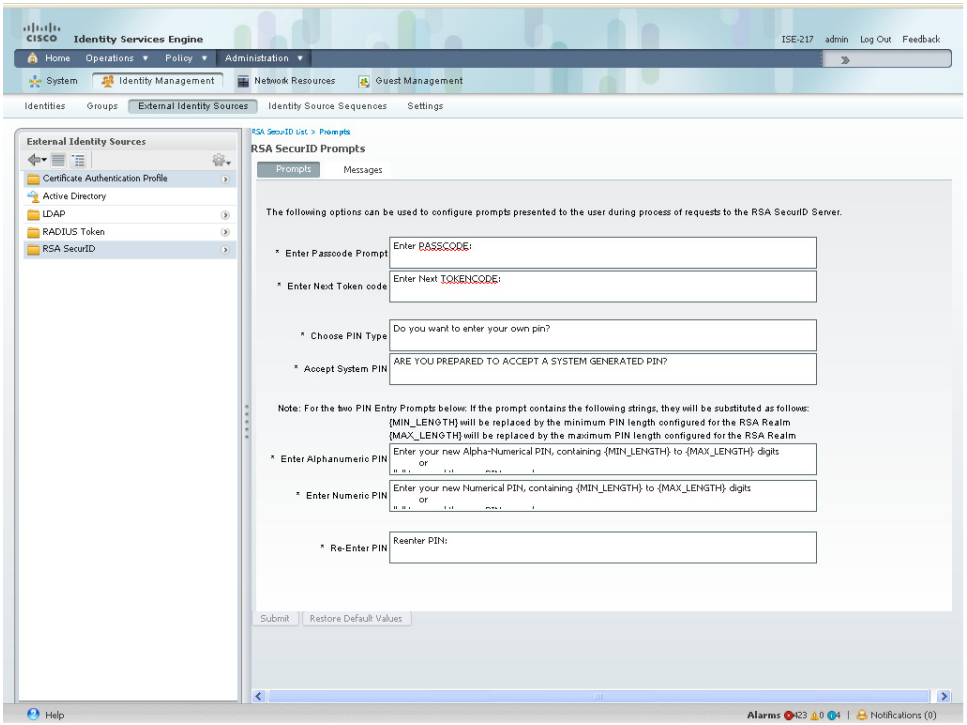
Step 2 From the External Identity Sources navigation pane on the left, click **RSA SecurID**.

The RSA SecurID Identity Sources list page appears.

Step 3 Click **Prompts**.

The RSA Prompts page appears with the default prompts as shown in Figure 5-21.

Figure 5-21 RSA Prompts Configuration Page



Step 4 Enter the information as described in Table 5-7.

Step 5 Click **Submit** to save your custom RSA Prompts or click **Reset Default Values** to apply the default RSA prompts.

RSA Prompts

Table 5-7 lists the fields in the RSA prompts tab and their default values.

Table 5-7 RSA Prompts Tab[1]

Option	Description
Enter Passcode Prompt	(Required) This field is a text string that is used to obtain the passcode. The default value is: Enter PASSCODE.
Enter Next Token Code	(Required) This field is a text string that is used to request the next token. The default value is: Enter Next TOKENCODE.
Choose PIN Type	(Required) This field is a text string that is used to request the PIN type. The default value is: Do you want to enter your own pin?
Accept System PIN	(Required) This field is a text string that is used to accept the system-generated PIN. The default value is: ARE YOU PREPARED TO ACCEPT A SYSTEM-GENERATED PIN?
Enter Alphanumeric PIN	This field is a text string that is used to request an alphanumeric PIN. The default value is: Enter your new Alpha-Numerical PIN, containing {MIN_LENGTH} to {MAX_LENGTH} digits\n or\n"x" to cancel the new PIN procedure.
Enter Numeric PIN	(Required) This field is a text string to request a numeric PIN. The default value is: Enter your new Numerical PIN, containing {MIN_LENGTH} to {MAX_LENGTH} digits\n or\n"x" to cancel the new PIN procedure.
Re-enter PIN	(Required) This field is a text string that is used to request the user to re-enter the PIN. The default value is: Reenter PIN.

1. For the prompts, enter a string with a maximum length of 256 characters.

Next Step:

See the "Configuring RSA Messages" section on page 5-49 for the next steps.

Configuring RSA Messages

ISE allows you to configure the messages that are presented to the user while processing requests to the RSA SecurID server.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure the RSA messages, complete the following steps:

Step 1 Choose **Administration > Identity Management > External Identity Sources**.

Step 2 From the External Identity Sources navigation pane on the left, click **RSA SecurID**.

The RSA SecurID Identity Sources list page appears.

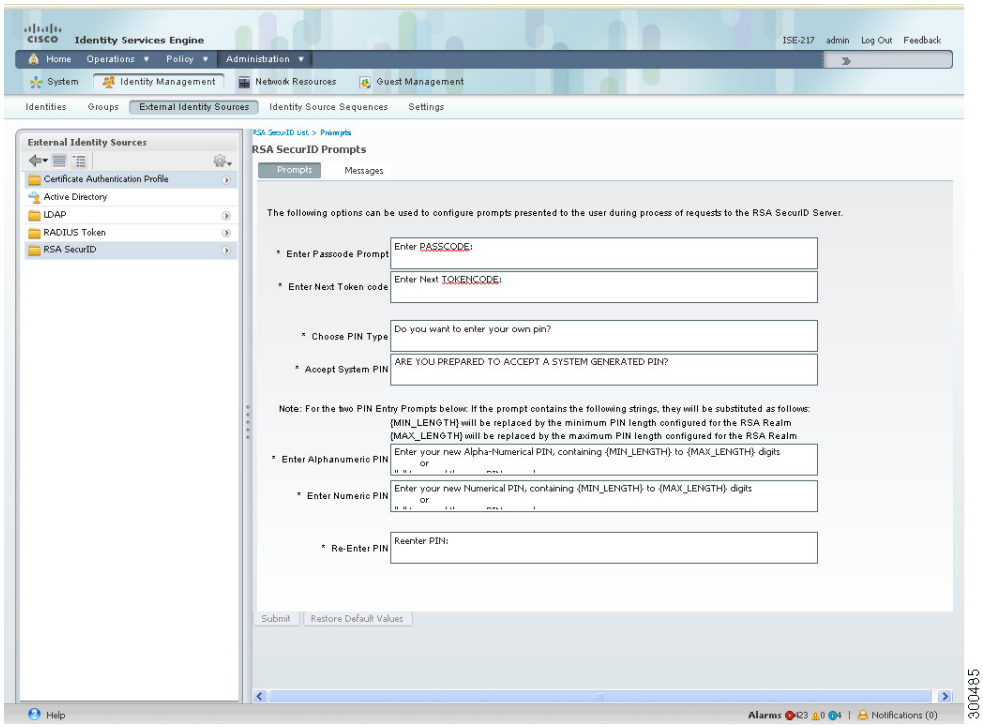
Step 3 Click **Prompts**.

The RSA Prompts page appears.

Step 4 Click the **Messages** tab.

The RSA Messages tab appears as shown in Figure 5-22.

Figure 5-22 RSA Messages Tab



Step 5 Enter the information as described in Table 5-8.

Step 6 Click **Submit** to save your custom RSA messages or click **Reset Default Values** to apply the default RSA messages.

RSA Messages

Table 5-8 lists the fields in the RSA messages tab and their default values.

Table 5-8 RSA Messages Tab

Option	Description
Display System PIN Message	Enter a text string to label the system PIN message. The default is: PIN.
Display System PIN Reminder	Enter a text string to inform the user to remember the new PIN. The default is: Please remember your new PIN, then press Return to continue.
Must Enter Numeric Error	Enter a message that instructs users to enter only numbers for the PIN. The default is: PIN must only contain numbers.
Must Enter Alpha Error	Enter a message that instructs users to enter only alphanumeric characters for PINs. The default is: PIN must only contain alphanumeric characters.
PIN Accepted Message	Enter a message that the users see when their PIN is accepted by the system. The default is: PIN accepted, wait for next card code before trying again.
PIN Rejected Message	Enter a message that the users see when the system rejects their PIN. The default is: PIN rejected.
User Pins Differ Error	Enter a message that the users see when they enter an incorrect PIN. The default is: PINs differ, not changed.
System PIN Accepted Message	Enter a message that the users see when the system accepts their PIN. The default is: Wait for next card code before trying again.
Bad Password Length Error	Enter a message that the users see when the PIN that they specify does not fall within the range specified in the PIN length policy. The default is: PIN must be between *minimum length* and *maximum length* characters.

Identity Source Sequences

Identity source sequences define the order in which ISE will look for user credentials in the different databases. ISE supports the following databases:

- Internal Users
- Internal Endpoints
- Active Directory
- LDAP
- RSA
- RADIUS Token Servers
- Certificate Authentication Profiles

If you have your user information in more than one of these databases that are connected to your ISE, you can define the order in which you want ISE to look for user information in these databases. Once a match is found, ISE does not look any further, but evaluates the credentials, and returns the result to the user. This policy is the first match policy.

This section contains the following topics:

- Creating Identity Source Sequences, page 5-52
- Deleting Identity Source Sequences, page 5-53

Creating Identity Source Sequences

Prerequisites:

1. Ensure that you have configured your external identity sources in ISE. See the "Identity Source Sequences" section on page 5-51 for information on how to configure external identity sources.
2. Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To define an identity source sequence, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identity Source Sequences**.

The Identity Source Sequences page appears with a list of identity source sequences that you have defined.

Step 2 Click **Add** to add an identity source sequence. You can check the check box next to an identity source sequence and click **Edit** or **Duplicate** to edit or duplicate it.

Step 3 Enter a name for the identity source sequence. You can also enter an optional description.

Step 4 In the Certificate-Based Authentication area, check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile from the drop-down list box, if you wish to use a certificate authentication profile for authentication.

Step 5 In the Authentication Search List area, the Available list box lists a set of databases that are connected to ISE. Choose a database that you want to include in the identity source sequence and click the > button to move it to the Selected list box. You can add more databases to the Selected list box if you want. You can click the >> button to move all the databases from the Available list to the Selected list.

Step 6 You can rearrange the databases in the Selected list using the move up (^) or move down (v) buttons.

Step 7 In the Advanced Search List area, choose one of the following options:

- Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError—Click this radio button if you want ISE to discontinue the search, if the user is not found in the first selected identity source.
- Treat as if the user was not found and proceed to the next store in the sequence—Click this radio button if you want ISE to continue searching the other selected identity sources in sequence, if the user is not found in the first selected identity source.

Step 8 After you have the correct sequence of databases in the Selected list, click **Submit** to create the identity source sequence that you can then use in policies.

Note While processing a request, ISE will search these identity sources in sequence. Ensure that you have the identity sources in the Selected list box listed in the order in which you want ISE to search the identity sources.

Note For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest Portal authentication source and the identity source sequence to contain the same identity stores. See "Specifying an Authentication Source" section on page 21-29 for more information on how to configure Guest Portal authentication source.

Next Steps:

See the "Configuring the Simple Authentication Policy" section on page 16-26 and the "Configuring the Rule-Based Authentication Policy" section on page 16-29 for information on how to use the identity source sequence in authentication policies.

Deleting Identity Source Sequences

Prerequisite:

1. Ensure that the identity source sequence that you are about to delete is not used in any authentication policies.
2. Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete an identity source sequence, complete the following steps:

Step 1 Choose **Administration > Identity Management > Identity Source Sequences**.

The Identity Source Sequences page appears with a list of identity source sequences that you have defined.

Step 2 Check the check box next to the identity source sequence or sequences that you want to delete, then click **Delete**.

Note An identity source sequence that is referenced in an authentication policy cannot be deleted. If you have selected multiple identity source sequences to be deleted and if one of the selected identity source sequence is referenced in an authentication policy, then the delete operation will fail.

The following message appears:

"Are you sure you want to delete?"

Step 3 Click **OK** to delete the identity source sequence or sequences.

Viewing and Monitoring the Identity Sources

ISE provides information about the identity sources through the following:

- ISE Dashboard, page 5-54
- Live Authentications, page 5-55
- Reports, page 5-56

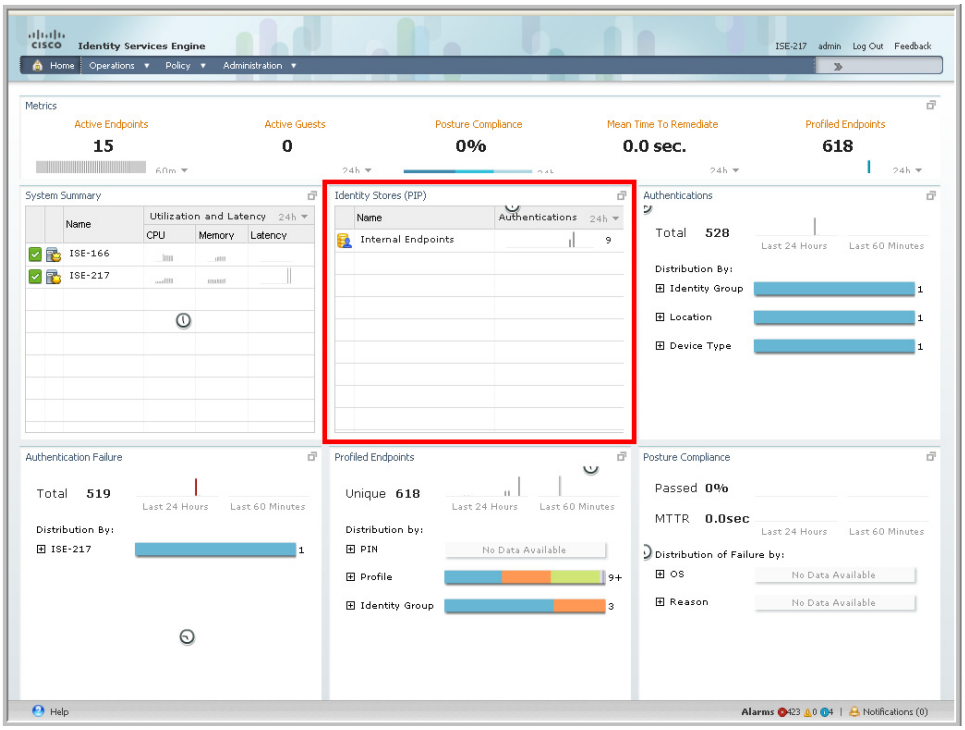
Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To view the reports in ISE, you must have one of the following roles assigned: Super Admin or Helpdesk Admin or Monitoring Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

ISE Dashboard

ISE provides an at-a-glance view of identity source-related information in a dashlet that appears on the ISE dashboard. Figure 5-23 shows the ISE dashboard and the Identity Sources dashlet that provides statistical data.

Figure 5-23 ISE Dashboard



Click the icon in the Identity Sources dashlet to view the details in a new window. You can drill down further for granular information.

For more information on the ISE dashboard and how to work with it, see the "Cisco ISE Dashboard Monitoring" section on page 23-3.

Live Authentications

From the Live Authentications page, you can drill down to find more information including failure reasons.

Figure 5-24 shows the live authentications page and highlights the magnifier icon that you must click to drill down for details.

Figure 5-24 Live Authentications Page

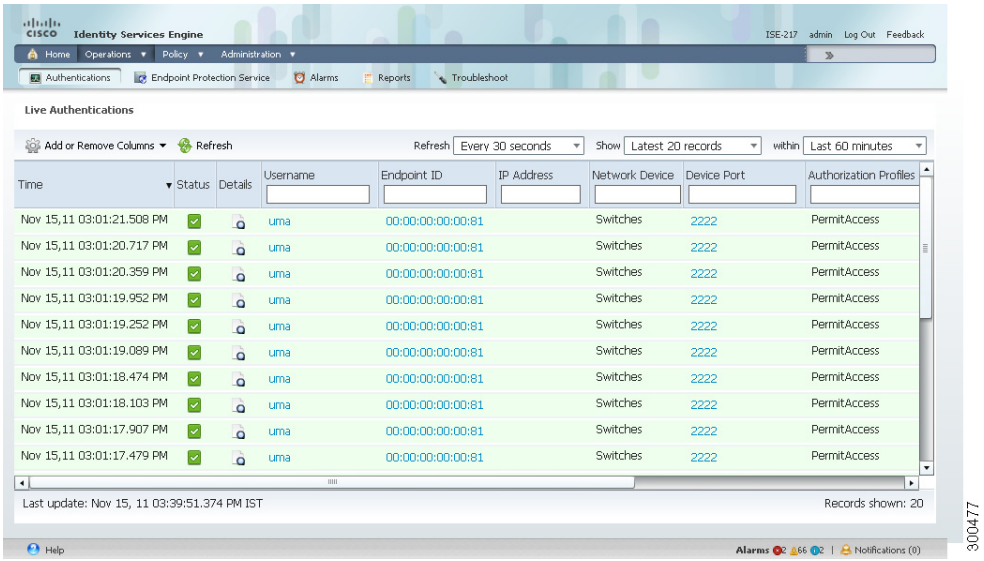
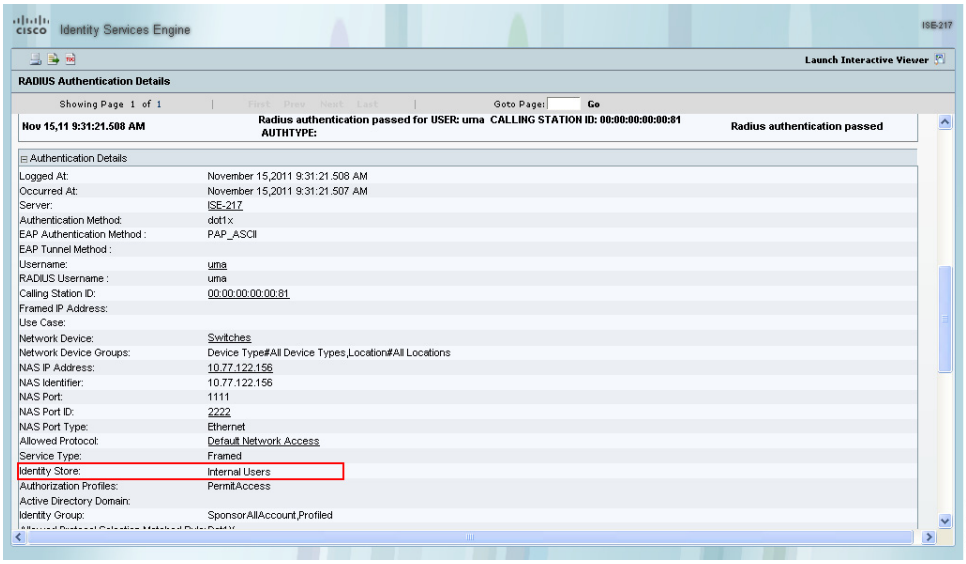


Figure 5-25 shows the drill-down view that identifies the identity source that was used for authentication.

Figure 5-25 Drill-Down View of Live Authentications Page



For more information on the Live Authentications page, see the "Monitoring Live Authentications" section on page 23-25.

Reports

ISE provides various reports that include information about identity sources. Authentication, authentication summary, and top N reports allow you to query for information based on identity sources. Table 5-9 provides a list of reports that allow you to run a query and generate a report based on identity sources.

Table 5-9 Identity Source Information in Reports

Type of Report	Report Name
AAA Protocol	Authentication Trend
	RADIUS Authentication
Allowed Protocol	Allowed Protocol Authentication Summary
	Top N Authentications By Allowed Protocol
Server Instance	Server Authentication Summary
	Top N Authentications By Server
Endpoint	Endpoint MAC Authentication Summary
	Top N Authentications By MAC Address
	Top N Authentications By Machine
Failure Reason	Failure Reason Authentication Summary
	Top N Authentications By Failure Reason
Network Device	Network Device Authentication Summary
	Top N Authentications By Network Device

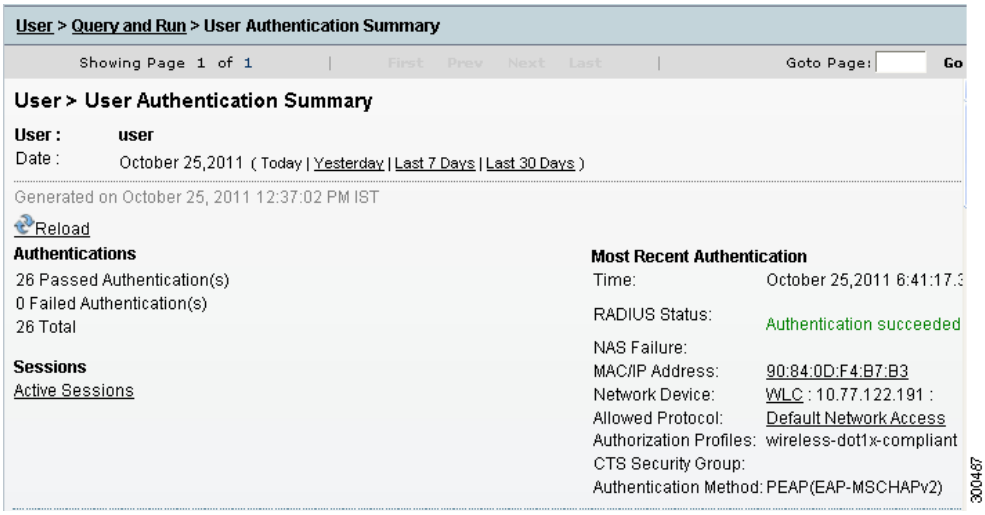
Table 5-9 Identity Source Information in Reports (continued)

Type of Report	Report Name
User	Top N Authentications By User
	User Authentication Summary

See the "Available Reports" section on page 24-42 for a description of these reports.

To run a query and generate a report, for example, the User Authentication Summary report, go to **Operations > Reports > Catalog**. Click **User** from the type of reports that are listed in the left pane. Click the **User Authentication Summary** radio button and choose **Run > Query And Run**. Enter the username and any other search criteria that you want to use to run the report and click **Run**. A report that is similar to the one that is shown in Figure 5-26 appears.

Figure 5-26 User Authentication Summary Report



You can run any of the reports listed in Table 5-9 for information on authentication, authentication summary, or top N details based on identity sources.

For information on how to run, view, navigate, customize, export, and print these reports, see the following sections:

- Running, Viewing, and Navigating Reports, page 24-3
- Accessing Catalog Reports, page 24-6
- Exporting and Printing Reports, page 24-4



CHAPTER 6

Managing Network Devices

This chapter describes how to manage the devices in your network. This chapter contains the following sections:

- Managing Network Devices, page 6-1
- Managing Network Device Groups, page 6-10
- Importing Network Devices and Network Device Groups, page 6-14
- Exporting Network Devices and Network Device Groups, page 6-21

Managing Network Devices

A network device is an authentication, authorization, and accounting (AAA) client through which AAA service requests are attempted, for example, switches, routers, and so on. The network device definition enables the Cisco Identity Services Engine (ISE) to interact with the network devices that are configured. A network device that is not defined in ISE cannot receive AAA services from ISE.

You can also define a default network device that ISE can use if it does not find the device definition for a particular IP address. ISE supports the default device definition for RADIUS authentications. This feature enables you to define a default RADIUS shared secret and level of access for newly provisioned devices.

When ISE receives a RADIUS request from a network device, it looks for the corresponding device definition to retrieve the shared secret that is configured. If it finds the device definition, it obtains the shared secret that is configured on the device and matches it against the shared secret in the request to authenticate access. If it does not find the device definition, it obtains the shared secret from the default network device and processes the request. If the shared secrets match, network access is granted. A passed authentication report is generated. If they do not match, a reject response is sent to the device. A failed authentication report is generated, which provides the failure reason.

ISE allows you to configure authentication and authorization policies based on device attributes such as device type, location, model name, and so on, which are available in the device dictionary. When you create a new network device group (NDG), a new device attribute is added to the dictionary, which you can use in policy definitions.

The network device definition must include the following:

- Device Name—The device name is a descriptive name that you can provide to the network device. It can be different from the hostname of the device. The device name is a logical identifier.
- IP Address and Subnet Mask—You must specify an IP address and a subnet mask. The following are some guidelines that must be followed while defining the IP addresses and subnet masks:
  - You can define a specific IP address, or a range with a subnet mask.
  - You cannot define two devices with the same specific IP addresses.
  - You cannot define two devices with the same IP range. The IP ranges must not overlap either partially or completely.

Note If device A has an IP address range defined, you can configure another device B with an individual address from the range that is defined in device A.

When ISE receives a RADIUS request and tries to match the request against a network device, it does the following:

a. It looks for a specific IP address that matches the one in the request.
b. It looks up the ranges to see if the IP address in the request falls within the range that is specified.
c. If both of these fail, it uses the default device definition (if defined) to process the request.

- Network Device Group—NDGs allow you to group devices based on location, type, and other groupings and allow you to define policy conditions based on these groupings. If you do not specifically assign a device to a group when you configure it, it becomes a part of the default All Locations and All Device Types device groups. See the "Managing Network Device Groups" section on page 6-10 for more information.

The following are optional settings that you can define for a network device:

- Model Name—The model name identifies the model of the network device. For example, CAT 6K, Nexus 7K, and so on. You can use the model name as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
- Software Version—The version of the software that is running on the network device. For example, Cisco IOS version 12.3, 12.3 (2), and so on. You can use the software version as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.

In addition, you can configure the following settings for network devices:

- Authentication Settings—Configure this setting for RADIUS authentications.
- Simple Network Management Protocol (SNMP) Settings—Configure this setting for the Profiler service in ISE to profile the end points. The ISE Profiler service can communicate with network devices that have SNMP settings defined. The Profiler service uses these settings to initiate SNMP-based communication with the device and obtains device-related information for monitoring purposes.
- Security Group Access (SGA) Settings—For devices that can be part of the Cisco Security Group Access solution. Any switch that supports the SGA solution is an SGA device. For example, the Nexus 7000 Series Switches, Catalyst 6000 Series Switches, Catalyst 4000 Series Switches, Catalyst 3000 Series Switches, and so on. SGA devices are authenticated using the SGA settings that you must define while adding SGA devices. See Chapter 22, "Configuring Cisco Security Group Access Policies" for more information on SGA settings.

You can also generate SGA PAC (Protected Access Credentials) by clicking the **Generate PAC** button. See the "Generating an SGA PAC from the Network Devices List Screen" section on page 22-33 for more information.

- Device Configuration Details—Credentials to edit the configuration of a network device.

You can configure these network devices manually or import a list of devices into ISE using a .csv file.

This section contains the following topics:

- Adding and Editing Devices, page 6-3
- Deleting a Device, page 6-6
- Filtering Network Devices on the Network Devices Page, page 6-7
- Configuring a Default Device, page 6-9
- Importing Network Devices and Network Device Groups, page 6-14
- Exporting Network Devices and Network Device Groups, page 6-21

Adding and Editing Devices

You can add devices or edit the device definition in the ISE server.

Prerequisites:

- Before you begin this task, you should have a basic understanding of network devices and how they are managed in ISE. See the "Managing Network Devices" section on page 6-1 for more information.
- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To add or edit a device, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears with a list of configured devices.

Step 3 Click **Add**, or check the check box next to a device and click **Edit** to edit it or click **Duplicate** to create a duplicate entry. You can alternatively click **Add new device** from the action icon on the Network Devices navigation pane or click a device name from the list to edit it.

Step 4 In the right pane, enter the values as described in Table 6-1.

Step 5 Check the **Authentication Settings** check box and define the following RADIUS authentication settings:

- Shared Secret—The shared secret can be up to 128 characters in length. The shared secret is the key that you have configured on the device using the **radius-host** command with the **pac** option.
- Enable KeyWrap—This option increases RADIUS protocol security via an AES KeyWrap algorithm to help enable FIPS 140-2 compliance in Cisco ISE.
- Key Encryption Key—This key is used for session encryption (secrecy).

- Message Authenticator Code Key—This key is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
- Key Input Format—Specify the format you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that available on the WLAN controller. (The value you specify must be the correct [full] length for the key as defined below; shorter values are not permitted.)
  - ASCII—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.
  - Hexadecimal—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.

Step 6 Check the **SNMP** check box to configure SNMP settings on the device. These settings are used by the Profiler service in ISE. Enter the values as described in Table 6-2.

For information on switch-related SNMP settings, see:

- Enable SNMP Traps, page C-8
- Enable SNMP v3 Query for Profiling, page C-8

Step 7 Check the **Security Group Access (SGA)** check box to configure an SGA device. SGA devices do not use the IP address. Instead, you must define other settings so that SGA devices can communicate with ISE. Enter the values as described in Table 22-4.

Step 8 Check the **Device Configuration Deployment** check box to enter user credentials to edit the configuration of the device. Enter the values as described in Table 6-3.

Step 9 Click **Submit** to save the device definition.

Network Devices Page

Table 6-1 lists the fields in the Network Devices page and their descriptions.

Table 6-1 Network Devices Page

Field	Description
Name	(Required) This field is the name of the device. **Note** You cannot edit the name of a device.
Description	This field is the description of the device.
IP Address	(Required) This field includes the IP address and subnet masks that are associated with the device. A single address or a range, the routable IP address should be one with which the ISE appliance can communicate.
Model Name	This field is the device model, for example, the Cisco Catalyst 6K, the Cisco Nexus 7K, and so on.
Software Version	This field is the version of the software on the device, for example, Version 12.2, 12.3, and so on.
Network Device Group	(Required) From the Location and Device Type drop-down list boxes, choose a location and device type to associate with the device. **Note** If you do not choose a device group, the default device groups (root NDGs) are assigned.

Network Devices: SNMP Settings

Table 6-2 lists the SNMP settings in the Network Devices page and their descriptions.

Table 6-2 Network Devices List Page: SNMP Settings

Field	Description
SNMP Version	(Required) This setting is the version of SNMP to be used for requests. Valid options are: • 1—SNMPv1 does not support informs. • 2c • 3—SNMPv3 is the most secure model because it allows packet encryption when you choose the Priv security level. **Note** If you have configured your network device with SNMPv3 parameters, you cannot generate the Network Device Session Status Summary report that is provided by the Monitoring service (**Operations > Reports > Catalog > Network Device > Session Status Summary**). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.
SNMP RO Community	(Required if you choose SNMP version 1 or 2c) This setting is the Read Only community string. A community string is similar to a password and it provides ISE with a particular type of access to the device.
SNMP Username	(Required if you choose SNMP version 3) This setting is the SNMPv3 username.
Security Level	(Required if you choose SNMP version 3) Choose the security level for SNMPv3. Valid options are the following: • Auth—Enables MD5[1] or Secure Hash Algorithm (SHA) packet authentication • No Auth—No authentication and no privacy security level • Priv—Enables DES[2] packet encryption
Auth Protocol	This setting is the authentication protocol that you want the device to use. Valid options are MD5 or SHA1.
Auth Password	Enter the authentication key. The authentication key must be at least 8 characters in length.
Privacy Protocol	This setting is the privacy protocol that you want the device to use. Valid options are DES, AES128, AES192, AES256, and 3DES.
Privacy Password	Enter the privacy key.
Polling Interval	This setting is the SNMP polling interval in seconds. Default is 3600 seconds.
Link Trap Query	Check this check box for the profiler service to query the device, if it receives the link trap from the NAD[3] connected to the device.

Table 6-2 Network Devices List Page: SNMP Settings (continued)

Field	Description
MAC Trap Query	Check this check box for the profiler service to query the device, if it receives the MAC trap from the NAD connected to the device.
Originating Policy Services Node	This setting indicates which server to use to poll for SNMP data. By default, it is automatic, but you can overwrite the setting by assigning different values.

1. MD5 = Message Digest 5.
2. DES = Data Encryption Standard.
3. NAD = Network Access Device

Network Devices: Device Configuration Deployment Settings

Table 6-3 Network Devices Page: Device Configuration Deployment Settings

Field	Description
Exec Mode Username	Enter the username that has privileges to edit the device configuration.
Exec Mode Password	Enter the device password.
Enable Mode Password	Enter the enable password for the device that would allow you to edit its configuration.

For more information:

- Managing Network Devices, page 6-1
- Managing Network Device Groups, page 6-10
- Importing Network Devices and Network Device Groups, page 6-14
- Exporting Network Devices and Network Device Groups, page 6-21

Deleting a Device

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete network devices, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices List page appears.

Step 3 Check the check boxes next to the devices that you want to delete and click **Delete > Delete Selected**. You can alternatively choose the network device listed in the navigation pane on the left and from the action icon ( ), and click **Delete device**.

Note You can click Delete > Delete All to delete all the devices that you have defined.

A dialog box appears with the following message:

Are you sure you want to delete "*Device name*"?

Step 4 Click **OK** to delete the device.

Filtering Network Devices on the Network Devices Page

You can use the Show drop-down list, or click the filter icon to both invoke a quick filter and close it on the Network Devices page. A quick filter is a simple filter that you can use to filter network devices based on field descriptions, such as the name of network devices, description, location, type, and an IP/Mask on the Network Devices page. Filtering network devices by a single IP address is an exclusive filter that disables all other filter fields in the quick filter.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, on the Network Devices page. The advanced filter filters network devices based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter. Filtering network devices by a single IP address is an exclusive filter and no other fields can be simultaneously used for filtering in the advanced filter.

You can use the Manage Preset Filters option, which lists all the preset filters. This option allows you to manage preset filters. Once you have created and saved, you can choose a preset filter from the list of filtered results on the Network Devices page. A preset filter has a session lifetime, which displays the filtered results on the Network Devices page. You can also edit preset filters and remove them from the preset filters list.

To filter network devices, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices** (menu window).

The Network Devices menu appears.

Step 2 From the Network Devices menu window, choose **Network Devices**.

The Network Devices page appears, which lists all the network devices.

Step 3 From the Network Devices page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 6-4.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 6-8 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 6-8.

Note To return to the network devices list, choose **All** from the Show drop-down list to display all the network devices without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters network devices based on each field description except the IP/Mask field on the Network devices page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Network Devices page. If you clear the field, it displays the list of all the network devices on the Network devices page. Filtering by IP/Mask disables all other fields in the quick filter.

Step 1 To filter, click the **Go** button within each field to refresh the page with the results that are displayed on the Network Devices page.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter network devices by using variables that are more complex. It contains one or more filters that filter network devices based on the values that match the field descriptions. A filter on a single row filters network devices based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter network devices by using any one or all of the filters within a single advanced filter. Filtering by IP/Mask disables filtering with all other fields simultaneously in the advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

If IP/Mask is selected, then no other filters can be used for simultaneous filtering in the advanced filter.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save.** Do not include spaces when creating the name for a preset filter. Click **Cancel** to clear the filter without saving the current filter.

Table 6-4 describes the fields that allow you to filter the network devices on the Network Devices page.

Table 6-4 Filtering Network Devices

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter network devices by the name of the network device.
	IP/Mask	This field enables you to filter network devices by a single IP address. Filtering by part of an IP address can yield many records, and the results includes all IP addresses with that part of the IP address.
	Location	This field enables you to filter network devices by the location of the network device.
	Type	This field enables you to filter network devices by the type of the network device.
	Description	This field enables you to filter network devices by the description of the network device.
Advanced Filter	Choose the field description from the following: • Name • IP/Mask • Location • Type • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter network devices.
	Value	From the Value field, choose the value for the field description that you selected against which the network devices are filtered.

Configuring a Default Device

You can use the default device definition when no specific device definition is found for a RADIUS request.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To define a default device, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 From the Network Devices navigation pane on the left, click **Default Device**.

The Default Network Device page appears.

Step 3 To enable the default network device definition, choose **Enable** from the Default Network Device Status drop-down list box.

Step 4 Define the following RADIUS authentication settings:

- Shared Secret—The shared secret can be up to 128 characters in length. The shared secret is the key that you have configured on the device using the **radius-host** command with the **pac** option.
- Enable KeyWrap—This option increases RADIUS protocol security via an AES KeyWrap algorithm to help enable FIPS 140-2 compliance in Cisco ISE.
- Key Encryption Key—This key is used for session encryption (secrecy).
- Message Authenticator Code Key—This key is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
- Key Input Format—Specify the format you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that available on the WLAN controller. (The value you specify must be the correct [full] length for the key as defined below; shorter values are not permitted.)
  - ASCII—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.
  - Hexadecimal—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.

Step 5 Click **Save** to save the default network device definition.

Result:

A dialog box appears with the following message:

The configuration was saved successfully.

For more information, see the "Managing Network Devices" section on page 6-1.

Managing Network Device Groups

A device group is a hierarchical structure that contains the network device groups (NDGs). NDGs logically group the devices based on various criteria such as location or device type. When you create a root NDG node, you must provide the name and the type of the NDG. For all subsequent child NDG nodes, you will need to provide only the name. The type is inherited from the parent NDG and hence all the child NDG nodes under a root NDG will be of the same type.

ISE allows you to create hierarchical NDGs. Thus, a device can be part of multiple NDGs. For example, you can group devices by continent, region, and country such as the following:

- Africa -> Southern -> Namibia
- Africa -> Southern -> South Africa
- Africa -> Southern -> Botswana

You can also group devices by device types such as the following:

- Africa -> Southern -> Botswana -> Firewalls
- Africa -> Southern -> Botswana -> Routers

- Africa -> Southern -> Botswana -> Switches

You can use NDGs in policy conditions. There are two predefined root NDGs in ISE (Location and Device Type). You cannot edit or delete these predefined NDGs. Devices can be assigned to a single NDG. After you create an NDG, you can use it while defining policies. When you create a new root NDG, a new device attribute is added to the dictionary. You can use this attribute in authentication and authorization policies.

Note The device type of the root NDG is available as an attribute in the device dictionary. You can define conditions based on this attribute. The name of the NDG is one of the values that this attribute can take.

This section contains the following topics:

- Creating a Network Device Group, page 6-11
- Editing a Network Device Group, page 6-12
- Deleting a Network Device Group, page 6-13
- Import Network Device Groups into ISE, page 6-19
- Exporting Network Device Groups, page 6-22

Creating a Network Device Group

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create an NDG, complete the following steps:

Note Default NDGs (All Locations and All Device Types) cannot be edited, but you can add new device subgroups under them.

Step 1 Choose **Administration > Network Resources > Network Device Groups**.

From the Network Device Groups navigation pane on the left, click **Group Types**.

The Network Device Groups page appears.

Step 2 Do one of the following:

- To create a root NDG, click **Add**.
- To create a child NDG, from the navigation pane on the left, choose a group to which you want to add a child NDG, and click **Add**.

Step 3 In the right-side pane, enter the following information:

- (Required) Name of the NDG. This name appears in the navigation pane.

  The full name of an NDG can have a maximum of 100 characters. For example, if you are creating a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you are creating would be Global#Asia#India and this full name should not exceed 100 characters. If the full name of the NDG exceeds 100 characters, the NDG creation fails.

- An optional description.
- (Required) Type of NDG. If this NDG is a root NDG, then this device type will be available as an attribute in the device dictionary. If this NDG is a child NDG, then the name of the parent NDG should appear in this field.

Step 4 Click **Save** to save the NDG configuration.

Result:

On successful creation of the NDG, a pop-up appears at the right bottom corner of your screen with the following message: *NDG_name* has been saved successfully.

Related Topics

- Managing Network Devices, page 6-1
- Editing a Network Device Group, page 6-12
- Deleting a Network Device Group, page 6-13

Editing a Network Device Group

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To edit an NDG, complete the following steps:

Note You cannot edit the predefined Location and Device Type NDGs.

Step 1 Choose **Administration > Network Resources > Network Device Groups**.

Step 2 From the navigation pane on the left, click **Group Types**.

The Network Device Groups listing page appears.

Step 3 From the Group Types navigation pane on the left, choose the parent NDG whose child NDG you want to edit.

The Network Device Group listing page appears with a list of child NDGs.

Step 4 Check the check box next to the NDG that you want to edit and click **Edit**.

Step 5 Edit the NDG name or description or both.

You cannot edit the NDG type.

Step 6 Click **Save** to save the changes.

Result:

On successful completion of the edit process, a pop-up appears at the right bottom corner of your screen with the following message: *NDG_name* has been saved successfully.

Related Topics

- Managing Network Devices, page 6-1
- Creating a Network Device Group, page 6-11
- Deleting a Network Device Group, page 6-13

Deleting a Network Device Group

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete an NDG, complete the following steps:

Note You cannot delete an NDG that has a subgroup under it.

Step 1 Choose **Administration > Network Resources > Network Device Groups**.

Step 2 From the navigation pane on the left, click **Group Types**.

The Network Device Groups listing page appears.

Step 3 From the Group Types navigation pane on the left, choose the parent NDG whose child NDG you want to delete.

The Network Device Group listing page appears with a list of child NDGs.

Step 4 Check the check box next to the NDG that you want to delete and click **Delete**. Alternatively, you can choose the child NDG that you want to delete from the navigation pane on the left and click **Delete Group** from the action icon.

A dialog box appears with the following message:

Are you sure you want to delete?

Step 5 Click **OK** to delete the NDG.

Result:

On successful completion of the delete process, a pop-up appears at the right bottom corner of your screen with the following message: Group was deleted successfully.

Related Topics

- Managing Network Devices, page 6-1
- Creating a Network Device Group, page 6-11

- Editing a Network Device Group, page 6-12

Importing Network Devices and Network Device Groups

ISE allows you to import a large number of network devices and network device groups using comma-separated value (.csv) files. While importing devices and device groups, you can create new records or update existing records. You can download the .csv import template from the ISE user interface, enter your device or device group details in the template, and save it as a .csv file, which you can then import back into ISE. When you configure an import job, you can also define whether you want ISE to overwrite the existing device definitions with the new definitions or stop the import process when it encounters the first error.

After an import job has begun, you can view the status of the job in the ISE user interface. You cannot run two import jobs of the same resource type at the same time. For example, you cannot concurrently run two import jobs to import network devices from two different import files.

To import devices into ISE, you must complete the following tasks:

1. Download the Import File Template, page 6-14
2. Create the CSV Import File, page 6-15
3. Import Devices into ISE, page 6-18 or Import Network Device Groups into ISE, page 6-19

Download the Import File Template

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To download the import file template, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears.

Note If you want to download the template for Network Device Groups, then choose **Administration > Network Resources > Network Device Groups** and from the navigation pane on the left, and click **Group Types**.

Step 3 Click **Import**.

The Import page appears.

Step 4 Click **Generate a Template**.

Step 5 Save the template file to your local hard disk.

Result:

The template is downloaded to your local hard disk.

Create the CSV Import File

You must first create the CSV import file before you can import it into ISE.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create the CSV import file, complete the following steps:

Step 1 Open the CSV template that you downloaded using Microsoft Excel or any spreadsheet application.

The first line in your CSV template is the header and it defines the format of the fields in the file. This header should not be edited and should be used as is.

- Table 6-5 lists the fields in the header and provides a description of the fields in the Network Device CSV file template.
- Table 6-6 lists the fields in the header and provides a description of these fields in the Network Device Group CSV file template.

Step 2 Enter the data for your network devices as shown in Figure 6-1 or network device groups as shown in Figure 6-2.

Figure 6-1 Sample CSV File for Importing Network Devices

	A	B	C	D	E	F	G	H
1	Name	Descriptic	IP Addres	Model	Software '	Network Dev	Authentic	Authentic
2	device_1	This is Dev	64.103.172	2700	2700	All Locations	RADIUS	cisco123
3	Test_01	This is Dev	10.10.0.01	1801A	13.01.01.0	All Locations	RADIUS	cisco001
4	Test_02	This is Dev	10.10.0.02	1802A	13.01.01.0	All Locations	RADIUS	cisco002
5	Test_03	This is Dev	10.10.0.03	1801A	13.01.01.0	All Locations	RADIUS	cisco003
6	Test_04	This is Dev	10.10.0.04	1802A	13.01.01.0	All Locations	RADIUS	cisco004
7	Test_05	This is Dev	10.10.0.05	1801A	13.01.01.0	All Locations	RADIUS	cisco005
8	Test_06	This is Dev	10.10.0.06	1802A	13.01.01.0	All Locations	RADIUS	cisco006
9	Test_07	This is Dev	10.10.0.07	1801A	13.01.01.0	All Locations	RADIUS	cisco007
10	Test_08	This is Dev	10.10.0.08	1802A	13.01.01.0	All Locations	RADIUS	cisco008
11	Test_09	This is Dev	10.10.0.09	1801A	13.01.01.0	All Locations	RADIUS	cisco009
12	Test_10	This is Dev	10.10.0.10	1802A	13.01.01.1	All Locations	RADIUS	cisco010
13	Test_11	This is Dev	10.10.0.11	1801A	13.01.01.1	All Locations	RADIUS	cisco011
14	Test_12	This is Dev	10.10.0.12	1802A	13.01.01.1	All Locations	RADIUS	cisco012
15	Test_13	This is Dev	10.10.0.13	1801A	13.01.01.1	All Locations	RADIUS	cisco013
16	Test_14	This is Dev	10.10.0.14	1802A	13.01.01.1	All Locations	RADIUS	cisco014
17	Test_15	This is Dev	10.10.0.15	1801A	13.01.01.1	All Locations	RADIUS	cisco015
18	Test_16	This is Dev	10.10.0.16	1802A	13.01.01.1	All Locations	RADIUS	cisco016
19	Test_17	This is Dev	10.10.0.17	1801A	13.01.01.1	All Locations	RADIUS	cisco017
20	Test_18	This is Dev	10.10.0.18	1802A	13.01.01.1	All Locations	RADIUS	cisco018
21	Test_19	This is Dev	10.10.0.19	1801A	13.01.01.1	All Locations	RADIUS	cisco019
22	Test_20	This is Dev	10.10.0.20	1802A	13.01.01.2	All Locations	RADIUS	cisco020

239652

Step 3 Save the .csv file.

Description of the Fields in the Network Device CSV Template

Table 6-5 CSV Template Fields and Description

Field	Description
Name:String(32):Required	(Required) This field is the network device name. It is an alphanumeric string, with a maximum of 32 characters.
Description:String(256)	This field is an optional description for the network device. A string, with a maximum of 256 characters.
IP Address:Subnets(a.b.c.d/m|...):Required	(Required) This field is the IP address and subnet mask of the network device (can take on more than one value separated by a pipe "|" symbol).
Model Name:String(32):Required	(Required) This field is the network device model name. It is a string, with a maximum of 32 characters.
Software Version:String(32):Required	(Required) This field is the network device software version. It is a string, with a maximum of 32 characters.
Network Device Groups:String(100):Required	(Required) This field should be an existing network device group. It can be a subgroup, but must include both the parent and subgroup separated by a space. It is a string, with a maximum of 100 characters, for example, Location#All Location#US
Authentication:Protocol:String(6)	This is an optional field. It is the protocol that you want to use for authentication. The only valid value is RADIUS (not case sensitive).
Authentication:Shared Secret:String(128)	(Required if you have entered a value for the Authentication Protocol field) This is a string, with a maximum of 128 characters.
SNMP:Version:Enumeration(1|2c|3)	This is an optional field, used by the Profiler service. It is the version of the SNMP protocol. Valid values are 1, 2c, or 3.
SNMP:RO Community:String(32)	(Required if you have entered a value for the SNMP Version field) SNMP RO Community. It is a string, with a maximum of 32 characters.
SNMP:RW Community:String(32)	(Required if you have entered a value for the SNMP Version field) SNMP RW Community. It is a string, with a maximum of 32 characters.
SNMP:Username:String(32)	This is an optional field. It is a string, with a maximum of 32 characters.
SNMP:Security Level:Enumeration(Auth|No Auth|Priv)	(Required if you have chosen SNMP version 3) Valid values are Auth, No Auth, Priv.
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	(Required if you have entered Auth or Priv for the SNMP security level) Valid values are MD5 or SHA.
SNMP:Authentication Password:String(32)	(Required if you have entered Auth for the SNMP security level) It is a string, with a maximum of 32 characters.

Table 6-5 CSV Template Fields and Description (continued)

Field	Description
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	(Required if you have entered Priv for the SNMP security level) Valid values are DES, AES128, AES192, AES256, or 3DES.
SNMP:Privacy Password:String(32)	(Required if you have entered Priv for the SNMP security level) It is a string, with a maximum of 32 characters.
SNMP:Polling Interval:Integer:600-86400 seconds	This is an optional field to set the SNMP polling interval. Valid value is an integer between 600 and 86400.
SNMP:Is Link Trap Query:Boolean(true|false)	This is an optional field to enable or disable the SNMP link trap. Valid values are true or false.
SNMP:Is MAC Trap Query:Boolean(true|false)	This is an optional field to enable or disable the SNMP MAC trap. Valid values are true or false.
SGA:Device Id:String(32)	This is an optional field. It is the security group access device ID, and is a string, with a maximum of 32 characters.
SGA:Device Password:String(256)	(Required if you have entered SGA device ID) It is the security group access device password and is a string, with a maximum of 256 characters.
SGA:Environment Data Download Interval:Integer	This is an optional field. It is the security group access environment data download interval. Valid value is an integer between 1 and 24850.
SGA:Peer Authorization Policy Download Interval:Integer	This is an optional field. It is the security group access peer authorization policy download interval. Valid value is an integer between 1 and 24850.
SGA:Reauthentication Interval:Integer	This is an optional field. It is the security group access reauthentication interval. Valid value is an integer between 1 and 24850.
SGA:SGACL List Download Interval:Integer	This is an optional field. It is the security group access SGACL list download interval. Valid value is an integer between 1 and 24850.
SGA:Is Other SGA Devices Trusted:Boolean(true|false)	This is an optional field. Indicates whether security group access is trusted or not. Valid value is true or false.
SGA:Is Device Included on SGT Mapping:Boolean(true|false)	This is an optional field. It is the security group access device included on SGT. Valid value is true or false.
Deployment:Execution Mode Username:String(32)	This is an optional field. It is the username that has privileges to edit the device configuration. It is a string, with a maximum of 32 characters.
Deployment:Execution Mode Password:String(32)	This is an optional field. It is the device password and is a string, with a maximum of 32 characters.
Deployment:Enable Mode Password:String(32)	This is an optional field. It is the enable password of the device that would allow you to edit its configuration and is a string, with a maximum of 32 characters.

For a detailed description of each of these fields, see Table 6-1, Table 6-2, Table 22-4, and Table 6-3.

Result:

You now have the .csv file to begin the import process.

Related Topics

- Importing Network Devices and Network Device Groups, page 6-14
- Import Devices into ISE, page 6-18

Import Devices into ISE

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

After you have created your .csv import file, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears.

Step 3 Click **Import**.

The Import page appears.

Step 4 Click **Browse** to choose the .csv file from the system that is running the client browser.

Step 5 Check or uncheck the following options:

a. Overwrite Existing Data with New Data—Check this check box if you want ISE to replace the existing network devices with the devices in your import file. If you do not check this check box, new network device definitions that are available in the import file are added to the network device repository. Duplicate entries are ignored.

b. Stop Import on First Error—Check this check box if you want ISE to discontinue the import process when it encounters an error in the import process. The records that were processed until that time are imported. If this check box is not checked and an error is encountered, the error is reported and ISE continues the import process.

Step 6 Click **Import**.

The Import Progress window appears and provides the status of the import process. The page appears with a summary of the number of devices that are imported and also reports any errors that were found during the import process.

Step 7 Click **Network Devices** from the navigation pane or the **Network Devices List** link at the top of this screen to view the imported devices.

Result:

On successful completion of the import process, a dialog box appears with the “Import Completed” message.

Import Network Device Groups into ISE

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To import NDGs, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Device Groups**.

Step 2 From the navigation pane on the left, click **Group Types**.

The Network Device Groups page appears.

Step 3 Click **Import**. You can alternatively click **Import** from the action icon on the navigation pane.

The Import page appears.

Step 4 Click **Generate a Template** to download the template for creating the import file.

Step 5 Save the template to your local hard disk.

Step 6 Open this template in Microsoft Excel or any spreadsheet application.

The first line in your CSV template is the header and it defines the format of the fields in the file. This header should not be edited and should be used as is.

Step 7 Enter the details as shown in Figure 6-2.

Figure 6-2 NDG Import File

	A	B	C	D	E	F	G	H
1	Name	Description	Type	Is Root				
2	Location#All Locations	All Locations	Location	TRUE				
3	Device Type#All Device Types	All Device Types	Device Type	TRUE				
4	Location#All Locations#WORLD		Location	FALSE				
5	Location#All Locations#ASIA		Location	FALSE				
6	DeviceGroup1#DeviceGroup1	THIS IS DEVICEGROUP 1	DeviceGroup1	TRUE				
7	DeviceGroup2#DeviceGroup2	THIS IS DEVICEGROUP 2	DeviceGroup2	TRUE				
8	DeviceGroup3#DeviceGroup3	THIS IS DEVICEGROUP 3	DeviceGroup3	TRUE				
9	DeviceGroup4#DeviceGroup4	THIS IS DEVICEGROUP 4	DeviceGroup4	TRUE				
10	DeviceGroup5#DeviceGroup5	THIS IS DEVICEGROUP 5	DeviceGroup5	TRUE				
11	DeviceGroup6#DeviceGroup6	THIS IS DEVICEGROUP 6	DeviceGroup6	TRUE				
12	DeviceGroup7#DeviceGroup7	THIS IS DEVICEGROUP 7	DeviceGroup7	TRUE				
13	DeviceGroup8#DeviceGroup8	THIS IS DEVICEGROUP 8	DeviceGroup8	TRUE				
14	DeviceGroup9#DeviceGroup9	THIS IS DEVICEGROUP 9	DeviceGroup9	TRUE				
15	DeviceGroup10#DeviceGroup10	THIS IS DEVICEGROUP 10	DeviceGroup10	TRUE				
16	DeviceGroup11#DeviceGroup11	THIS IS DEVICEGROUP 11	DeviceGroup11	TRUE				
17	DeviceGroup12#DeviceGroup12	THIS IS DEVICEGROUP 12	DeviceGroup12	TRUE				
18	DeviceGroup13#DeviceGroup13	THIS IS DEVICEGROUP 13	DeviceGroup13	TRUE				
19	DeviceGroup14#DeviceGroup14	THIS IS DEVICEGROUP 14	DeviceGroup14	TRUE				
20	DeviceGroup15#DeviceGroup15	THIS IS DEVICEGROUP 15	DeviceGroup15	TRUE				
21	DeviceGroup16#DeviceGroup16	THIS IS DEVICEGROUP 16	DeviceGroup16	TRUE				
22	DeviceGroup17#DeviceGroup17	THIS IS DEVICEGROUP 17	DeviceGroup17	TRUE				
23	DeviceGroup18#DeviceGroup18	THIS IS DEVICEGROUP 18	DeviceGroup18	TRUE				
24	DeviceGroup19#DeviceGroup19	THIS IS DEVICEGROUP 19	DeviceGroup19	TRUE				
25	DeviceGroup20#DeviceGroup20	THIS IS DEVICEGROUP 20	DeviceGroup20	TRUE				

239651

Step 8 Save the import file to your local hard disk.

Step 9 Click **Browse** from the Import page to choose your import file.

Step 10 Check or uncheck the following options:

a. Overwrite Existing Data with New Data—Check this check box if you want ISE to replace the existing network device groups with the device groups in your import file. If you do not check this check box, new network device group definitions that are available in the import file are added to the network device group repository. Duplicate entries are ignored.

b. Stop Import on First Error—Check this check box if you want ISE to discontinue the import process when it encounters an error in the import process. The records that were processed until that time are imported. If this check box is not checked and an error is encountered, the error is reported and ISE continues the import process.

Step 11 Click **Import**.

The import progress is displayed on the screen and the result appears at the end of the import process.

Description of Fields in the Network Device Groups CSV Template

Table 6-6 Network Device Groups CSV Template Fields

Field	Description
Name:String(100):Required	(Required) This field is the network device group name. It is a string with a maximum of 100 characters. The full name of an NDG can have a maximum of 100 characters. For example, if you are creating a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you are creating would be Global#Asia#India and this full name should not exceed 100 characters. If the full name of the NDG exceeds 100 characters, the NDG creation fails.
Description:String(1024)	This is an optional network device group description. It is a string, with a maximum of 1024 characters.
Type:String(64):Required	(Required) This field is the network device group type. It is a string, with a maximum of 64 characters.
Is Root:Boolean(true|false):Required	(Required) This is a field that determines if the specific network device group is a root group or not. Valid value is true or false.

Related Topics

- Importing Network Devices and Network Device Groups, page 6-14
- Create the CSV Import File, page 6-15

Exporting Network Devices and Network Device Groups

You can export the list of network devices and network device groups configured in Cisco ISE in the form of a .csv file that you can import into another ISE node.

This section contains the following topics:

- Exporting Network Devices, page 6-21
- Exporting Network Device Groups, page 6-22

Exporting Network Devices

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To export the network device configuration, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears with a list of device configurations.

Step 3 Check the check boxes next to the devices that you want to export, and choose **Export > Export Selected**.

Note To export all the network devices that are defined, choose **Export > Export All**.

Step 4 Save the export.csv file to your local hard disk.

Result:

You have your network device configuration in the form of a .csv file that you can import into another ISE node.

Exporting Network Device Groups

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To export network device groups, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Device Groups**.

Step 2 From the navigation pane on the left, click **Group Types**.

The Network Device Groups page appears.

Step 3 Click **Export**. Alternatively, you can click **Export** from the action icon on the navigation pane.

Step 4 Save the export.csv file to your local hard disk.

Result:

You have exported the network device group configuration from an ISE node, which can now be imported into another ISE node.



CHAPTER 7

Managing Resources

This chapter describes how to manage the resources in your Cisco Identity Services Engine (ISE) network. This chapter contains the following topics that provide information and procedures for managing the Cisco ISE network resources:

- Dictionaries and Dictionary Attributes, page 7-1
- Configuring Dictionaries and Dictionary Attributes, page 7-2
- Configuring RADIUS Vendors, page 7-8

Dictionaries and Dictionary Attributes

A dictionary represents a collection of individual parameters for use in configuring vendor-specific attributes. The default supported dictionary and dictionary defaults are those for the IETF RADIUS set of attribute pairs defined by the Internet Engineering Task Force (IETF). When you display the Dictionary page, it lists two types of dictionaries that are supported by Cisco ISE: System and User.

The Cisco ISE system also contains Cisco ISE system-defined dictionaries with dictionary attributes that are read-only attributes. This type of system-defined dictionary is known as a system dictionary. All system-defined attributes are populated during the installation of the Cisco ISE system software. New dictionaries are created when you create any Active Directory or Lightweight Directory Access Protocol (LDAP) server instances.

Note You cannot create, modify, or delete any system-defined values or any attributes in a system dictionary. You can only perform a search using a quick filter that is based on dictionary name and description, or you can perform a more advanced search using an advanced filter search that is based on a search rule you define.

Cisco ISE allows you to create, edit, and delete user-defined dictionaries and dictionary attributes that you can use in policy conditions. This type of user-defined dictionary is known as a user dictionary. The RADIUS protocol supports vendors and vendor attributes. Cisco ISE provides a set of standard IETF RADIUS attributes that are part of the system-defined dictionaries.

However, Cisco ISE also allows you to define a set of vendors, and for each vendor, define a set of attributes. These attributes can be used in authorization profiles and in policy conditions. You can create, edit, and delete RADIUS vendor dictionaries and vendor-specific attributes.

The following topics provide descriptions of the Cisco ISE user interface controls you can use to configure a user dictionary and its attributes, and also procedures for performing dictionary- and attribute-related tasks:

- Dictionary and Attribute User Interface, page 7-2
- Configuring Dictionaries and Dictionary Attributes, page 7-2

Dictionary and Attribute User Interface

This section provides examples of the Cisco ISE user interface that you can use for managing dictionary and related attributes using the Policy, Policy Elements, and Dictionaries tabs. Use the Cisco ISE main window as your starting point for displaying and performing dictionary-related operations for the following Cisco ISE dictionary components:

- System
- User

To manage the System and User dictionaries, use the controls and the navigation pane within the corresponding user interface window. The following list identifies the Cisco ISE user interface tab or menu option choices sequence that contains the controls needed to perform these tasks:

- To display or search for specific attributes in System-defined dictionaries—choose Policy > Policy Elements > Dictionaries > System
- To display, create, modify, delete, or search for specific attributes in User-defined dictionaries—choose Policy > Policy Elements > Dictionaries > User

For more information:

- For more information on displaying or searching for attributes in System dictionaries, see Managing Dictionary Attributes in System-Defined Dictionaries, page 7-2.
- For more information on configuring User dictionaries, see Configuring User-Defined Dictionaries and Dictionary Attributes, page 7-4.

Configuring Dictionaries and Dictionary Attributes

This section provides procedures that apply to both System-defined and User-defined dictionaries.

Managing Dictionary Attributes in System-Defined Dictionaries

Because of the nature of System-defined dictionaries, you can only use the Dictionaries window to display existing System-defined dictionaries or perform two types of searches for dictionary attributes. The following topics provide procedures for performing these two management tasks:

Note The Cisco ISE system-defined dictionary and dictionary attributes are read-only. All system-defined attributes are populated during the installation of the Cisco ISE system software, and you cannot create, modify, or delete the system-defined values or any attributes in a system dictionary. You can only perform a Quick Filter search based on dictionary name and description, or an Advanced Filter search based on a search rule you define.

- Displaying Existing Cisco ISE System-Defined Dictionaries, page 7-3
- Searching for Attributes in an Existing Cisco ISE System-Defined Dictionary, page 7-3

Displaying Existing Cisco ISE System-Defined Dictionaries

To display existing Cisco ISE System dictionaries, choose **Policy > Policy Elements > Dictionaries > System**. The System Dictionary page appears, which lists all current Cisco ISE System-defined dictionaries.

Searching for Attributes in an Existing Cisco ISE System-Defined Dictionary

To search for an attribute in an existing Cisco ISE System-defined dictionary, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Dictionaries > System**.

The Dictionary pane appears, which lists all existing Cisco ISE System-defined dictionaries.

Step 2 Click **Filter** and select from one of the following options:

- Quick Filter
- Advanced Filter

To perform a Quick Filter, enter search criteria in one or more of the following attribute fields:

- Name
- Description

To perform an Advanced Filter, create a matching rule by performing the following:

- In the Filter drop-down list, select one of the following options:
  - Description
  - Name
- In the second drop-down list, select one of the following options:
  - Contains
  - Does not contain
  - Does not equal
  - Ends with
  - Is empty
  - Is exactly (or equals)
  - Is greater than
  - Is greater than or equal to
  - Is less than
  - Is less than or equal to
  - Is not empty
  - Starts with

- In the text box, enter your desired search value.
- Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.
- Click **Clear Filter** to reset the filter process.

Configuring User-Defined Dictionaries and Dictionary Attributes

The Dictionaries window lets you display, create, modify, delete, and search user dictionaries and dictionary attributes that are used within the Cisco ISE system. The following topics provide procedures for performing these tasks:

- Displaying Existing Cisco ISE User-Defined Dictionaries, page 7-4
- Creating a New Cisco ISE User-Defined Dictionary, page 7-4
- Deleting an Existing Cisco ISE User-Defined Dictionary, page 7-5
- Modifying an Existing Cisco ISE User-Defined Dictionary, page 7-5
- Searching for Attributes in an Existing Cisco ISE User-Defined Dictionary, page 7-6
- Creating a New Cisco ISE User-Defined Dictionary Attribute, page 7-7
- Deleting an Existing Cisco ISE User-Defined Dictionary Attribute, page 7-8
- Configuring RADIUS Vendors, page 7-8
- Creating and Editing RADIUS Vendors, page 7-9
- Creating and Editing RADIUS VSAs, page 7-9
- Deleting RADIUS Vendors, page 7-10
- Importing and Exporting RADIUS Vendor Dictionary, page 7-11

Displaying Existing Cisco ISE User-Defined Dictionaries

To display existing Cisco ISE User-defined dictionaries, choose **Policy > Policy Elements > Dictionaries > User**. The User Dictionary page appears, which lists all current Cisco ISE User-defined dictionaries.

Creating a New Cisco ISE User-Defined Dictionary

To create a new Cisco ISE use-defined dictionary, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Dictionaries > User**.

The Dictionary pane appears, which lists all existing Cisco ISE User-defined dictionaries.

Step 2 Click **action** (icon) and choose **New Dictionary** to display the Create Dictionary page, or click **Add (+)**.



Note When you click **action**, four options are displayed: **New Dictionary**, **New Dictionary Attribute**, **Delete Dictionary**, and **Delete Dictionary Attribute**.

Step 3 Enter or choose values for the following fields in the use-defined dictionary:

- Dictionary Name*
- Description
- Version*
- Dictionary Attribute Type*
- Dictionary Type

Note All Dictionary fields marked with an asterisk (*) require you to enter a value. All other fields are optional.

Step 4 Click **Submit** to save this new Cisco ISE user-defined dictionary in the Cisco ISE system local database.

Deleting an Existing Cisco ISE User-Defined Dictionary

To delete an existing Cisco ISE user-defined dictionary, complete the following steps:

Step 1 Choose **Administration> Resources> Dictionaries > User**.

The Dictionary pane appears, which lists all existing Cisco ISE User-defined dictionaries.

Step 2 Choose the check box that corresponds to the user-defined dictionary you want to delete, and click **Delete**.

A delete confirmation page appears that indicates that you have deleted the selected user-defined dictionary.

Step 3 Click **OK** to close the delete confirmation page.

Modifying an Existing Cisco ISE User-Defined Dictionary

To modify values in an existing Cisco ISE user-defined dictionary, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Dictionaries > User**.

The Dictionary pane appears, which lists all existing Cisco ISE User-defined dictionaries.

Step 2 Choose the check box that corresponds to the user dictionary that you want to modify, and click **Edit**.

The Edit Dictionary page is displayed.

Step 3 Modify the **Description**, **Version**, or **Dictionary Attribute Type** value as desired.

Note You cannot modify the values for Dictionary Name or Dictionary Type for an existing dictionary

Step 4 Click **Save** to save the modified Cisco ISE user-defined dictionary value(s) in the Cisco ISE system local database.

Searching for Attributes in an Existing Cisco ISE User-Defined Dictionary

To search for an attribute in an existing Cisco ISE user-defined dictionary, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Dictionaries > User**.

The Dictionary pane appears, which lists all existing Cisco ISE User-defined dictionaries.

Step 2 Click **Filter** and choose one of the following options:

- Quick Filter
- Advanced Filter

To perform a Quick Filter, enter search criteria in one or more of the following attribute fields:

- Name
- Description

To perform an Advanced Filter, create a matching rule by performing the following:

- In the Filter drop-down list, choose one of the following options:
  - Description
  - Name
- In the second drop-down list, chooser one of the following options:
  - Contains
  - Does not contain
  - Does not equal
  - Ends with
  - Is empty
  - Is exactly (or equals)
  - Is greater than
  - Is greater than or equal to
  - Is less than
  - Is less than or equal to
  - Is not empty
  - Starts with
- In the text box, enter your desired search value.
- Click **Go** to launch the filter process, or click plus (+) to add additional search criteria.
- Click **Clear Filter** to reset the filter process.

Creating a New Cisco ISE User-Defined Dictionary Attribute

To create a new Cisco ISE user-defined dictionary attribute, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Dictionaries > User**.

The Dictionary pane appears, which lists all existing Cisco ISE User-defined dictionaries.

Step 2 In the User navigation pane, choose the user dictionary in which you want to create a new attribute, click **action** (icon), and choose **New Dictionary Attribute** to display the Edit Dictionary page.

(Optional) In the list of existing User-defined dictionaries, choose the check box that corresponds to the user dictionary in which you want to create a new dictionary attribute, click **Edit**, and click **Dictionary Attributes** tab.

The Dictionary Attributes page appears.

Step 3 Enter or choose values for the following fields for the dictionary attribute that is being created:

- Attribute Name*
- Description
- Internal Name*
- Data Type*
- Dictionary*

Note All attribute fields marked with an asterisk (*) require that you enter a value. All other fields are optional. The Data Type and Dictionary fields are drop-down lists that allow you to choose from a list of options.

Step 4 In the Allowed Values table, click **Add (+)** and click on the new line to display the configurable fields.

Step 5 Enter or choose values for each of the following attribute types in the corresponding fields:

- Name
- Value
- IsDefault (choose Yes or No)

Step 6 Click **Save** to save the configured attribute value, or click **Cancel** to close the configurable fields.

Note When you click **Cancel** it does not delete this allowed attribute value. Use Step 7 to delete an attribute value.

Step 7 (Optional) If you want to delete an allowed attribute value, in the Allowed Values table, choose the check box that corresponds to the attribute value that you want to delete, and click **Remove** to delete this attribute from the table.

Step 8 Click **Submit** to save your attribute changes in the Cisco ISE system database.

Deleting an Existing Cisco ISE User-Defined Dictionary Attribute

To delete an existing Cisco ISE user-defined dictionary attribute, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Dictionaries > User**.

The Dictionary pane appears, which lists all existing Cisco ISE User-defined dictionaries.

Step 2 In the User navigation pane, choose the user dictionary in which you want to delete a dictionary attribute.

Step 3 Click the **Dictionary Attributes** tab.

A list of dictionary attributes for the selected dictionary is displayed.

Step 4 Choose the check box that corresponds to the attribute that you want to delete, and click **Delete**.

A delete confirmation page appears that indicates that you have deleted the selected dictionary attribute.

Step 5 Click **OK** to close the delete confirmation page.

Configuring RADIUS Vendors

To access the RADIUS vendor list in Cisco ISE, choose **Policy > Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors**. This page lists the RADIUS vendors that Cisco ISE supports. Each vendor definition in the list contains the vendor name, vendor ID, and a brief description. If you click on any of the listed vendor names, you can also view the following two properties, which are also related to the relevant RADIUS vendor dictionary attribute:

- Type Field Length—The number of bytes taken from the attribute value, which are used to specify the attribute type.
- Size Field Length—The number of bytes taken from the attribute value to specify the attribute length.

Each vendor attribute has a name, data type, direction (which specifies whether it is relevant to requests only, responses only, or both), and description.

The following default vendor dictionaries are available in Cisco ISE:

- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

This section contains the following topics:

- Creating and Editing RADIUS Vendors, page 7-9
- Creating and Editing RADIUS VSAs, page 7-9
- Deleting RADIUS Vendors, page 7-10
- Importing and Exporting RADIUS Vendor Dictionary, page 7-11

Creating and Editing RADIUS Vendors

To create and edit a RADIUS vendor, complete the following steps:

Step 1 From the Policy mega menu, choose **Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors**.

The RADIUS Vendors page appears with a list of RADIUS vendors that ISE supports.

Step 2 Click **Add** to create a new RADIUS vendor, or click the check box next to the RADIUS vendor that you want to edit and click **Edit**.

Step 3 Enter the following information:

- Name—(Required) Name of the RADIUS vendor.
- Description—An optional description for the vendor.
- Vendor ID—(Required) The Internet Assigned Numbers Authority (IANA)-approved ID for the vendor.
- Vendor Attribute Type Field Length—(Required) The number of bytes taken from the attribute value to be used to specify the attribute type. Valid values are 1, 2, and 4. The default value is 1.
- Vendor Attribute Size Field Length—(Required) The number of bytes taken from the attribute value to be used to specify the attribute length. Valid values are 0 and 1. The default value is 1.

Step 4 Click **Submit** to save the RADIUS vendor.

For more information:

See the "Configuring RADIUS Vendors" section on page 7-8.

Creating and Editing RADIUS VSAs

To create and edit RADIUS vendor-specific attributes (VSAs), complete the following steps:

Step 1 From the Policy mega menu, choose **Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors**.

The RADIUS Vendors page appears with a list of vendors.

Step 2 Click the check box next to the RADIUS vendor dictionary for which you to want add attributes or whose attributes you want to edit.

Step 3 Click **Edit Attributes**.

The RADIUS Vendor Attributes page appears.

Step 4 Click **Add** to create an attribute, or click the check box next to the attribute that you want to edit, and then click **Edit**.

Step 5 Enter the following information:

- Name—(Required) Name of the VSA
- Description—An optional description
- Internal Name—Internal name of the VSA

- Data Type—Could be one of the following:
  - STRING
  - INTEGER
  - FLOAT
  - BOOLEAN
  - IPv4
  - OCTET_STRING
  - UINT32
  - UINT64
- Direction—Could be one of the following:
  - IN—Requests only
  - OUT—Responses only
  - BOTH—Bidirectional
- ID—The vendor attribute ID. Click the **Allowed Values** tab to enter allowed values for the vendor attribute ID. The allowed values for the vendor attribute ID depend on the type and size specified for the corresponding vendor. For example, if 1 byte is chosen, then a range of 1 to 255 is permitted and 0 is not permitted. For *n* bytes, the range would be 1 to ((2^*n*) – 1).

Step 6 To add an allowed value, click the **Allowed Values** tab.

- Click **Add**.
- Enter the name in the Please enter name for new Attribute Allowed Value dialog box.

  A record is created.
- Choose the record to add value and choose Yes from the isDefault drop-down list box if you want this value to be the default value.
- Click **Submit** to save your changes.

  You can add additional allowed values for this VSA.

Step 7 Click **Submit** to save the VSA.

For more information:

- Configuring RADIUS Vendors, page 7-8
- Creating and Editing RADIUS Vendors, page 7-9

Deleting RADIUS Vendors

To delete a RADIUS vendor, complete the following steps:

Step 1 From the Policy mega menu, choose **Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors**.

The RADIUS Vendors page appears with a list of vendors.

Step 2 Click the check box next to the vendor that you want to delete, then click **Delete**.

A dialog box displays the following message: Are you sure you want to delete this vendor?

Step 3 Click **OK** to delete the RADIUS vendor.

For more information:

- For more information on configuring RADIUS vendors, see Configuring RADIUS Vendors, page 7-8.
- For more information on configuring RADIUS vendors, see Creating and Editing RADIUS Vendors, page 7-9.

Importing and Exporting RADIUS Vendor Dictionary

You can import RADIUS vendor dictionaries into Cisco ISE and export the RADIUS vendor dictionaries from Cisco ISE.

To import a RADIUS vendor dictionary, complete the following steps:

Before you can import a RADIUS vendor dictionary into Cisco ISE, ensure that you have the dictionary in the file system that is running the Cisco ISE browser.

Step 1 From the Policy mega menu, choose **Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors**.

Step 2 The RADIUS Vendors page appears.

Step 3 Click **Import**.

Step 4 Click the **Import Vendor** radio button.

Step 5 Click **Browse** to choose the vendor dictionary from the file system that is running your client browser.

Step 6 Click **Import** to import the vendor dictionary.

To export a RADIUS vendor dictionary, complete the following steps:

Step 1 From the Policy mega menu, choose **Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors**.

Step 2 Click the check box next to the vendor dictionary that you want to export and click **Export**.

Step 3 Save the vendor dictionary on the file system that is running your client browser.



CHAPTER 8

Administering Cisco ISE

This chapter describes the administrative activities for the Cisco Identity Services Engine (ISE) and how to perform them. The following topics are covered:

- Logging In, page 8-1
- Enabling FIPS Mode in Cisco ISE, page 8-2
- Configuring Cisco ISE for Administrator CAC Authentication, page 8-4
- Specifying Proxy Settings in Cisco ISE, page 8-17
- System Time and NTP Server Settings, page 8-18
- Configuring Email Settings, page 8-20
- Configuring System Alarm Settings, page 8-21
- Configuring Alarm Syslog Targets, page 8-22
- Managing Software Patches, page 8-24

Logging In

The Cisco ISE GUI is supported on the following HTTPS-enabled following browsers:

- Mozilla Firefox version 3.6
- Mozilla Firefox version 9
- Microsoft Internet Explorer version 8
- Microsoft Internet Explorer version 9 (in Internet Explorer version 8 compatibility mode).

Note The Cisco ISE GUI is not supported on Internet Explorer version 8 running in Internet Explorer 7 compatibility mode. For a collection of known issues regarding Microsoft Internet Explorer version 8, see the "Known Issues" section of the *Release Notes for Cisco Identity Services Engine, Release 1.1*.

After you have installed Cisco ISE as described in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*, you can log into Cisco ISE.

To log into the Cisco ISE GUI, complete the following steps:

Step 1 Enter the ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*).

The ISE login window appears.

Step 2 Enter the Username and Password which you would have configured during initial Cisco ISE Setup.

The Password field is case-sensitive.

If you have to reset Administrator password, refer to the "Performing Post-Installation Tasks" chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

Step 3 Click **Login** or press **Enter**.

You can now access the menus in the ISE user interface.

Note Any time your login is unsuccessful, click the **Problem logging in?** link in the Login window and follow the instructions in Step 2.

Tip The minimum required screen resolution to view the Cisco ISE GUI and for a better user experience is 1280X800 pixels.

Related Topic

Administrator Lockout Following Failed Login Attempts, page 8-2

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for your specified administrator user ID enough times, the Cisco ISE user interface "locks you out" of the system, adds a log entry in the **Operations > Reports > Catalog > Server Instance > Server Administrator Logins** report, and suspends the credentials for that administrator ID until you have an opportunity to reset the password that is associated with that administrator ID, as described in the "Performing Post-Installation Tasks" chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*. The number of failed attempts that is required to disable the administrator account is configurable according to the guidelines that are described in Configuring a Password Policy for Administrator Accounts, page 4-62. After an administrator user account gets locked out, an email is sent to the associated administrator user.

Disabled System administrators' status can be enabled by any Super Admin including AD users.

Enabling FIPS Mode in Cisco ISE

Cisco ISE supports Federal Information Processing Standard (FIPS) 140-2, the United States government computer security standard that is used to accredit cryptographic modules. Cisco ISE uses an embedded FIPS 140-2 implementation using validated C3M and Cisco ACS NSS modules, per FIPS 140-2 Implementation Guidance section G.5 guidelines.

In addition, the FIPS standard places limitations on the use of certain algorithms. In order to enforce this standard, you must enable FIPS operation in Cisco ISE. Cisco ISE enables FIPS 140-2 compliance via Key Management measures. While in FIPS mode, any attempt to perform functions using a non-FIPS compliant algorithm fails, and, as such, certain authentication functionality is disabled. For more details, including protocol support, see the "Support for FIPS 140-2 Implementation" section on page 1-3 and "Support Common Access Card Functions" section on page 1-3 section in Chapter 1, "Overview of Cisco ISE."

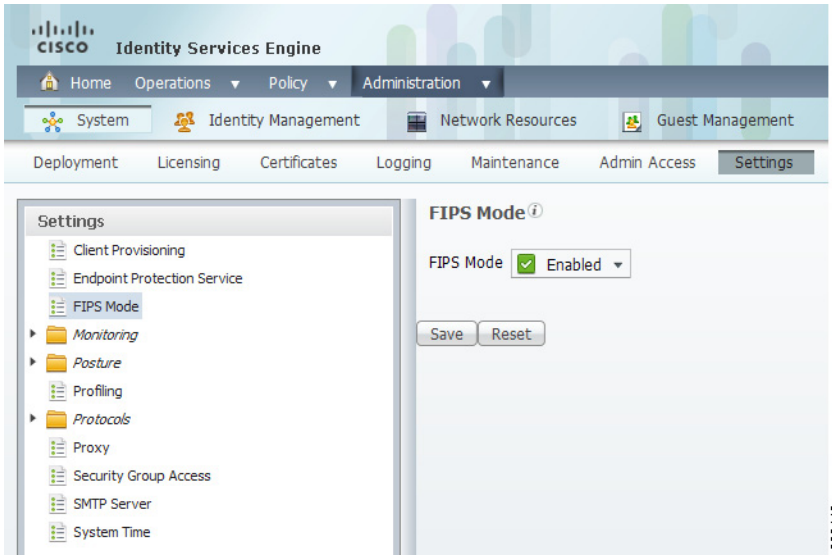
When FIPS mode is enabled, The Cisco ISE administrator interface displays a FIPS mode icon in the upper right portion of the screen, immediately to the left of the node name.

Note Cisco recommends that you not enable FIPS mode before completing any database migration process.

To enable FIPS 140-2 compliant operations on Cisco ISE, complete the following steps:

Step 1 Choose **Administration > System > Settings > FIPS Mode**.

Figure 8-1 Administration > System > Settings > FIPS Mode



Note If Cisco ISE detects at least one protocol or certificate that is not supported by the FIPS 140-2 level 1 standard, Cisco ISE displays a warning with the names of the protocols and FIPS mode is not enabled until those protocols have been addressed appropriately.

Step 2 Choose the **Enabled** option from the FIPS Mode drop-down list.

Step 3 Click **Save**. Cisco ISE automatically prompts you to restart your machine.

Once you have enabled FIPS mode, you must also reboot all other nodes in the deployment. To minimize disruption to your network, Cisco ISE automatically performs a "rolling restart" by first, restarting the primary Administration ISE node, and then restarting each secondary node, one node at a time.

To fully enable FIPS 140-2 compliance once you have turned on this setting, be sure to also configure the FIPS-specific functions that are included under "Next Steps" below and then reboot all Cisco ISE nodes in your deployment.

Next Steps

Once you have enabled FIPS mode, Cisco recommends that you also enable and configure the following FIPS 140-2 compliant functions:

- Adding and Editing Devices, page 6-3
- Generating a Self-Signed Certificate, page 13-7
- Generating a Certificate Signing Request, page 13-8
- Creating RADIUS Servers, page 16-23

In addition, you may wish to enable administrator account authorization using a Common Access Card (CAC) function according to the guidelines in Configuring Cisco ISE for Administrator CAC Authentication, page 8-4. Although using CAC functions for authorization is not strictly a FIPS 140-2 requirement, it is a well-known secure access measure that is used in a number of environments to bolster FIPS 140-2 compliance.

Cisco NAC Agent Requirements when FIPS Mode is Enabled

The (temporal) Cisco NAC Web Agent and (persistent) Cisco NAC Agent always look for the Windows Internet Explorer TLS 1.0 settings to discover the Cisco ISE network. (These TLS 1.0 settings should be enabled in Internet Explorer.) Therefore, client machines must have Windows Internet Explorer version 7, 8, or 9 installed with TLS1.0 enabled to allow for Cisco ISE posture assessment functions to operate on client machines accessing the network. See the following guidelines:

- The Cisco NAC Agent can automatically enable the TLS 1.0 setting in Windows Internet Explorer if FIPS mode has been enabled in Cisco ISE.
- The Cisco NAC Web Agent does not automatically enable the TLS 1.0 settings in Windows Internet Explorer.
- You also need to ensure that TLS 1.0 settings are enabled for end users launching Mozilla Firefox or Google Chrome browsers on client machines going through Cisco ISE posture assessment.

Configuring Cisco ISE for Administrator CAC Authentication

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee of, for example, the U.S Department of Defense (DoD). Access via the CAC requires a card reader into which the user inserts the card and enters a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

The administrator user interface can be configured so that administrators can only authenticate themselves by using a client certificate (credentials-based authentication—such as a user ID and password—is not required or even permitted). In this setup, an administrator inserts the CAC card, enters the correct PIN, then enters the Cisco ISE administrator user interface URL into the browser address field. The browser forwards the certificate to Cisco ISE, and Cisco ISE authenticates and authorizes the

administrator, based on the contents of the certificate. If this process is successful, the user is presented with the Cisco ISE Monitoring and Troubleshooting home page, and is given the appropriate RBAC permissions.

The following sections describe how to set up Cisco ISE to allow certificate-based administrator authentication using a CAC device:

- Preliminary Setup Done by ISE Administrator, page 8-5
- Step 1: Enable FIPS Mode, page 8-6
- Step 2: Configure Active Directory, page 8-6
- Step 3: Create Certificate Authentication Profile, page 8-9
- Step 4: Import CA Certificates into ISE Certificate Trust Store, page 8-9
- Step 5: Configure CA Certificates for Revocation Status Check, page 8-10
- Step 6: Enable Client Certificate-Based Authentication, page 8-12
- Step 7: Configure Admin Group to AD Group Mapping, page 8-13
- Step 8: Configure Admin Authorization Policy, page 8-16

Note Windows Internet Explorer version 8 and 9 users running the Windows 7 operating system must install the ActiveIdentity "ActivClient" version 6.2.0.133 third-party middleware software product for Cisco ISE to interoperate with CAC. For more information on ActiveIdentity security client products, please refer to http://www.actividentity.com/products/securityclients/ActivClient/.

Preliminary Setup Done by ISE Administrator

Before beginning configuration, ensure that the following is done:

- The DNS server setting in Cisco ISE is set correctly for Active Directory.
- Active Directory user and user group membership has been defined for each administrator certificate.

To ensure that Cisco ISE can authenticate and authorize an administrator based on the CAC-based client certificate that is submitted from the browser, be sure that you have configured the following:

- The external identity source (Active Directory in the following example)
- The user groups in Active Directory to which the administrator belongs
- How to find the user's identity in the certificate
- Active Directory user groups to Cisco ISE RBAC permissions mapping
- The Certificate Authority (trust) certificates that sign the client certificates
- A method to determine if a client certificate has been revoked by the CA

Step 1: Enable FIPS Mode

Note This step is optional in CAC configuration. FIPS mode is not required for certificate-based authentication, but the two security measures often go hand-in-hand. If you do plan to deploy Cisco ISE in a FIPS 140-2 compliant deployment and to use CAC certificate-based authorization as well, be sure to turn FIPS mode on and specify the appropriate private keys and encryption/decryption settings *first*.

To enable FIPS 140-2 compliant mode on Cisco ISE, see the guidelines and subsequent setup steps as described in Enabling FIPS Mode in Cisco ISE, page 8-2.

Tip You will be prompted to restart all Cisco ISE nodes in your deployment when enabling FIPS mode.

Step 2: Configure Active Directory

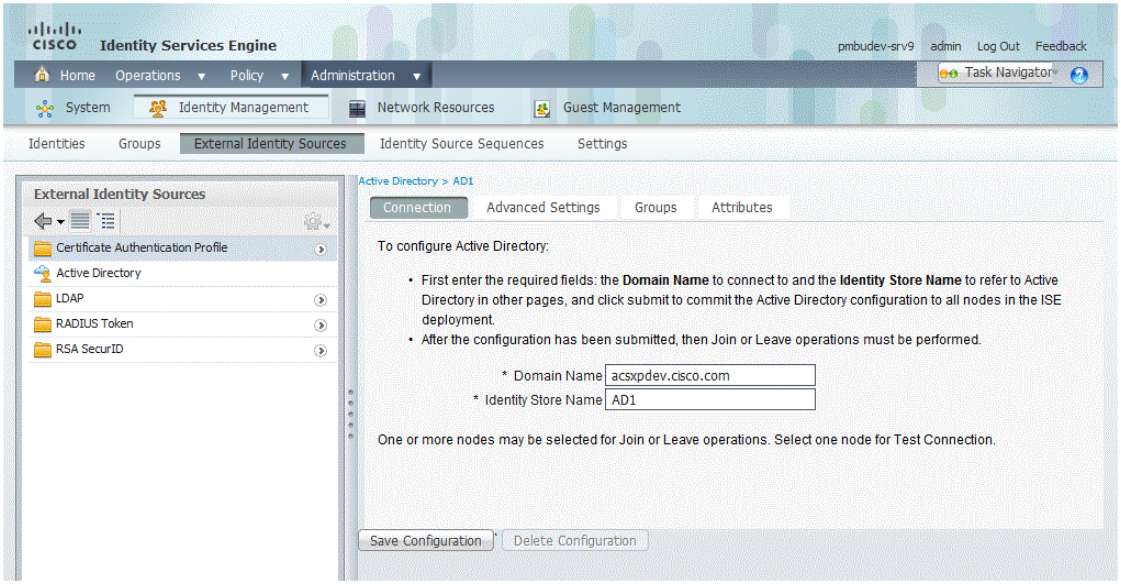
Active Directory is used to authenticate and authorize administrators using CAC cards. See Microsoft Active Directory, page 5-4.

To configure Cisco ISE to use Active Directory in this example, complete the following steps:

Step 1 Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.

Step 2 Enter the Active Directory Domain Name and an Identity Store Name, then click **Save Configuration**.

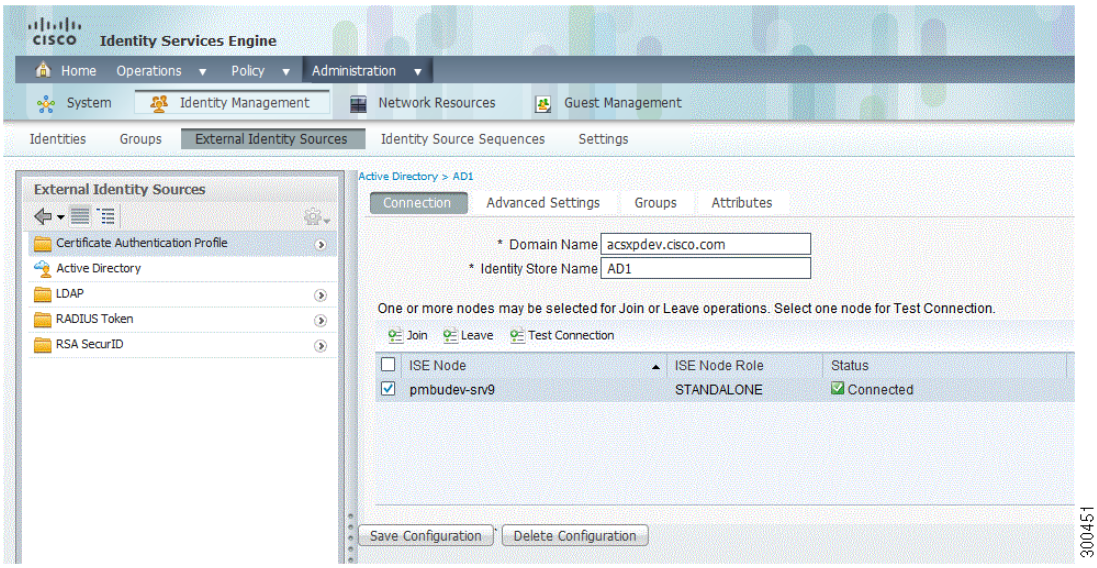
Figure 8-2 Using Active Directory for CAC



Step 3 Click **Save Configuration**.

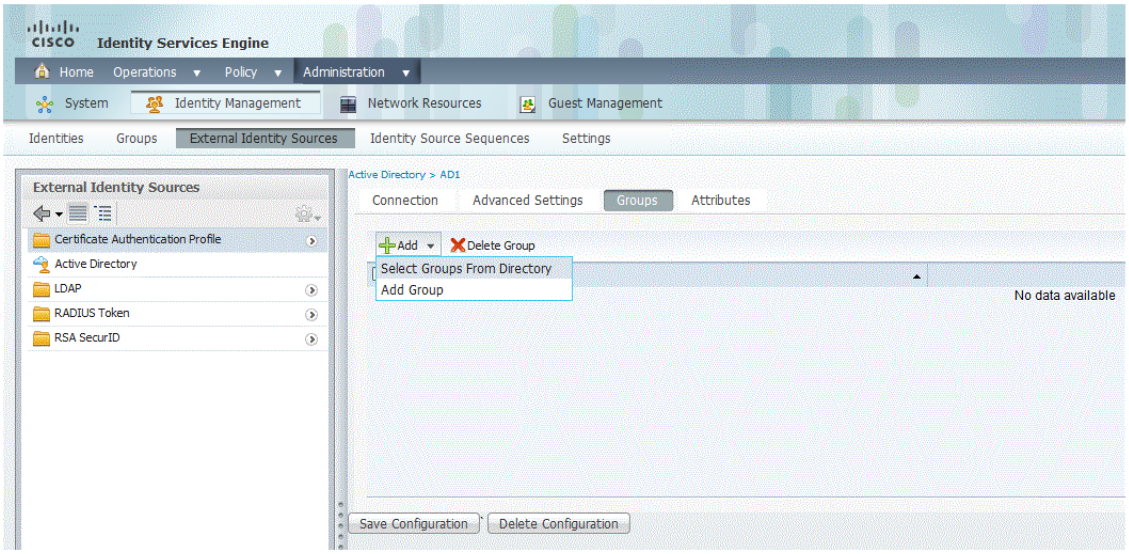
Step 4 Join your Cisco ISE deployment nodes to Active Directory.

Figure 8-3 Join Cisco ISE to Active Directory for CAC



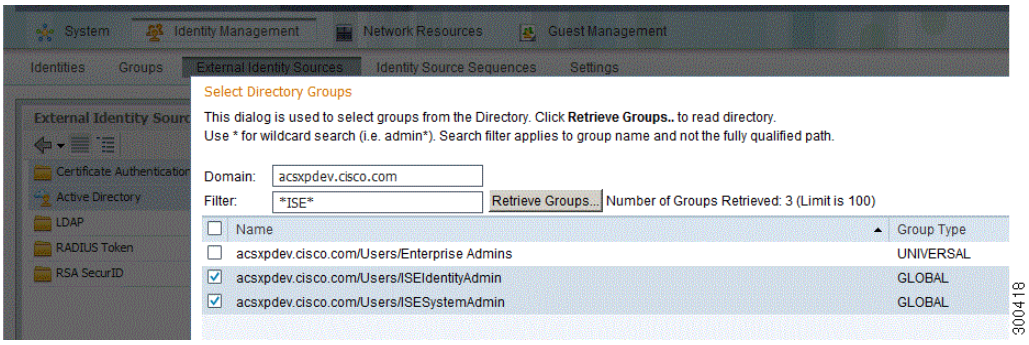
Step 5 You will want to eventually map Administrator Groups to AD Groups; therefore, you need to import some AD Groups to which your administrator belongs. Click the Groups tab, click **Add**, and choose the **Select Groups From Directory** drop-down option.

Figure 8-4 Select Groups from Directory for CAC



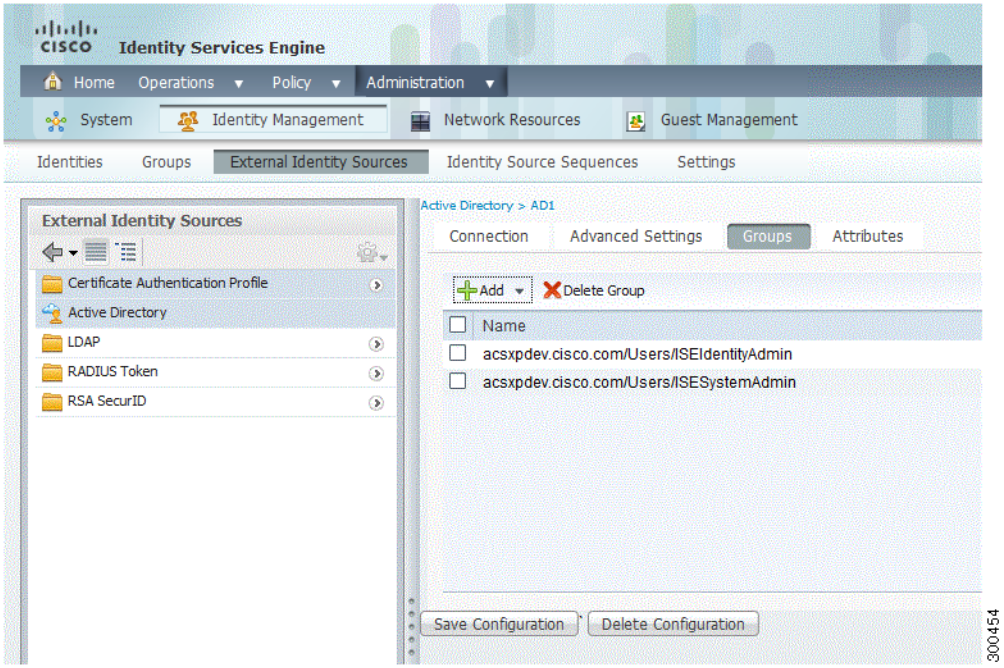
Step 6 In the resulting pop-up dialog, select one or more directory groups. In this example, two Cisco ISE administrator groups are defined in AD.

Figure 8-5 Select Directory Groups for CAC



Step 7 After selecting the groups, be sure to press the **Save Configuration** button again. Otherwise, your group selections will not be saved.

Figure 8-6 Save CAC Configuration



Step 3: Create Certificate Authentication Profile

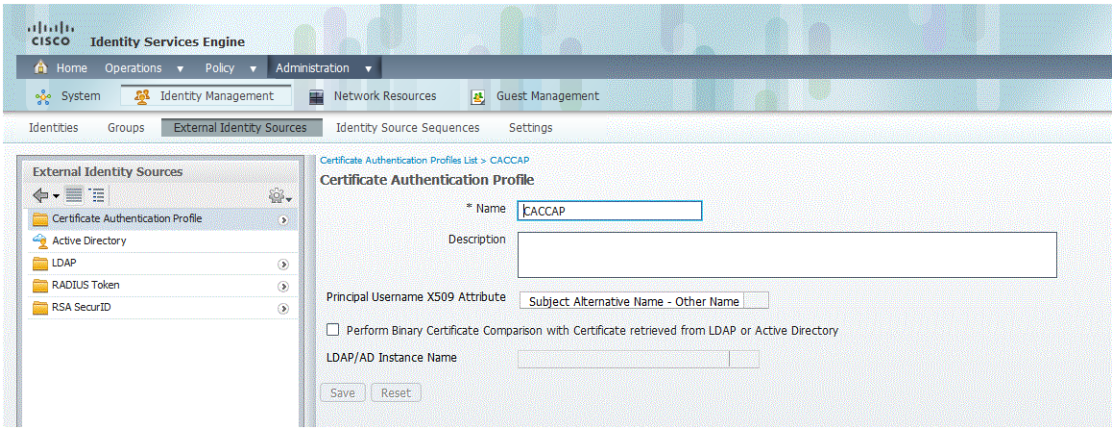
The Certificate Authentication Profile tells ISE where to find the user's identity in the client certificate. See Adding or Editing a Certificate Authentication Profile, page 5-2.

To create the authentication profile in this example, complete the following steps:

Step 1 Navigate to **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**.

Step 2 Click **Add** to bring up the profile configuration pane.

Figure 8-7 Create Authentication Profile for CAC



Step 3 Enter the profile name and an optional description.

Step 4 Be sure to select the attribute in the certificate that contains the administrator user name in the Principal Name X.509 Attribute field. (For CAC cards, the Signature Certificate on the card is normally used to look up the user in Active Directory. The Principal Name is found in this certificate in the "Subject Alternative Name" extension, specifically in a field in that extension that is called "Other Name." So the attribute selection here should be "Subject Alternative Name - Other Name.")

Step 5 If the AD record for the user contains the user's certificate, and you want to compare the certificate that is received from the browser against the certificate in AD, check the **Binary Certificate Comparison** check box, and select the Active Directory instance name (which was specified this earlier in Step 2: Configure Active Directory, page 8-6).

Step 4: Import CA Certificates into ISE Certificate Trust Store

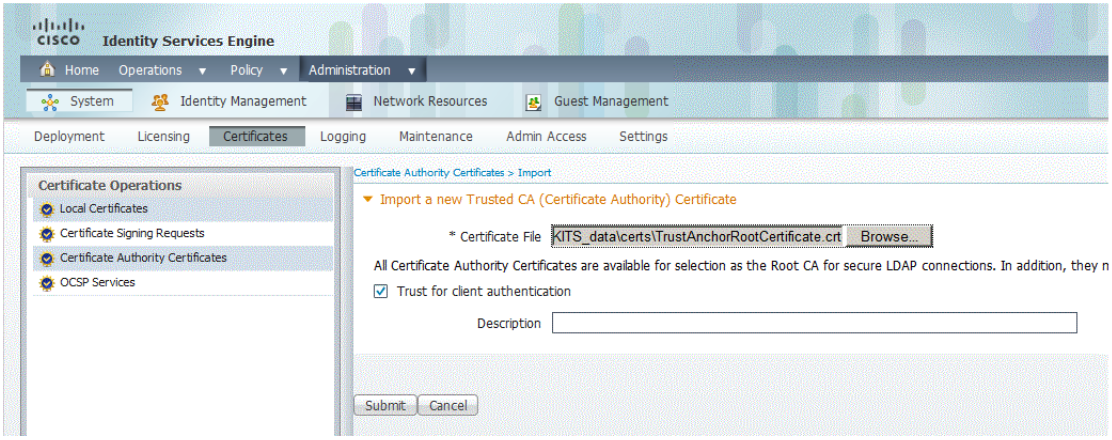
The ISE application server will not accept a client certificate unless the CA certificates in the client certificate's trust chain are placed in the ISE trust store. This means you will need to import the appropriate CA certificate into the ISE trust store. See Importing Root and CA Certificates into the CTL of the Primary Node, page 13-23.

Step 1 Navigate to **Administration > System > Certificates > CA Certificates**.

Step 2 On the list page, click **Add**.

Step 3 Select the file containing the CA certificates you want to import, and check the **Trust for client authentication** check box.

Figure 8-8 Specify CA Certificates for CAC



Step 4 Click **Submit**.

Tip Cisco recommends that you import the CA certificates that are needed to trust client certificates *before* you enable client certificate-based authentication. Importing CA certificates after enabling client certificate-based authentication requires an application server restart on all ISE nodes in your deployment.

If you must import a CA certificate after enabling client certificate-based authentication, you have the option to defer the restart. This is convenient if you are going to import multiple CA certificates, and you wish to avoid having to restart each time. If you defer the restart, a Deferred Restart notification appears on the Notifications tab, which is accessible at the bottom right portion of the page. You must access this tab and enable the restart for your CA certificate changes to take effect.

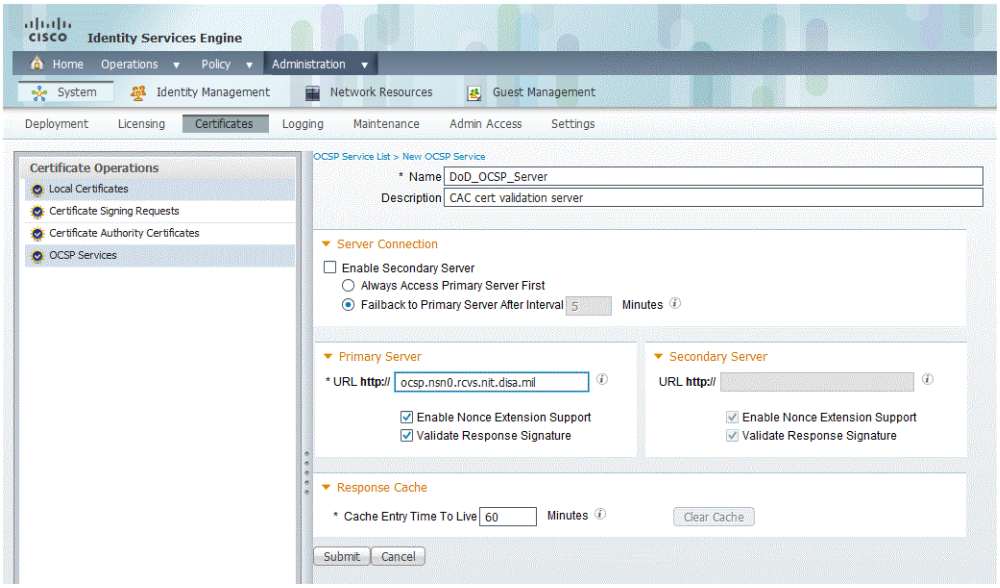
Step 5: Configure CA Certificates for Revocation Status Check

A certificate authority may revoke or declare a certificate “unusable” prior to its expiration date. You can use Cisco ISE to query the certificate authority to verify the revocation status of a certificate via the Online Certificate Status Protocol (OCSP) server or the Certificate Revocation Lists (CRLs). You can perform this check when a client certificate is authenticated. See OCSP Services, page 13-25 and Editing a Certificate Authority Certificate, page 13-19.

Step 1 If you are going to use OCSP, first navigate to **Administration > System > Certificates > OCSP Services**. Otherwise, skip to Step 3.

Step 2 Enter a name for the OCSP server, an optional description, and the URL of the server.

Figure 8-9 Specify CA Certificates for Revocation Using OCSP

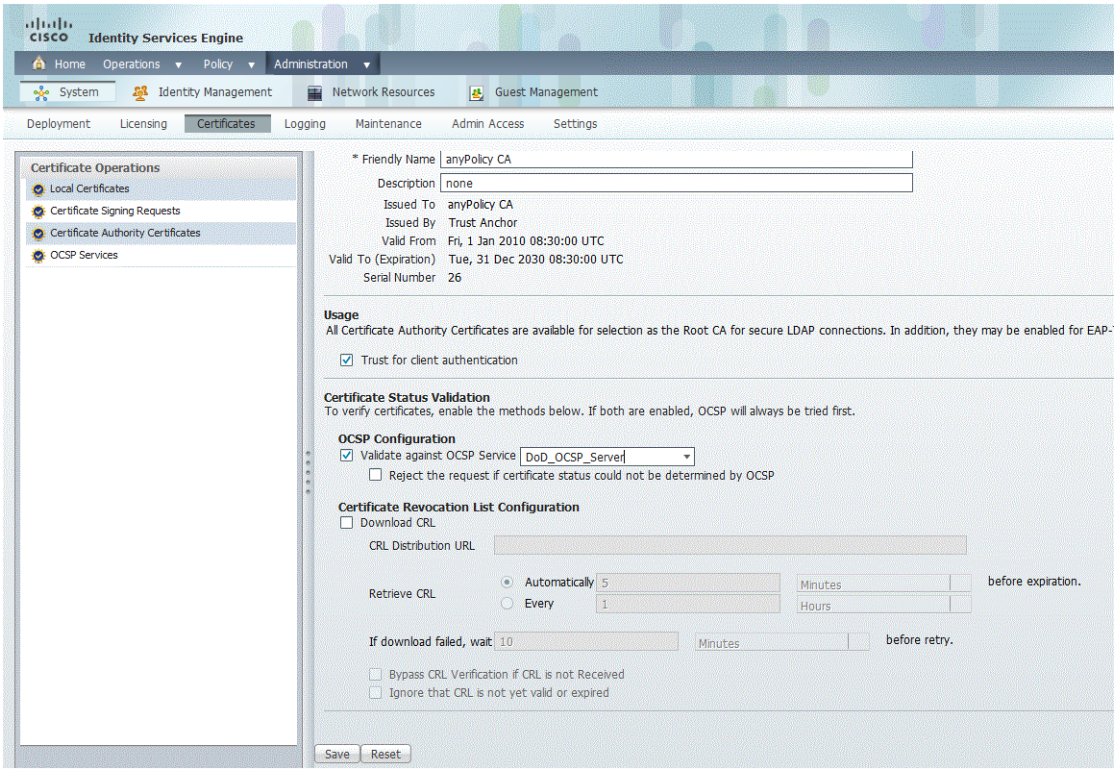


Step 3 Navigate to **Administration > System > Certificates > CA Certificates**.

Step 4 For each CA certificate that can sign a client certificate, you must specify how to do the revocation status check for that CA. Select a CA certificate from the list and click **Edit**.

Step 5 On the edit page that appears, you can select OCSP or the CRL validation. If you select OCSP, you must select an OCSP service to use for that CA. If you select CRL, you must specify the CRL Distribution URL and other applicable configuration parameters.

Figure 8-10 Specify CA Certificates for Revocation Using CRL



Step 6 Click **Save**.

Step 6: Enable Client Certificate-Based Authentication

Switch from the default password-based authentication to certificate-based authentication.

The method you use to authenticate the administrator certificate is specified by a Certificate Authentication Profile. User authorization is done through an external identity store, which in this case is Active Directory. Note that the Principal Name attribute from the Certificate Authentication Profile is used to look up the user in Active Directory. See Configuring the Simple Authentication Policy, page 16-26.

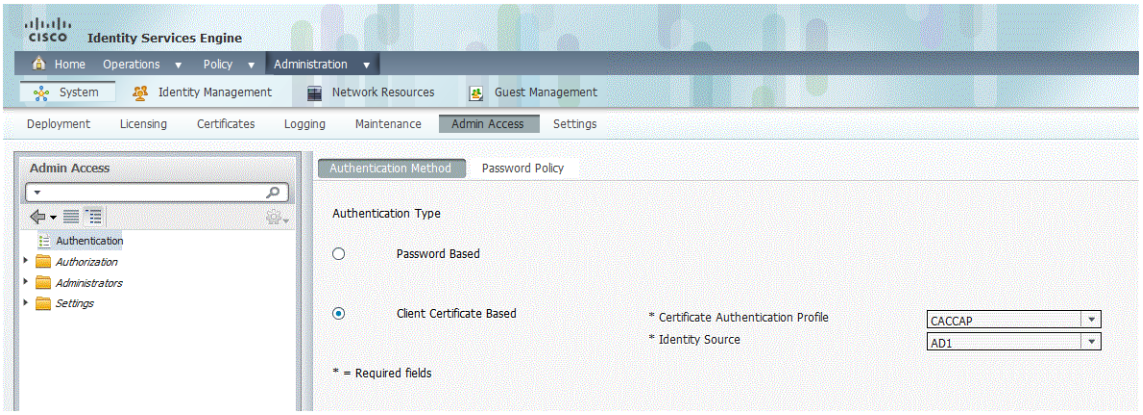
To enable client certificate-based authentication in this example, complete the following steps:

Step 1 Navigate to **Administration > System > Admin Access > Authentication**.

Step 2 On the Authentication Method tab, select the **Client Certificate Based** option.

Step 3 Select the Certificate Authentication Profile that you created earlier. For Identity Source, select the Active Directory instance name.

Figure 8-11 Enable Certificate-Based Authentication for CAC



Note You will be prompted to restart the application server on all Cisco ISE nodes in your deployment, when enabling client certificate-based authentication.

Step 7: Configure Admin Group to AD Group Mapping

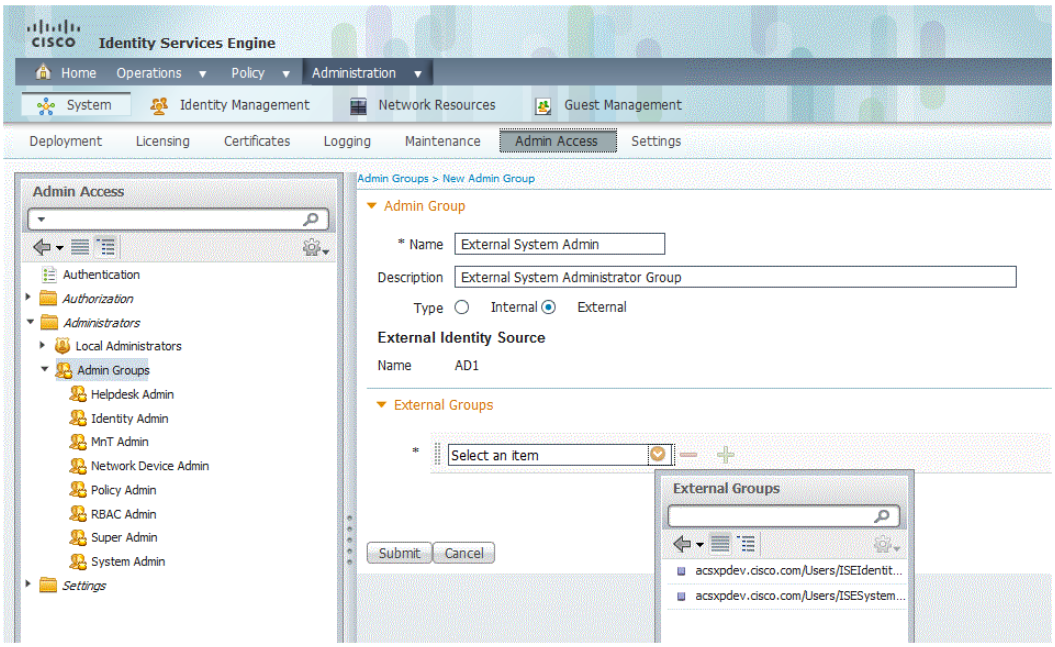
Define one or more Cisco ISE Admin Groups, and map each one to Active Directory groups. This allows user authorization to determine the RBAC permissions for the administrator, based on group membership in Active Directory. See Managing Admin Access (RBAC) Policies, page 4-49.

Note You cannot map predefined Admin Groups to AD groups; you must create new Admin Groups, and you *must* do this step after you have enabled client certificated-based authentication (Step 6: Enable Client Certificate-Based Authentication, page 8-12). Otherwise, you will not see any available AD Groups to which you can map.

Step 1 Navigate to **Administration > System > Admin Access > Administrators > Admin Groups**.

Step 2 Click **Add** in the table header to bring up the new Admin Group configuration pane.

Figure 8-12 Configure Admin Group to AD Group Mapping for CAC



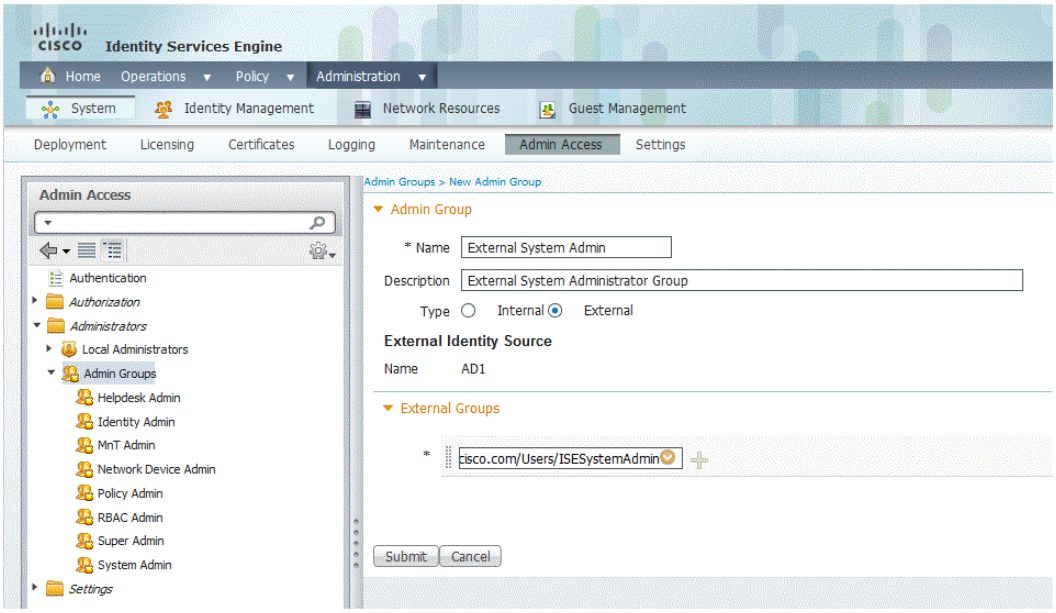
Step 3 Enter a name and optional description for the new Admin Group.

Step 4 For the group Type, select **External**. The instance name for Active Directory appears.

Step 5 Under External Groups, where it says "Select an item," click the down arrow to display a list of the AD Groups that you imported when setting up Active Directory.

Step 6 Select the AD Group to which you want this Admin Group to map. If you require a one-to-many mapping, click the "+" (plus) icon and select another AD Group.

Figure 8-13 Configure Additional Admin Group to AD Group Mapping for CAC

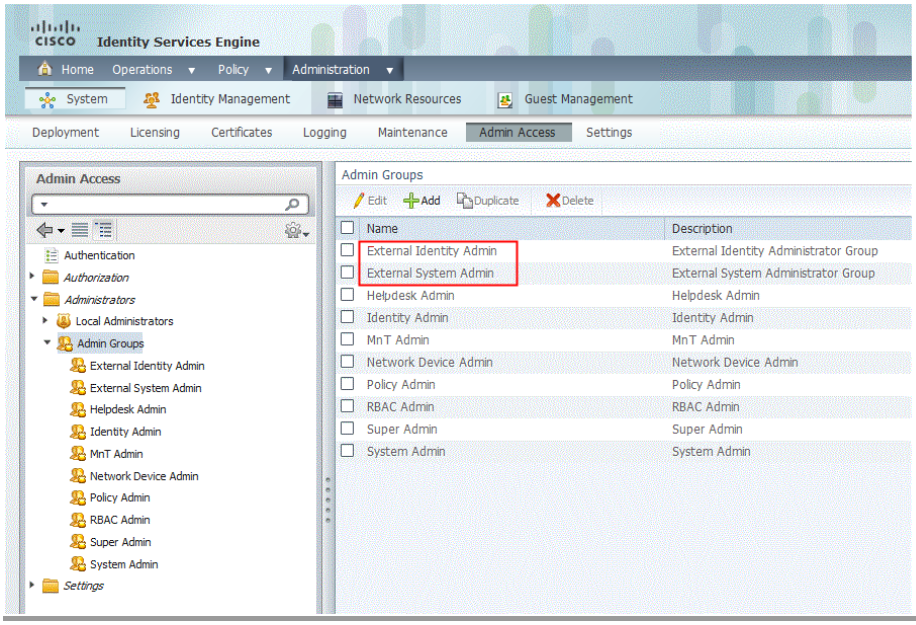


In this example, you have created an Admin Group called External System Admin and mapped it to an AD Group called ISESystemAdmin.

Step 7 Click **Submit** to save the new Admin Group.

To further illustrate the different RBAC permissions that you can assign to Admin Groups, you have created a second group called External Identity Admin, which is mapped to the AD Group ISEIdentityAdmin.

Figure 8-14 Display New Admin Group for CAC



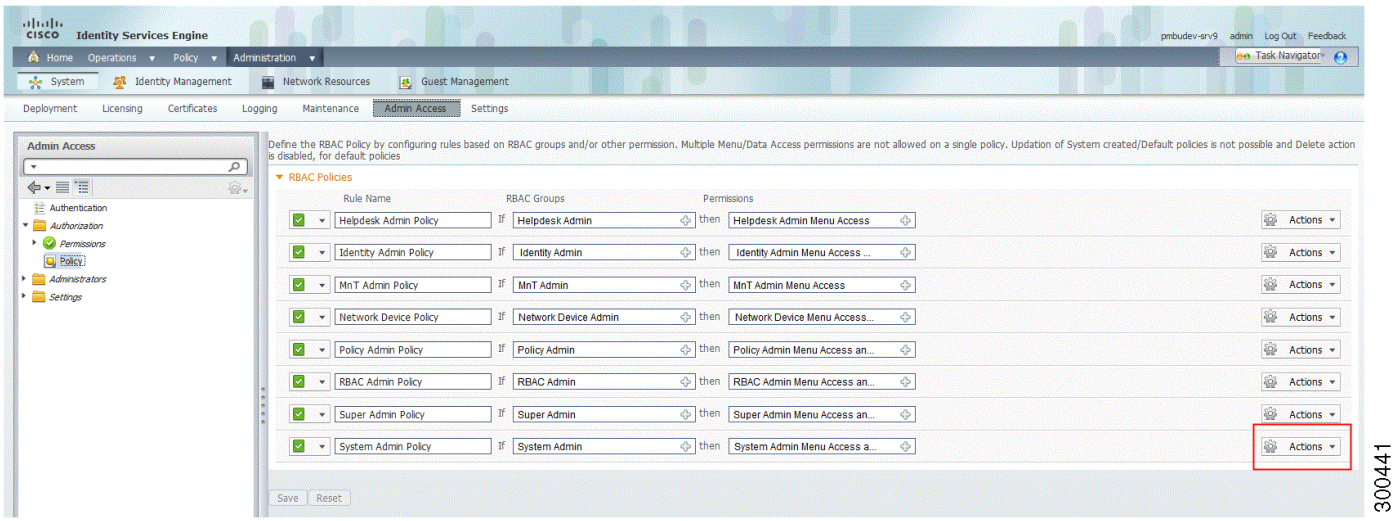
Step 8: Configure Admin Authorization Policy

Assign RBAC permissions to each of the Admin Groups created in Step 7: Configure Admin Group to AD Group Mapping, page 8-13. See Configuring Authorization Policies, page 17-14.

Step 1 Navigate to **Administration > System > Admin Access > Authorization > Policy**.

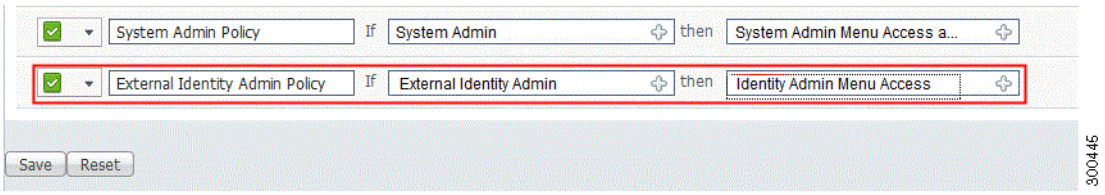
This page shows the RBAC polices that are in effect for administrative access. You can add a new by clicking the Actions drop-down list on the right and selecting **Insert new policy below**.

Figure 8-15 Insert New Admin Policy for CAC



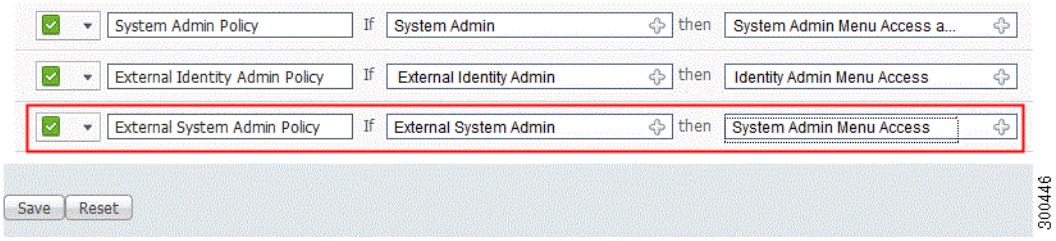
Step 2 Create a new policy called External Identity Admin Policy, which specifies the new External Identity Admin group and assigns it Identity Admin Menu Access permissions.

Figure 8-16 Specify the New Admin Policy Attributes for CAC



Step 3 Create another policy for your other new Admin Group, External System Admin.

Figure 8-17 Create Additional Admin Policy for CAC



Step 4 Click **Save** after adding the policies.

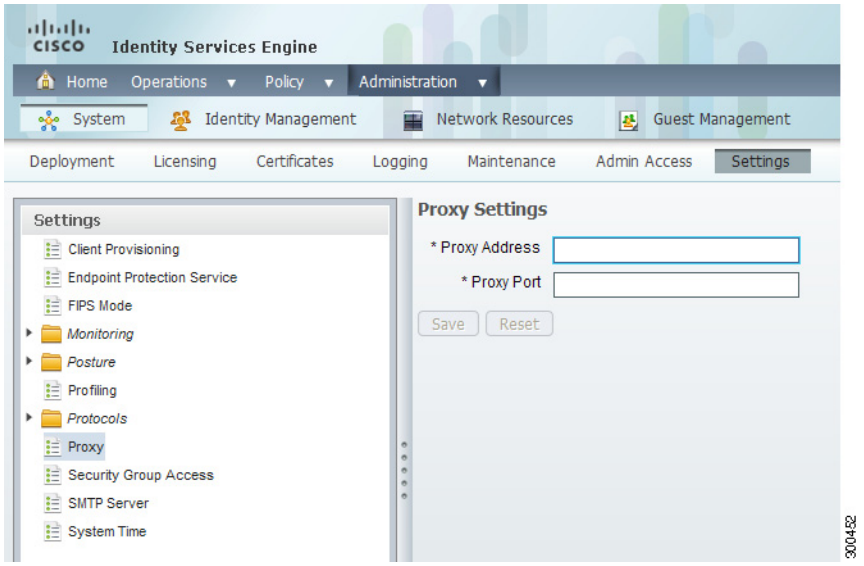
Specifying Proxy Settings in Cisco ISE

If your existing network topology requires you to use a proxy for Cisco ISE, to access external resources (like the remote download site where you can find client provisioning and posture-related resources), you can use the Cisco ISE user interface to specify proxy properties.

To specify proxy settings for Cisco ISE, complete the following steps:

Step 1 Choose **Administration > System > Settings > Proxy**.

Figure 8-18 Administration > System > Settings > Proxy



Step 2 Enter the proxy IP address or DNS-resolvable host name in the Proxy Address field, and specify the port through which proxy traffic travels to and from Cisco ISE in the Proxy Port field.

Step 3 Click **Save**.

Next Steps

Once you have specified your proxy settings, you can optionally enable the following systemwide client provisioning functions:

- Enabling and Disabling the Client Provisioning Service, page 19-26
- Downloading Client Provisioning Resources Automatically, page 19-27

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

System Time and NTP Server Settings

Cisco ISE allows you to view the system time settings through the administrator user interface. The Cisco Application Deployment Engine (ADE) operating system, which is the operating system in the Cisco ISE, allows you to configure up to three Network Time Protocol (NTP) servers. You can use the NTP servers to maintain accurate time and synchronize time across different timezones. This procedure ensures that your logs are always reliable. You can also specify whether or not Cisco ISE should use only authenticated NTP servers, and you can enter one or more authentication keys for that purpose.

Note You must configure the system time and NTP server settings on each ISE node in your deployment individually.

Prerequisite:

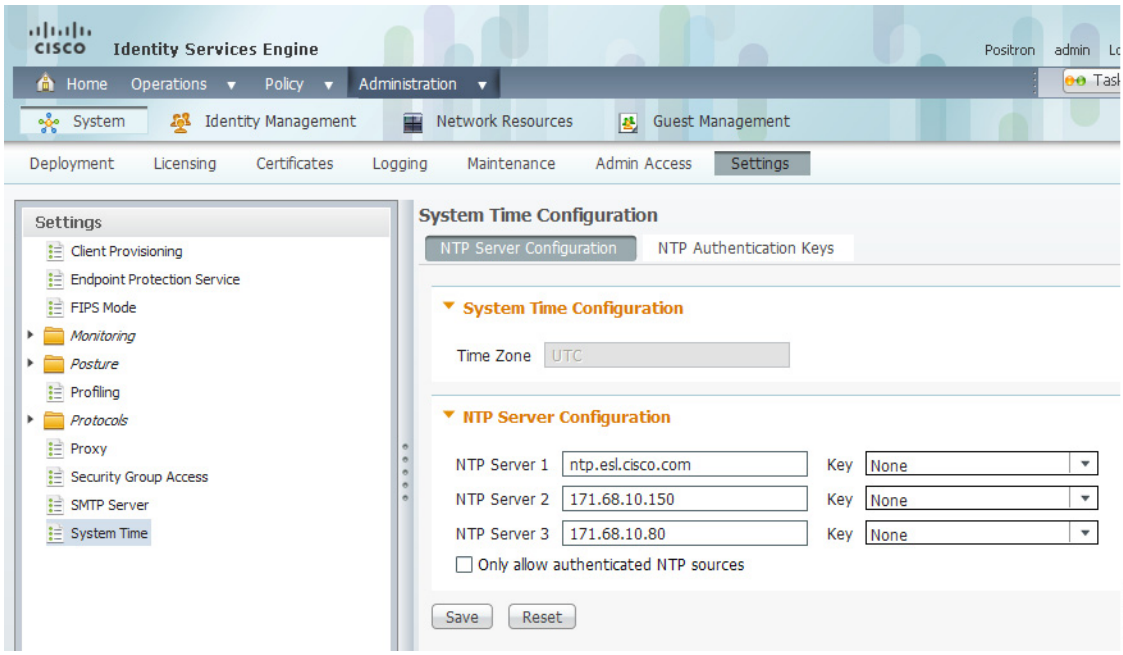
Every ISE administrator account is assigned one or more administrative roles. To perform the operations that are described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See "Cisco ISE Admin Group Roles and Responsibilities" for more information on the various administrative roles and the privileges that are associated with each of them.

To view the system time settings and configure NTP server settings, complete the following steps:

Step 1 From your primary ISE node, choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **System Time**.

Figure 8-19 Administration > System > Settings > System Time



Note If you want to view the system time settings and configure NTP server settings on a secondary Cisco ISE node, you must log into the user interface of the secondary node and choose **Administration > System > Settings > System Time**.

The timezone that you have configured appears in the Time Zone field. You cannot edit this value from the ISE user interface. To configure the timezone, you must enter the following command from the ISE CLI:

clock timezone *timezone*

For more information on the **clock timezone** command, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

Step 3 In the NTP Server Configuration area, enter the IP address of your NTP servers.

If you have only one NTP server in your network, enter the IP address in the Primary Server text box. If you have two NTP servers, enter the IP address in the **NTP Server 1** and **NTP Server 2** text boxes, respectively.

Note If you enter the same IP address for NTP server 1 and 2, then when NTP server 1 is down, Cisco ISE cannot access any other NTP server, because you have specified the same identity as the "other" NTP server. Cisco recommends that you verify the IP address of NTP server 2 and ensure that it is different than NTP server 1.

Step 4 If you want to restrict Cisco ISE to use only authenticated NTP servers to keep system and network time, check (enable) the **Only allow authenticated NTP servers** check box.

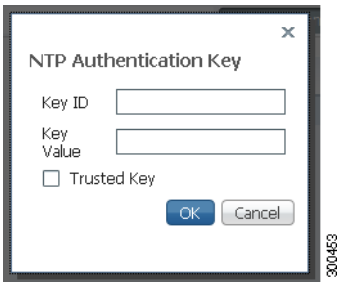
Step 5 If any of the servers that you specify requires authentication via an authentication key, be sure to also click the **NTP Authentication Keys** tab and specify one or more authentication keys, as follows:

a. Click **Add**.

b. Enter the necessary **Key ID** and **Key Value**, and specify whether the key in question is trusted by activating or deactivating the **Trusted Key** option.

c. Click **OK**.

Figure 8-20 Administration > System > Settings > System Time



d. When you are finished entering the NTP Server Authentication Keys, return to the **NTP Server Configuration** tab.

Step 6 Click **Save** to save the NTP server settings.

The saved NTP Authentication Keys are displayed in the NTP Server Configuration page, and when you place your cursor over to the hostname in the top right corner of the Cisco ISE dashboard window, the current server role and server system time appear in the Server Information quick-view pop-up.

Note We recommend that you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

Configuring Email Settings

This section shows you how to specify the address of the email server and the name that is displayed for this address. This address is used for sending and receiving log messages.

Note Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. For more information, see Understanding the Impact of Roles and Admin Groups.

To specify email settings for the mail server, complete the following steps:

Step 1 Select **Administration > System > Settings**

Step 2 In the left-hand Settings panel, expand **Monitoring** and then choose **Email Settings**.

Step 3 In the Mail Server field, enter the hostname or IPV4 address of the outgoing SMTP mail server. This information is required to send email notifications for alarms.

Note A hostname requires a format such as mailman.cisco.com. An IPv4 address requires a format such as, 192.168.1.1.

Step 4 Enter a name or email address (such as admin@somedomain.com) in the Mail From field. This name or email address is what users see when they receive a message from the mail server.

Step 5 Click **Submit.**

Configuring System Alarm Settings

System alarms notify you of critical conditions that are encountered. System alarms are standard and cannot be created or deleted.

This section describes the available system alarms, shows you how to enable and disable the alarms, and how to configure to receive notification. Cisco ISE provides the following system alarms:

- Distributed Management—This alarm is sent during the following operations:
  - Registering a node (Success or Failure)
  - Deleting a node
  - Unregistering a node (Success or Failure)
  - Updating a node (Success or Failure)
- License Enforcement—This alarm is sent when the number of concurrent endpoints or users exceed the total amount allowed for a particular license.
- Software Management—This alarm is sent during the following operations:
  - Patch Installation (Success or Failure) on a node
  - Patch Rollback (Success or Failure) on a node
- Purging Failed—This alarm is sent whenever a purge fails.
- Collector—This alarm is sent whenever collection failures occur.
- Alarm Manager—This alarm is sent when the **Alarm** manager cannot complete monitoring of all thresholds.
- Backup Failed—This alarm is sent whenever there is backup failure.
- DNS Resolution Failed—This alarm indicates that you are not using a proper DNS server, or your host is not defined in the DNS server that you are using. Both of these lead to DNS resolution failure. For Cisco ISE to work properly, you should use DNS servers and have your host resolvable from DNS.

You can choose to send alarm notifications through email and as syslog messages. To send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. For more information, see Configuring Alarm Syslog Targets.

Enabling and Configuring System Alarms

The following task shows you how to activate and configure notification for system alarms.

To enable and configure a system alarm, complete the following steps:

Step 1 Select **Administration > System > Settings**.

Step 2 In the left Settings panel, expand **Monitoring** and then choose **System Alarm Settings**.

Step 3 Check the **Notify System Alarms** check box. A green check mark appears to show that the option has been activated.

Step 4 Designate the number of hours to suppress duplicate system alarms from being sent to the Email Notification User List.

Step 5 To request Email Notification, enter a valid email address in the text field. Then, check the **Email in HTML Format** check box, as desired.

When a system alarm occurs, an email is sent to all the recipients in the Email Notification User List.

Step 6 To request Syslog Notification, check the **Send Syslog Message** check box.

Step 7 Click **Submit** to apply the settings.

For more information:

See the System Alarm Settings section of Appendix A, "User Interface Reference."

Disabling System Alarms

The following task shows you how to deactivate system alarms.

To disable system alarms, complete the following steps:

Step 1 Select **Administration > System > Settings**.

Step 2 In the left Settings panel, expand **Monitoring** and then choose **System Alarm Settings**.

Step 3 Uncheck the **Notify System Alarms** check box. The green check mark disappears to show that the option has been deactivated.

For more information:

See the System Alarm Settings section of Appendix A, "User Interface Reference."

Configuring Alarm Syslog Targets

This section shows you how to create, edit, and delete alarm syslog targets.

If you configure system alarm notifications to be sent as syslog messages, then you need a syslog target to receive the notification. Alarm syslog targets are the destinations to which alarm syslog messages are sent. A system that is configured as a syslog server is also required to receive syslog messages.

Creating and Editing Alarm Syslog Targets

When you create or edit an alarm syslog target, you establish or modify the destination to which syslog messages are sent.

To create and edit an alarm syslog target, complete the following steps:

Step 1 Select **Administration > System > Settings**.

Step 2 In the left Settings panel, expand **Monitoring** and then choose **Alarm Syslog Targets**.

Step 3 To create an alarm syslog target, do the following:

a. Click **Create**.

b. Enter a unique name in the Name field and a meaningful description in the Description field.

c. Enter a valid IP address in the IP Address field and click **Submit**.

The newly created alarm syslog target appears in the list.

Step 4 To edit an alarm syslog target, do the following:

a. Click the alarm syslog target Name link from the list.

b. Modify the Name and Description, as necessary.

c. Change the IP Address as needed, and click **Submit.**

Your changes are applied to the alarm syslog target.

For more information:

See the Alarm Syslog Targets section of Appendix A, "User Interface Reference."

Deleting Alarm Syslog Targets

You can delete an alarm syslog target at any time.

To delete an alarm syslog target, complete the following steps:

Step 1 Select **Administration > System > Settings**.

Step 2 In the left Settings panel, expand **Monitoring** and then choose **Alarm Syslog Targets**.

Step 3 Check the check box next to the alarm syslog target that you want to delete. A green check mark appears to show that it is selected.

Step 4 Click **Delete**, and then click **Yes** in the dialog prompt to confirm the deletion.

For more information:

See the Alarm Syslog Targets section of Appendix A, "User Interface Reference."

Managing Software Patches

You can install patches on ISE servers in your deployment from the primary administration node. ISE patches are usually cumulative, however, any restrictions on the patch installation will be described in the *README* file that will be included with the patch. Cisco ISE allows you to perform patch installation and rollback from either the command-line interface (CLI) or GUI.

When you install or roll back a patch from a standalone or primary administration node, ISE restarts the application. You might have to wait for a few minutes before you can log back in.

Note When you install or roll back a patch from the primary administration node that is part of a distributed deployment, Cisco ISE installs the patch on the primary and all the secondary nodes in the deployment. If the patch installation is successful on the primary node, Cisco ISE then proceeds to the secondary nodes. If it fails on the primary node, the installation is aborted. However, if the installation fails on any of the secondary nodes for any reason, it still continues with the next secondary node in your deployment.

To roll back a patch from ISE nodes in a deployment, you must roll back the change from the primary node and if successful, the patch is rolled back from the secondary nodes. If it fails on the primary node, the rollback process is aborted. However, if it fails on any of the secondary nodes, it still continues to roll back the patch from the next secondary node in your deployment.

Note You cannot install a patch whose version is lower than the patch that is currently installed on ISE. Similarly, you cannot roll back changes of a lower version patch if a higher version is currently installed on Cisco ISE. For example, if patch 3 is installed on your ISE servers, you cannot install patch 1 or 2, or roll back patch 1 or 2.

To install and roll back patches from the CLI, refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

This section contains:

- Installing a Software Patch, page 8-24
- Rolling Back Software Patches, page 8-28
- Viewing Patch Install and Rollback Changes in the Audit Report, page 8-29

Installing a Software Patch

To install a patch from the GUI, you must download the patch from the following location to the system that runs your client browser:

Note Cisco ISE allows you to install a patch on an Inline Posture node only through the CLI.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To install a patch on Cisco ISE nodes in a deployment, complete the following steps:

Step 1 Choose **Administration > System > Maintenance > Patch Management**.

The Patch Management page appears, which lists the patches that are installed on your ISE node.

Step 2 Click **Install**.

The Install Patch Bundle page appears.

Step 3 Click **Browse** to choose the patch that you downloaded earlier.

Step 4 Click **Install** to install the patch.

Ensure that you install patches that are applicable for the Cisco ISE version that is deployed in your network. Cisco ISE reports any mismatch in versions and also any errors in the patch file.

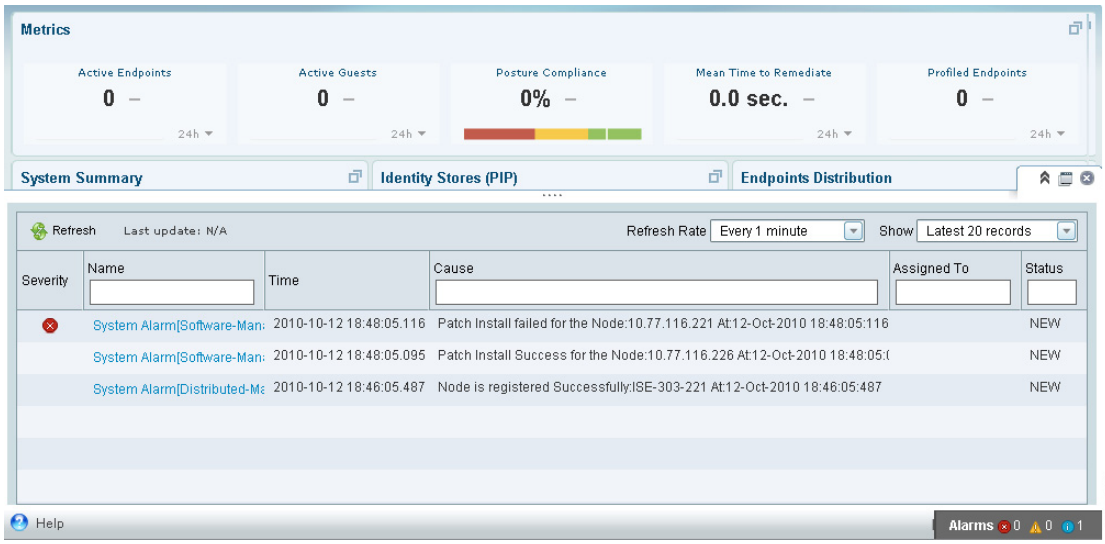
After the patch is installed on the primary administration node, Cisco ISE logs you out and you have to wait for a few minutes before you can log back in.

Note When patch installation is in progress, Show Node Status is the only option that is enabled in the Patch Management page.

Step 5 After you log back in, from the dashboard, click the **Alarms** link at the bottom of your screen as shown in Figure 8-21.

Note The alarms are generated only for patch install or rollback operations performed from the GUI. To view the status of patch installation from the CLI, you must check the *ade.log* file, which you can access by Downloading Support Bundles.

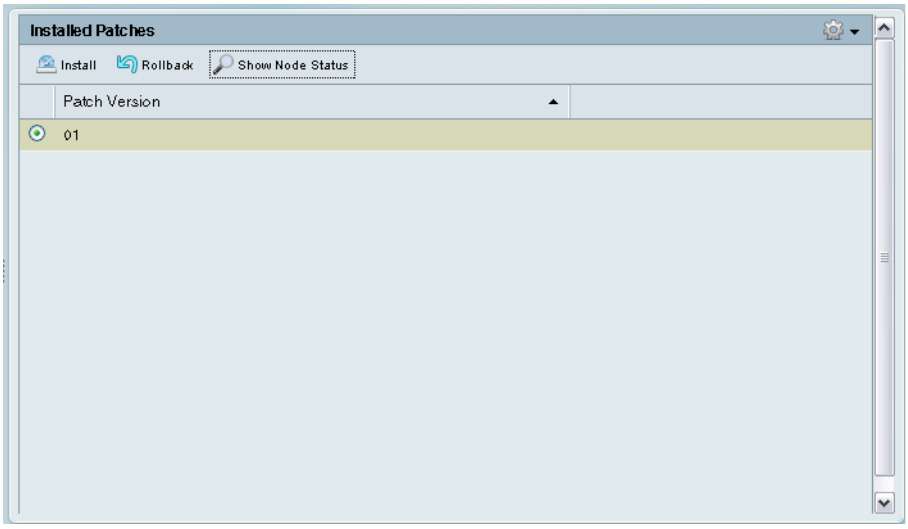
Figure 8-21 Patch Installation Status in the Dashboard



Step 6 You can go back to the Patch Installation page (choose **Administration > System > Maintenance > Patch Management**).

Step 7 The Installed Patches page appears as shown in Figure 8-22.

Figure 8-22 Patch Listing Page

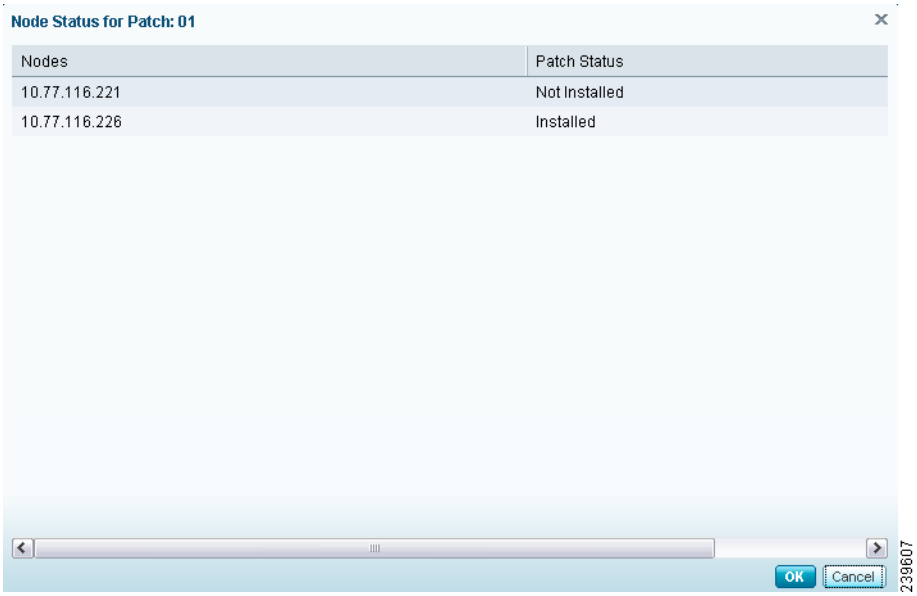


This page lists all the patches that you have installed so far.

Step 8 Click the radio button next to the patch whose status you want to view and click **Show Node Status**.

A pop-up appears that shows the status of this patch (Installed, Not Installed, or Node is Down) on the various nodes in your deployment as shown in Figure 8-23.

Figure 8-23 Node Status Pop-Up



Step 9 After the patch is installed on the primary node, ISE will install it on your secondary nodes consecutively.

While installing a patch on the secondary nodes, the primary administration node is not restarted and you can continue to perform your tasks on the primary administration node. During this time, the secondary ISE nodes are restarted consecutively after the patch is installed on those nodes. At any point during the installation process, you can click the **Show Node Status** button to see the status of patch installation.

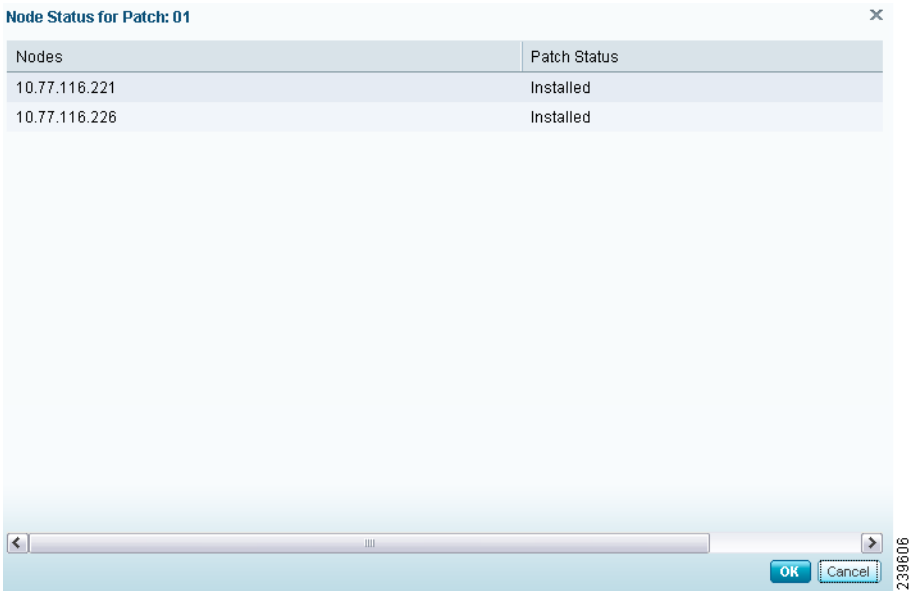
If for some reason, the patch installation fails on the primary administration node, the installation does not proceed to the secondary nodes.

Step 10 To check if the installation is complete, click the radio button next to the patch that you have installed and click **Show Node Status**.

Note The Node Status pop-up only provides information about patch installation on ISE nodes. Patch installation and rollback on Inline Posture nodes can only be done through the Cisco ISE CLI and this status will not be displayed in the Node Status pop-up.

A pop-up similar to the one shown in Figure 8-24 appears.

Figure 8-24 Node Status Pop Up: Installation Complete



Patch installation is now complete on all the ISE nodes.

If for some reason the patch is not installed on one or more secondary nodes, ensure that the node is up and repeat the process from Step 2 to install it on the remaining nodes. Cisco ISE installs the patch on those nodes that do not have this version of the patch.

Related Topics:

- Managing Software Patches, page 8-24
- Rolling Back Software Patches, page 8-28
- Viewing Patch Install and Rollback Changes in the Audit Report, page 8-29

Rolling Back Software Patches

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To roll back a patch from Cisco ISE nodes in your deployment, complete the following steps:

Step 1 Choose **Administration > System > Maintenance > Patch Management**.

The Installed Patches page appears.

Step 2 Click the radio button for the patch version whose changes you want to roll back, then click **Rollback**.

Note When patch rollback is in progress, Show Node Status is the only option that is enabled in the Patch Management page.

After the patch has been rolled back on the primary administration node, Cisco ISE will roll back the patch from the secondary nodes. If for some reason the patch rollback fails on the primary node, the patches are not rolled back from the secondary nodes.

After the patch is rolled back from the primary administration node, Cisco ISE logs you out and you have to wait for a few minutes before you can log back in.

Step 3 After you log in, click the **Alarms** link at the bottom of the dashboard screen to view the status of the rollback operation.

Note The alarms are generated only for patch install or rollback operations performed from the GUI. To view the status of patch installation from the CLI, you must check the *ade.log* file, which you can access by Downloading Support Bundles.

Step 4 Go back to the Installed Patches page (choose **Administration > System > Maintenance > Patch Management**) to check the status of this rollback on the other nodes in your deployment.

Step 5 If the patch rollback is in progress, this status will be visible in the Installed Patches page. To view the status of the patch rollback, you can choose the patch and click **Show Node Status**.

A pop-up appears that shows the status of the patch on the various ISE nodes in your deployment.

While Cisco ISE rolls back the patch from the secondary nodes, you can continue to perform other tasks from your primary administration node GUI. The secondary nodes will be restarted after the rollback.

Step 6 Click the radio button for the patch and click **Show Node Status** to ensure that the patch is rolled back from all the nodes in your deployment.

If the patch is not rolled back from any of the secondary nodes, ensure that the node is up and repeat the process from Step 2 to roll back the changes from the remaining nodes. Cisco ISE rolls back the patch only from those nodes that still have this version of the patch installed.

Related Topics:

- Managing Software Patches, page 8-24
- Installing a Software Patch, page 8-24
- Viewing Patch Install and Rollback Changes in the Audit Report, page 8-29

Viewing Patch Install and Rollback Changes in the Audit Report

The monitoring and troubleshooting component of Cisco ISE provides information on the patch installation and rollback operations that are performed on your ISE nodes.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Monitoring Admin or Helpdesk Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

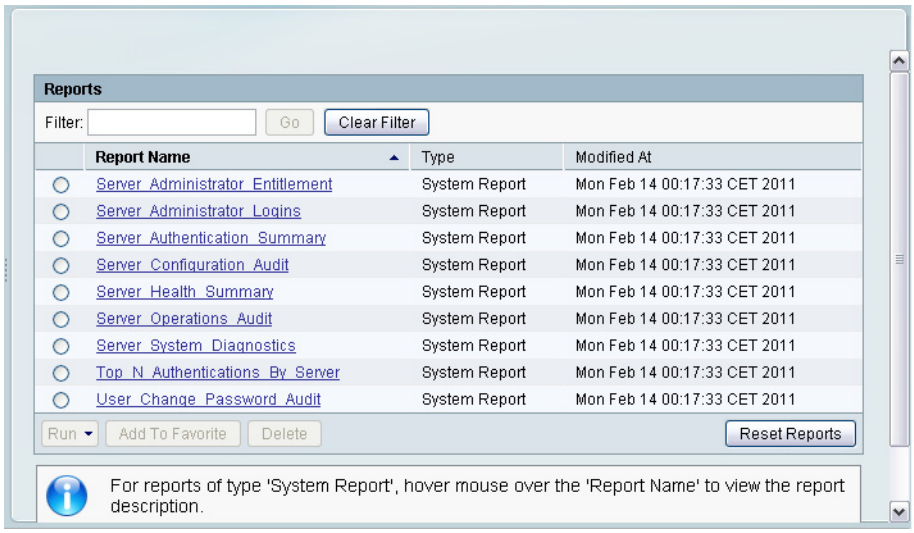
To view these reports, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog**.

Step 2 From the Reports navigation pane on the left, click **Server Instance**.

A page similar to the one shown in Figure 8-25 appears.

Figure 8-25 Server Instance Reports Page

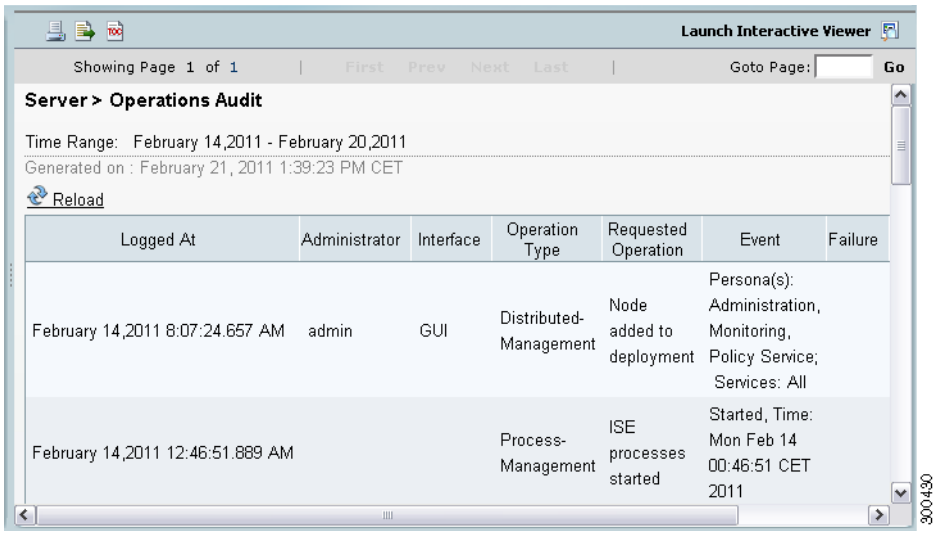


Step 3 Click the **Server Operations Audit** radio button, then click **Run** and choose the time period for which you want to generate the report.

Step 4 A report similar to the one shown in Figure 8-26 appears.

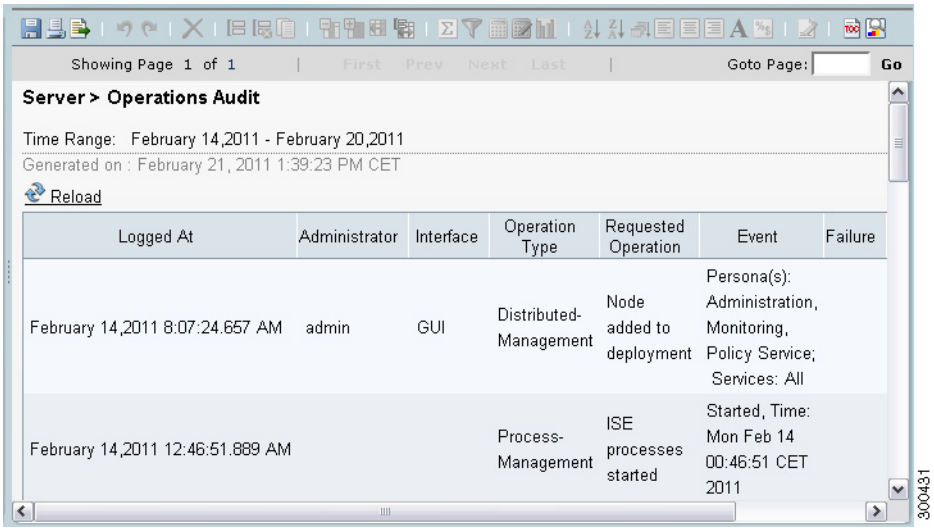
This report provides information on the patch installation and rollback operations that were performed within the time period that you have chosen.

Figure 8-26 ISE Operations Audit Report



Step 5 Click the Launch Interactive Viewer link in the upper right corner of the screen to view, sort, and filter the data in this report. A screen similar to the one that is shown in Figure 8-27 appears.

Figure 8-27 ISE Operations Report: Interactive View



For information on how to use the interactive viewer features, see the "Working with the Interactive Viewer Toolbar" section on page 24-12.

Related Topics:

- Managing Software Patches
- Installing a Software Patch
- Rolling Back Software Patches



CHAPTER 9

Setting Up Cisco ISE in a Distributed Environment

The Cisco Identity Services Engine (ISE) provides distributed deployment of runtime services with centralized configuration and management. Multiple nodes can be deployed together in a distributed fashion to support failover.

This chapter describes the type of nodes, personas, roles, and services that constitute Cisco ISE, and how to configure Cisco ISE nodes and create a Cisco ISE distributed environment.

For information about the Cisco ISE deployment scenarios, refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

This chapter covers the following topics:

- Understanding Node Types, Personas, Roles, and Services, page 9-2
- Understanding Distributed Deployment, page 9-5
- Guidelines for Setting Up a Distributed Deployment, page 9-6
- Configuring a Cisco ISE Node, page 9-7
- Registering and Configuring a Secondary Node, page 9-13
- Configuring Administration Cisco ISE Nodes for High Availability, page 9-15
- Viewing Nodes in a Deployment, page 9-17
- Managing Node Groups, page 9-19
- Changing Node Personas and Services, page 9-23
- Configuring Monitoring ISE Nodes for Automatic Failover, page 9-24
- Removing a Node from Deployment, page 9-26
- Changing the IP Address of the Monitoring Node, page 9-27
- Replacing the Cisco ISE Appliance Hardware, page 9-28

Note See Chapter 10, "Setting Up Inline Posture" for information on setting up an Inline Posture node on your network.

Understanding Node Types, Personas, Roles, and Services

Cisco ISE has a highly available and scalable architecture that supports standalone and distributed deployments. In a distributed environment, you configure one primary Administration ISE node to manage the secondary ISE nodes that are deployed onto the network. This section covers the following topics:

- Cisco ISE Deployment Terminology, page 9-2
- Types of Nodes, page 9-2
- Cisco ISE Nodes and Available Menu Options, page 9-4

Cisco ISE Deployment Terminology

This section describes some of the common terms used in ISE deployment scenarios. Table 9-1 lists these terms and their descriptions.

Table 9-1 Cisco ISE Deployment Terminology

Term	Description
Service	A service is a specific feature that a persona provides such as network access, profiler, posture, security group access, monitoring and troubleshooting, and so on.
Node	A node is an individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as a software that can be run on VMware. Each instance (appliance or VMware) that runs the Cisco ISE software is called a node.
Node Type	A node can be of two types: ISE node and Inline Posture node. The node type and persona determine the type of functionality provided by that node.
Persona	The persona or personas of a node determine the services provided by a node. An ISE node can assume any or all of the following personas: Administration, Policy Service, and Monitoring. The menu options that are available through the administrative user interface are dependent on the role and personas that an ISE node assumes. See Cisco ISE Nodes and Available Menu Options for more information.
Role	Determines if a node is a standalone, primary, or secondary node. Applies only to administration and Monitoring ISE nodes.

Types of Nodes

In a Cisco ISE distributed deployment, there are two types of nodes. These include:

- ISE node—An ISE node could assume any of the following personas:
  - Administration—Allows you to perform all administrative operations on Cisco ISE. It handles all system-related configuration and configurations that are related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have only one or a maximum of two nodes running the administration persona. The administration

persona can take on any one of the following roles: Standalone, Primary, or Secondary. If the primary Administration ISE node goes down, you have to manually promote the secondary Administration ISE node. There is no automatic failover for the Administration persona.

Note At least one node in your distributed setup should assume the Administration persona.

- Policy Service—Provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assume this persona. Typically, there would be more than one Policy Service ISE node in a distributed deployment. All Policy Service ISE nodes that reside behind a load balancer share a common multicast address and can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes detect the failure and reset any pending sessions.

Note At least one node in your distributed setup should assume the Policy Service persona.

- Monitoring—Enables Cisco ISE to function as the log collector and store log messages from all the administration and Policy Service ISE nodes in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources. A node with this persona aggregates and correlates the data that it collects to provide you with meaningful information in the form of reports. Cisco ISE allows you to have a maximum of two nodes with this persona that can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring ISE nodes collect log messages. In case the primary Monitoring ISE node goes down, the secondary Monitoring ISE node automatically becomes the primary Monitoring ISE node.

Note At least one node in your distributed setup should assume the Monitoring persona. We recommend that you not have the Monitoring and Policy Service personas enabled on the same Cisco ISE node. We recommend that the node be dedicated solely to monitoring for optimum performance.

- Inline Posture node—A gatekeeping node that is positioned behind network access devices such as wireless LAN controllers (WLC) and virtual private network (VPN) concentrators on the network. Inline Posture enforces access policies after a user has been authenticated and granted access, and handles change of authorization (CoA) requests that a WLC or VPN are unable to accommodate. Cisco ISE allows you to have two Inline Posture nodes that can take on primary or secondary roles for high availability. For more information, see Chapter 10, “Setting Up Inline Posture”

Note An Inline Posture node is dedicated solely to that service, and cannot operate concurrently with other ISE services. Likewise, due to the specialized nature of its service, an Inline Posture node cannot assume any persona. For example, it cannot act as an Administration ISE node (that offers administration service), or a Policy Service ISE node (that offers network access, posture, profile, and guest services), or a Monitoring ISE node (that offers monitoring and troubleshooting services) for an ISE network.

Each node in a deployment, with the exception of the Inline Posture node, can assume the Administration, Policy Service, and Monitoring personas. The Inline Posture node must be a dedicated node.

In a distributed deployment, you can have the following combination of nodes on your network:

- Primary and secondary Administration ISE nodes for high availability
- A pair of Monitoring ISE nodes for automatic failover
- One or more Policy Service ISE nodes for session failover
- A pair of Inline Posture nodes for high availability

Cisco ISE Nodes and Available Menu Options

The menu options that are available for Cisco ISE nodes that are part of a distributed deployment depend on the personas that are enabled on them. All administration and monitoring activities should be performed through the administrative user interface of the primary Administration ISE node. Some of the operations, though, need to be performed on the secondary nodes. Hence the administrative user interface of the secondary nodes provides limited menu options based on the personas that have been enabled on them. Table 9-2 lists the nodes and the menu options that are available through the administrative user interface. If a node assumes more than one persona, for example, the Policy Service persona, and a Monitoring persona with an Active role, then the menu options listed for Policy Service ISE nodes and Active Monitoring ISE node will be available on that node.

Note After you have registered your secondary nodes to your primary Administration ISE node, while logging into the administrative user interface of any of the secondary nodes, you must use the login credentials of the primary Administration ISE node.

Table 9-2 Cisco ISE Nodes and Available Menu Options

Node and Persona	Menu Options
All Nodes	Options to: • View and configure system time and NTP server settings. • Install server certificate, manage certificate signing request. **Note** The server certificate operations must be performed directly on each individual node. The private keys are not stored in the local database and are not copied from the relevant node; the private keys are stored in the local file system.
Primary Administration ISE Node	All options.
Active Monitoring ISE Node	Access to Home and Operations menus. Provides redundant access to monitoring data that can be accessed from both the Primary and the Active Monitoring ISE nodes.

Table 9-2 Cisco ISE Nodes and Available Menu Options (continued)

Node and Persona	Menu Options
Policy Service ISE Nodes	Option to join, leave, and test Active Directory connection. **Note** Each Policy Service ISE node must be separately joined to the Active Directory domain. You must first define the domain information and join the primary Administration ISE node to the Active Directory domain. Then, join the other Policy Service ISE nodes to the Active Directory domain individually.
Secondary Administration ISE Node	Option to promote the secondary Administration ISE node to become the primary Administration ISE node.

Understanding Distributed Deployment

A Cisco ISE distributed deployment consists of one primary Administration ISE node and multiple secondary nodes. Each ISE node in a deployment can assume any of the following personas: Administration, Policy Service, and Monitoring.

Note The Inline Posture node cannot assume any other persona, due to its specialized nature. The Inline Posture node must be a dedicated node. For more information, see Chapter 10, "Setting Up Inline Posture"

After you install Cisco ISE on all your nodes, as described in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*, the nodes come up in a standalone state. You must then define one node as your primary Administration ISE node. While defining your primary Administration ISE node, you must enable the Administration and Monitoring personas on that node. You can optionally enable the Policy Service persona on the primary Administration ISE node. After you complete the task of defining personas on the primary Administration ISE node, you can then register other secondary nodes to the primary Administration ISE node and define personas for the secondary nodes.

Note There must be at least one Monitoring ISE node in a distributed deployment. At the time of configuring your primary Administration ISE node, you must enable the Monitoring persona. After you have registered a secondary Monitoring ISE node in your deployment, you can edit the primary Administration ISE node and disable the Monitoring persona, if required.

When you register an ISE node as a secondary node, Cisco ISE immediately creates a database link from the primary to the secondary node and begins the process of replication. Replication is the process of sharing ISE configuration data from the primary to the secondary nodes. Replication ensures consistency among the configuration data present in all the ISE nodes that are part of your deployment.

A full replication typically occurs when you first register an ISE node as a secondary node. An incremental replication occurs after a full replication, and ensures that any new changes such as additions, modifications, or deletions to the configuration data in the primary Administration ISE node

are reflected in the secondary nodes. The process of replication ensures that all ISE nodes in a deployment are in sync. You can view the status of replication from the deployment pages of the ISE administrative user interface.

The Policy Service ISE nodes that reside in a single location behind a load balancer and share a common multicast address can be grouped together. In such scenarios, you can define node groups and assign the nodes to the particular group. See the "Managing Node Groups" section on page 9-19 for information on how to manage node groups.

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the primary Administration ISE node, the status of the deregistered node changes to standalone and the connection between the primary and the secondary node will be lost. Replication updates are no longer sent to the deregistered standby node.

Note You cannot deregister a primary Administration ISE node.

See Chapter 10, "Setting Up Inline Posture" for information on how to deregister Inline Posture nodes.

The application server in an ISE node restarts when you make any of the following changes:

- Register a node (Standalone to Secondary)
- Deregister a node (Secondary to Standalone)
- Primary node is changed to Standalone (if no other nodes are registered with it; Primary to Standalone)
- Administration ISE node is promoted (Secondary to Primary)
- Change the personas (when you assign or remove the Policy Service or Monitoring persona from a node)
- Modify the services in the Policy Service ISE node (enable or disable the session and profiler services)
- Restore a backup on the primary and a sync up operation is triggered to replicate data from primary to secondary nodes

Note When you make any of the above changes, the application services are restarted. You must expect a delay while these services restart.

Guidelines for Setting Up a Distributed Deployment

Read the following statements carefully before you set up Cisco ISE in a distributed environment:

- There are two types of nodes in a Cisco ISE distributed deployment: the ISE node and the Inline Posture node. An ISE node can assume the Administration, Policy Service, and Monitoring personas at the same time. An ISE node can be a primary, secondary, or standalone node.
- The Administration, Policy Service, and Monitoring personas will be enabled by default in a standalone ISE node.
- You must first configure a primary Administration ISE node and then register secondary nodes to set up a distributed deployment.

- There can be only one primary ISE node in a distributed deployment and it must assume the Administration persona. You can have a maximum of two ISE nodes that assume the Administration persona, one being your primary and the other a secondary node.
- All Cisco ISE system-related configuration and configuration related to functionality should be done only on the primary Administration ISE node. The configuration changes that you perform on the primary Administration ISE node is replicated to all the secondary nodes in your deployment.
- In order to avoid timezone issues among the nodes, you must provide the same NTP server name during the setup mode of each node.
- When the primary Administration ISE node goes down, you must log into the user interface of the secondary Administration ISE node and make it the primary node.
- The Inline Posture node requires a dedicated node. No other persona or service can run on a node that is designated as an Inline Posture node.
- A properly configured Domain Name System (DNS) server is required for a distributed deployment to work correctly. You must enter the IP addresses and fully qualified domain names (FQDNs) of the ISE nodes that are part of your distributed deployment in the DNS server.
- If you want to uninstall Cisco ISE from a secondary node, you must first deregister it from the primary Administration ISE node. You can then reimage the standalone node and reregister it with the primary Administration ISE node.

Configuring a Cisco ISE Node

After you install an ISE node, all the default services provided by the Administration, Policy Service, and Monitoring personas will run on it. This node will be in a standalone state. You must log into the administrative user interface of the ISE node to configure it. You cannot edit the personas or services of a standalone ISE node. You can, however, edit the personas and services of ISE nodes that are part of a distributed setup.

Note If you are logging into the node for the first time, you must change the default administrator password and install a valid license. For more information on these tasks, see *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

Note If you are logging into the secondary Administration ISE node to promote it as your primary Administration ISE node, see "Configuring Administration Cisco ISE Nodes for High Availability" section on page 9-15.

Note It is recommended not to change the host name and the domain name on Cisco ISE that have been configured or in production. If it is required, then reimage the appliance, make changes, and configure the details during the initial deployment.

Prerequisites:

Before you perform this task, you should:

- Have a basic understanding of how distributed deployments are set up in Cisco ISE. See the "Understanding Distributed Deployment" section on page 9-5 for more information.

- Read the "Guidelines for Setting Up a Distributed Deployment" section on page 9-6.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Note For a standalone Cisco ISE deployment, no specific node configuration is required. All the default personas and services are running on a newly installed Cisco ISE node.

To configure a Cisco ISE node, complete the following steps:

Step 1 From the ISE administrative user interface, choose **Administration > System > Deployment**.

Step 2 From the Deployment navigation pane on the left, click **Deployment**.

The Deployment List page appears.

Step 3 Check the check box next to the ISE node and click **Edit**.

The Node Edit page appears with a list of fields as described in Table 9-3.

Step 4 To set up Cisco ISE in a distributed environment, you must complete the following tasks:

a. Configuring a Primary Administration Cisco ISE Node, page 9-11

b. Registering and Configuring a Secondary Node, page 9-13

Troubleshooting Topics:

- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7

Description of the Fields in the Cisco ISE Node Edit Page

Table 9-3 describes the fields in the Cisco ISE Node Edit page.

Table 9-3 Cisco ISE Node Edit Page

Field	Description
Hostname	(Display only) Hostname of the ISE node.
FQDN	(Display only) The fully qualified domain name of the ISE node. For example, ise1.cisco.com.
IP Address	(Display only) IP address of the ISE node.
Node Type	(Display only) Could be any one of the following: • Identity Services Engine (ISE) • Inline Posture Node

Table 9-3 Cisco ISE Node Edit Page (continued)

Field	Description
Personas	
Administration	Check this check box if you want this ISE node to assume the Administration persona. **Note** You can enable the Administration persona only on nodes that are licensed to provide the administrative services. For more information, see Chapter 12, "Managing Licenses" • Role—(Display only) The role that the Administration persona has assumed in the deployment. Could take on any one of the following values: – Standalone – Primary – Secondary • Make Primary—Click this button to make this node your primary ISE node. You can have only one primary ISE node in a deployment. The other options on this page will become active only after you make this node primary. – You can have only two Administration ISE nodes in a deployment. If the node has a Standalone role, a Make Primary button appears next to it. – If the node has a Secondary role, a Promote to Primary button appears next to it. – If the node has a Primary role and there are no other nodes registered with it, a Make Standalone button appears next to it. You can click this button to make your primary node a standalone node.

Table 9-3 Cisco ISE Node Edit Page (continued)

Field	Description
Monitoring	**Note** To configure a Cisco ISE node on a VMware platform as your log collector, use the following guidelines to determine the minimum amount of disk space that you need: – 180 KB per endpoint in your network per day – 2.5 MB per Cisco ISE node in your network per day You can calculate the maximum disk space that you need based on how many months of data you want to have in your Monitoring ISE node. Check this check box if you want this ISE node to assume the Monitoring persona and function as your log collector. **Note** There must be at least one Monitoring ISE node in a distributed deployment. At the time of configuring your primary Administration ISE node, you must enable the Monitoring persona. After you have registered a secondary Monitoring ISE node in your deployment, you can edit the primary Administration ISE node and disable the Monitoring persona, if required. When you have only one Monitoring ISE node in your deployment, it will assume the standalone role. When you have two Monitoring ISE nodes in your deployment, Cisco ISE displays the name of the other monitoring and troubleshooting node for you to configure the Primary-Secondary roles. To configure these roles, from the Role drop-down list box, you can choose one of the following: • Primary—For the current node to be the primary Monitoring ISE node. • Secondary—For the current node to be the secondary Monitoring ISE node. • None—If you do not want the Monitoring ISE nodes to assume the primary-secondary roles. **Note** You can access the Monitoring menu from the primary Administration ISE node and the primary Monitoring ISE node in your deployment. Both the primary and secondary Monitoring ISE nodes receive Administration and Policy Service logs. You can have only two Monitoring ISE nodes in a deployment. If you configure one of your Monitoring ISE nodes as primary or secondary, the other Monitoring ISE node automatically becomes the secondary or primary node, respectively. If you change the role for one Monitoring ISE node to None, the role of the other Monitoring ISE node also becomes None, thereby cancelling the high availability pair. After you designate a node as a Monitoring ISE node, you will find this node listed as a syslog target in the following page: **Administration > System > Logging > Remote Logging Targets** All the other Administration and Policy Service ISE nodes will send their logs to this log collector. If you have two Monitoring ISE nodes defined, then you will find both of them listed as your log collectors.

Table 9-3 Cisco ISE Node Edit Page (continued)

Field	Description
Policy Service	When you check this check box, you must enable any one or all of the following services: • Check the Enable Session Services check box to enable network access, posture, guest, and client provisioning services. – Click the Include Node in Node Group drop-down list box to choose the group to which this Policy Service ISE node belongs. Choose <none> if you do not want this Policy Service ISE node to be part of any group. See Managing Node Groups for more information on node groups. **Note** All nodes within a node group should be Layer 2 adjacent (should be on the same subnet) and there should be multicast connectivity between the nodes. • Check the Enable Profiling Service check box to enable the Profiler service. If you enable the Profiling service, you must click the Profiling Configuration tab and enter the details as required. For more information, see Chapter 18, "Configuring the Probes" **Note** When you enable or disable any of the services that run on the Policy Service ISE node or make any changes to this node, you will be restarting the application server processes on which these services run. You must expect a delay while these services restart. You can determine when the application server has restarted on a node by using the **show application status ise** command from the CLI.

Configuring a Primary Administration Cisco ISE Node

To set up a distributed deployment, you must first configure an ISE node as your primary Administration ISE node.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure a primary Administration ISE node, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

Step 2 Click **Deployment** from the navigation pane on the left to launch the Deployment Nodes list page.

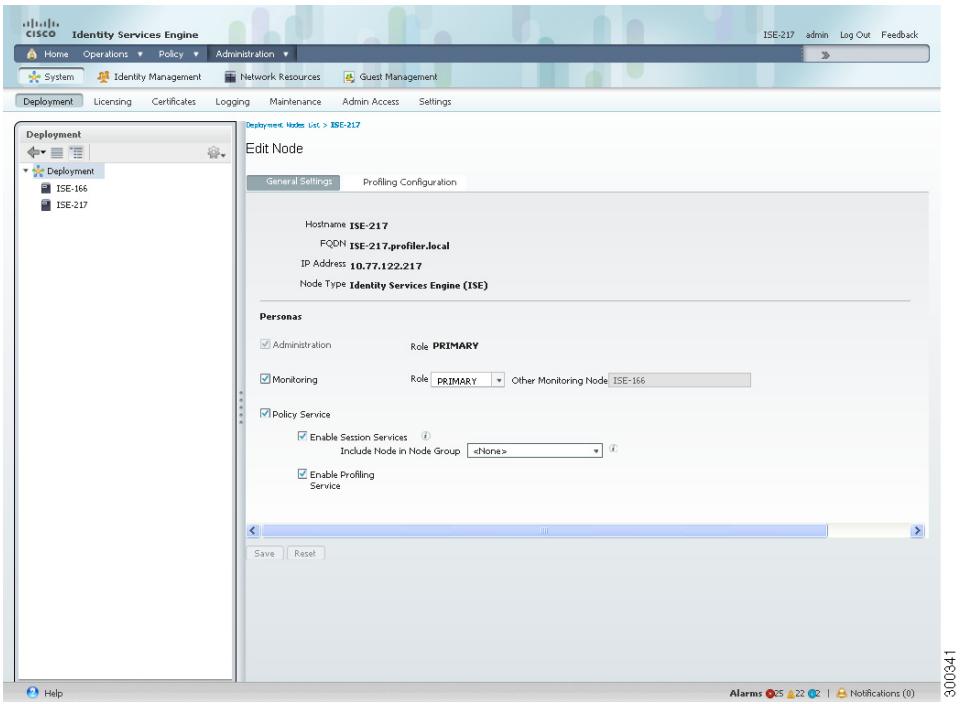
All the operations related to deployment can be performed from this page.

Note The Register button will be disabled initially. To enable this button, you must configure a primary Administration ISE node.

Step 3 Check the check box next to the current node and click **Edit**.

Step 4 The Edit Node page appears as shown in Figure 9-1.

Figure 9-1 Edit Node Page



Step 5 The Administration persona is enabled by default. Click the **Make Primary** button to configure your primary Administration ISE node.

Step 6 Enter data in the General Settings tab as described in Table 9-3.

Step 7 Click the **Profiling Configuration** tab if you have enabled the Profiler service, and configure the probes as described in the "Configuring the Probes" section on page 18-12.

Step 8 Click **Save** to save the node configuration.

Step 9 Click the **Deployment Node List** link at the top of this page or the Deployment link from the left navigation pane to go to the list page.

Next Step

To add secondary nodes to your deployment, you must successfully complete the task described in the "Registering and Configuring a Secondary Node" section on page 9-13.

Troubleshooting Topics

- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7

Registering and Configuring a Secondary Node

Note If you register a secondary Monitoring ISE node, it is recommended that you first back up the primary Monitoring ISE node, and then restore the data to the new secondary Monitoring ISE node. This ensures that the history of the primary Monitoring ISE node is in sync with the new secondary node as new changes are replicated. For more information, see Performing On-Demand Backups, page 23-50 and Restoring the Monitoring Database, page 23-51.

Prerequisites:

- The fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *ise1.cisco.com* must be DNS-resolvable from the primary Administration ISE node. Otherwise, node registration will fail. You must enter the IP addresses and FQDNs of the ISE nodes that are part of your distributed deployment in the DNS server.
- The primary Administration ISE node and the standalone node that you are about to register as a secondary node should be running the same version of Cisco ISE.
- You must configure the ISE Admin password at the time you install the Cisco ISE, Release 1.1. The previous ISE Admin default login credentials (admin/cisco) are no longer valid.
- Use the username/password that was created during the initial Setup or the current password, if it was changed later.
- The DB passwords of the primary and secondary nodes should be the same. If these passwords are set to be different during node installation, you can modify them using the following commands:
  - application reset-passwd ise internal-database-admin
  - application reset-passwd ise internal-database-user

  See the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more details on how to use the CLI commands.
- You can alternatively create an administrator account on the node that is to be registered and use those credentials for registering that node. Every ISE administrator account is assigned one or more administrative roles. To register and configure a secondary node, you must have either the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- If you plan to register a secondary Administration ISE node for high availability, we recommend that you register the secondary Administration ISE node with the primary first before you register other Cisco ISE nodes. If Cisco ISE nodes are registered in this sequence, you do not have to restart the secondary ISE nodes after you promote the secondary Administration ISE node as your primary.
- If you plan to register multiple Policy Service ISE nodes running Session services and you require mutual failover among those nodes, you must place the Policy Service ISE nodes in a node group. You must create the node group first before you register the nodes because you need to select the node group to be used on the registration page. See "Creating, Editing, and Deleting Node Groups" section on page 9-21 for more information.
- Ensure that the Certificate Trust List (CTL) of the primary node is populated with the appropriate Certificate Authority (CA) certificates that can be used to validate the HTTPS certificate of the standalone node (that you are going to register as the secondary node). See the "Creating Certificate Trust Lists in the Primary ISE Node" section on page 13-23 for more information.

- After registering your secondary node to the primary node, if you change the HTTPS certificate on the registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node's HTTPS certificate and import it to the CTL of the primary node. See "Creating Certificate Trust Lists in the Primary ISE Node" section on page 13-23 for more information.

Note We recommend that you set all Cisco ISE nodes to the same timezone. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

To register a secondary node, complete the following steps:

Step 1 Log into the primary Administration ISE node.

Step 2 Choose **Administration > System > Deployment**.

Step 3 Click **Deployment** from the navigation pane on the left.

The Deployment list page appears.

Step 4 After you have configured your primary Administration ISE node, do one of the following:

- Choose **Register > Register an ISE Node** to register a secondary ISE node. See the "Configuring a Cisco ISE Node" section on page 9-7 for information on how to configure your primary Administration ISE node.
- Choose **Register > Register an Inline Posture Node** to register a secondary Inline Posture node. For more information on deploying an Inline Posture node, see Chapter 10, "Setting Up Inline Posture."

Note We recommend that you decide on the type of node at the time of registration. If you want to change the node type later, you have to deregister the node from the deployment, restart Cisco ISE on the standalone node, and then reregister it.

Cisco ISE prompts you to enter the following information:

- Node hostname or IP address.
- User Name
- Password

Step 5 Enter a DNS-resolvable hostname or IP address of the secondary Cisco ISE node.

Note You must have defined the IP address and the FQDN of the secondary node in the DNS server.

Step 6 Enter a UI-based administrator credential for the standalone node in the Username and Password fields.

Before you register, the secondary node should be in the standalone state. After you register it to the primary, it begins to receive database updates from the primary. To view the status of the replication, you can go to the Deployment list page (**Administration > System > Deployment**) and look at the Replication Status information provided there.

Step 7 Click **Next** to go to the edit configuration page. Cisco ISE contacts the secondary node, obtains some basic information such as the hostname, default gateway, and so on, and displays it in this page.

If you have chosen to register a secondary ISE node, you can edit the configuration of the secondary node. See Next Step for information on the Administration, Monitoring, and Policy Service options.

If you have chosen to register a secondary Inline Posture node, no additional configuration needs to be performed at this point.

Step 8 Click **Save** to save the configuration.

After you register the secondary node, the configuration of the secondary node is added to the database of the primary node and the application server on the secondary node is restarted. After the restart is complete, the secondary node will be running the personas and services that you have enabled on it.

Result

After a secondary node is registered successfully, an alarm is generated on your primary Administration ISE node that confirms a successful node registration. If the secondary node fails to register with the primary Administration ISE node, the alarm is not generated. When a node is registered, the application server on that node is restarted. After successful registration and database synchronization, you must enter the credentials of the primary administrative node to log into the administrative user interface of the secondary node and perform any of the operations listed in Cisco ISE Nodes and Available Menu Options.

Next Steps

- For time-sensitive tasks such as time profiles, guest user access and authorization, logging, and so on, ensure that the system time on your nodes are synchronized. See the "System Time and NTP Server Settings" section on page 8-18 for information on how to synchronize the system time.
- To configure for high availability, you must complete the tasks described in the following sections:
  - Configuring Administration Cisco ISE Nodes for High Availability, page 9-15
  - Configuring Monitoring ISE Nodes for Automatic Failover, page 9-24
- To add an inline PEP node to your deployment, follow the instructions as described in the "Setting Up Inline Posture" section on page 10-1.

Configuring Administration Cisco ISE Nodes for High Availability

Cisco ISE allows you to have a maximum of two Administration ISE nodes in your deployment, for high availability. To create a high availability pair, you configure one Administration ISE node as primary active, and the other Administration ISE node a secondary standby.

High Availability

In a high availability configuration, the primary Administration ISE node is in the active state to which all configuration changes are made. The secondary Administration ISE node is in the standby state, and will receive all configuration updates from the primary Administration ISE node. Therefore, it will always have a complete copy of the configuration from the primary Administration ISE node.

When the primary Administration ISE node becomes unavailable, you must log into the secondary Administration ISE node and promote it to become the primary Administration ISE node. There is no automatic failover for the Administration ISE node.

Note When the primary Administration ISE node is down, Sponsor administrators cannot create new guest user accounts. During this time, the guest and sponsor portals will provide read-only access to already created guest and sponsor users, respectively. Also, a sponsor administrator who has never logged into the sponsor portal before the primary Administration ISE node went offline, will not be able to log into the sponsor portal until a secondary Administration ISE node is promoted or the primary Administration ISE node becomes available.

Prerequisites:

- Ensure that you have a second ISE node configured with the Administration persona before you can promote it to become your primary Administration ISE node.
- Before you configure the Administration ISE nodes for high availability, we recommend that you obtain a backup of the Cisco ISE configuration from the standalone node that you are going to register as a secondary Administration ISE node.
- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To promote the secondary Administration ISE node to become the primary, complete the following steps:

Step 1 Log into the user interface of the secondary Administration ISE node.

Step 2 Choose **Administration > System > Deployment**.

The Edit Node page appears.

Step 3 In the Edit Node page, click the **Promote to Primary** button.

Note You can only promote a secondary Administration ISE node to become a primary Administration ISE node. Cisco ISE nodes that assume only the Policy Service or Monitoring persona or both cannot be promoted to a primary Administration ISE node.

Step 4 Click **Save** to promote the secondary Administration ISE node to become the primary Administration ISE node.

Step 5 Restart the secondary Cisco ISE nodes (Policy Service and Monitoring nodes) that were registered with the primary Administration ISE node before the secondary Administration ISE node was registered.

For example, after you configure your primary Administration ISE node, you register a few Policy Service nodes, and then the secondary Administration ISE node followed by a few Policy Service nodes. In this case, if your primary Administration ISE node fails and you promote the secondary Administration ISE node to become your primary, then you must restart the Policy Service nodes that were registered before the secondary Administration ISE node was registered.

If the node that was originally the primary Administration ISE node comes back up again, it will become a secondary Administration ISE node.

From the Edit Node page of a secondary node, you cannot modify any persona or service. These options will be disabled. You have to log into the user interface of the primary Administration ISE node, choose the secondary node whose personas or services you want to change, and then click **Edit** to make these changes.

Note After you promote your secondary Administration ISE node to become the primary Administration ISE node, you must reconfigure your scheduled ISE backups in the newly promoted primary Administration ISE node because scheduled backups are not replicated from the primary to secondary Administration ISE nodes. See "Scheduled Backups" section on page 15-6 for more information.

Viewing Nodes in a Deployment

From the Deployment Nodes page, you can view all the Cisco ISE nodes that are part of your deployment (both the primary and secondary nodes).

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To view all the nodes, complete the following steps:

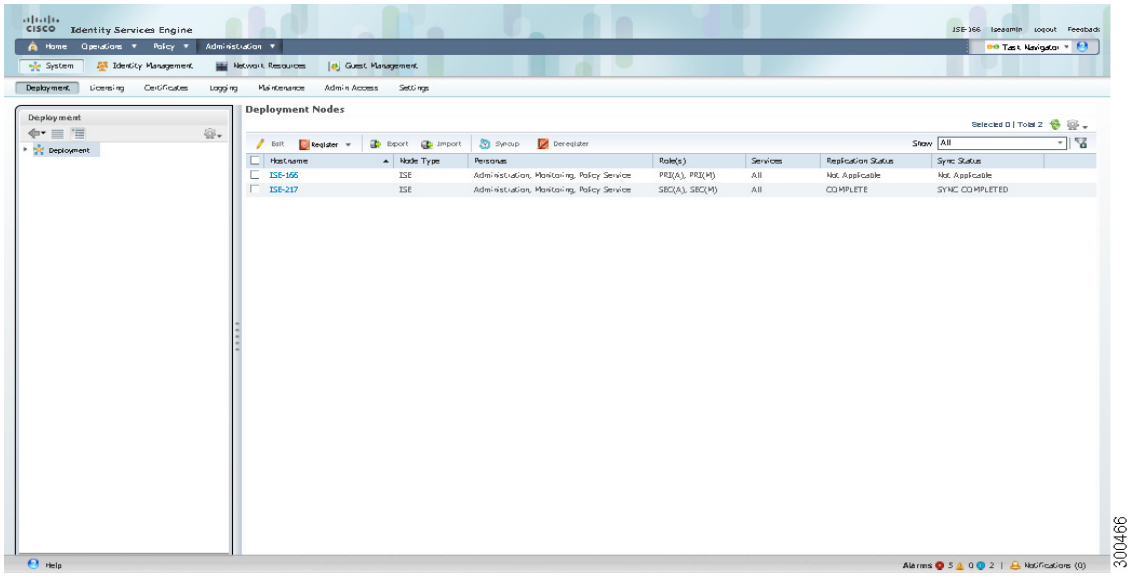
Step 1 Log into the primary or secondary ISE administrative user interface.

Step 2 Choose **Administration > System > Deployment**.

Step 3 Click **Deployment** from the navigation pane on the left.

The Deployment Nodes page appears with a list of nodes as shown in Figure 9-2.

Figure 9-2 Distributed Deployment Listing Page



This page provides the following information:

- Hostname—Hostname of the node.
- Node Type—The node type can be one of the following:
  - ISE
  - Inline Posture node.
- Personas—(Only appears if the node type is ISE) Lists the personas that an ISE node has assumed. For example, Administration, Policy Service.
- Role—Indicates the role (primary, secondary, or standalone) that the Administration and Monitoring personas have assumed, if these personas are enabled on this node. The role can be any one or more of the following:
  - PRI(A)—Refers to a primary Administration ISE node
  - SEC(A)—Refers to a secondary Administration ISE node
  - PRI(M)—Refers to a primary Monitoring ISE node
  - SEC(M)—Refers to a secondary Monitoring ISE node
- Services—(Only appears if the Policy Service persona is enabled) Lists the services that run on this ISE node. Services can include any one of the following:
  - Session
  - Profiling
  - All
- Replication Status—(Only appears for secondary ISE nodes) Indicates whether incremental replication from the primary Administration ISE node to the secondary node is complete or not. You will see one of the following states:
  - Failed—Incremental database replication has failed.
  - In-Progress—Incremental database replication is currently in progress.
  - Complete—Incremental database replication is complete.
  - Not Applicable—Displayed if the ISE node is a standalone or primary node.
  - Replication Disabled—Displayed if the certificate on that node gets expired or if the node is not reachable for more than 6 hours.
- Sync Status—(Only appears for secondary ISE nodes) Indicates whether full database replication from the primary Administration ISE node to the secondary node is complete or not. A full database replication happens when a node is registered as secondary or when you click Syncup to force a full database replication. You will see one of the following states:
  - Sync Completed—Full database replication is complete.
  - Sync in Progress—Database replication is currently in progress.
  - Out of Sync—Database was down when the secondary node was registered with the primary ISE node.
  - Not Applicable—Displayed if the ISE node is a standalone node.
  - Replication Disabled—Displayed if the certificate on that node gets expired or if the node is not reachable for more than 6 hours. In such a case, a manual sync needs to be done on the node.

Step 4 If the sync status for any secondary node is out of sync, check the check box next to that node and click **Syncup** to force a full database replication.

Note You must use the Syncup option to force a full replication if the Sync Status is *Out of Sync* or the Replication Status is *Failed* or *Disabled*.

From this page, you can do the following:

- Edit a node. This option is enabled only when you choose a single node. After you choose a node, click the Edit button to edit the personas and roles of that node.
- Register a secondary node. This option is enabled only after you configure a primary Administration ISE node. Click the Register button to register an ISE or Inline Posture node.
- Initiate a full database replication from the primary to the selected secondary nodes.
- Deregister one or more secondary nodes.

Troubleshooting Topics

- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7

Managing Node Groups

In distributed deployments, you might have multiple Policy Service ISE nodes located behind a load balancer to distribute the requests evenly. The load balancer distributes load to the functional nodes behind it. Also, in order to detect node failure and to reset sessions in pending state on the failed node, two or more Policy Service ISE nodes can be placed in the same node group. When a node that belongs to a node group goes down, another node in the same node group issues a CoA for pending sessions on the failed node.

Note A session is said to be in the pending state if it has been authorized, but posture assessment is not yet complete. It is possible to set up a distributed deployment without node groups, but sessions in pending state on a failed Policy Service ISE node will not be automatically reset.

All the nodes in a node group share the same multicast address and use it to communicate their health status.

Session Failover in Policy Service ISE Nodes

The heartbeat functionality in Cisco ISE handles session failover in Policy Service ISE nodes. When a Policy Service ISE node that has a few active sessions goes down, the endpoints are stuck in an intermediate state. Even if the posture agent detects that the Policy Service ISE node that it has been communicating with has gone down, it cannot re-initiate authorization. If the Policy Service ISE nodes are part of a node group, the nodes within a node group exchange heartbeats to detect node failures. If a node fails, one of its peers from the node group learns about the active sessions on the failed node and issues a CoA to disconnect those sessions. As a result, restarts and the sessions are handled by another Policy Service ISE node that is available using RADIUS load balancing. The session failover does not automatically move the sessions over from a Policy Service ISE node that has gone down to one that is available, but issues a CoA to achieve that.

Note The PDP nodes in a distributed deployment do not share their Machine Access Restriction (MAR) cache with each other. For example, If a client machine is authenticated by one of the Policy Service ISE nodes, PDP1 and PDP1 goes down, then another Policy Service ISE node in the deployment, PDP2 handles the user authentication. The user authentication in this case fails because PDP2 does not have the host authentication information in its MAR cache.

All the nodes in a node group must be configured on the network access device (NAD) as RADIUS clients to issue a CoA. Typically, these nodes would also be configured as RADIUS servers. See the "Enable RADIUS Change of Authorization (CoA)" section on page C-4 for CoA-related configuration on the switch.

While a single NAD can be configured with many ISE nodes (as RADIUS servers and dynamic-author clients), it is not necessary that all these nodes are in the same node group.

All the nodes within the same node group should be configured on the NAD as RADIUS servers and clients, because any one of them can issue a CoA request for the sessions that are established through that NAD to any node in the node group. The nodes in a node group should be the same as, or a subset of, the RADIUS servers and clients configured on the NAD.

For information about session failover in Policy Service ISE nodes, you can view the Server Operations Audit report (Operations > Reports > Catalog > Server Instance > Server Operations Audit).

Number of Nodes in a Node Group

The number of nodes that you can have in a node group depends on your deployment requirements. Node groups ensure that node failures are detected and that a peer issues a CoA for sessions that are authorized, but not yet postured. The size of the node group does not have to be very large.

If you want to minimize the number of node groups and thereby reduce the number of multicast addresses that must be managed, then you can group all the RADIUS servers and clients that are configured on the NADs as one node group.

If management of multiple multicast addresses is not a problem, but there is a need for minimizing multicast traffic, then you can have fewer nodes in a node group.

Note We recommend that you have two, three, or a maximum of four nodes in a node group.

If the size of the node group increases, the number of messages and heartbeats that are exchanged between nodes increases significantly. As a result, multicast traffic also increases. Having fewer nodes in a node group helps reduce the multicast traffic and at the same time provides sufficient redundancy to detect Policy Service ISE node failures.

You can create, edit, and delete node groups. You can perform these operations from the Deployment pages of the Cisco ISE administrative user interface.

This section contains the following topic:

- Creating, Editing, and Deleting Node Groups, page 9-21

Creating, Editing, and Deleting Node Groups

You can create and edit node groups in Cisco ISE.

Prerequisites:

- All nodes within a node group should be Layer 2 adjacent (should be on the same subnet). Layer 2 adjacent means that the nodes are connected to the same switch and are in the same VLAN.
- You must enable IP multicast between nodes that are part of the same node group. Typically, all the nodes in a node group will be connected to the same switch and be in the same VLAN.
- Two node groups cannot have the same multicast address.
- The multicast address that you assign to a node group should not be reserved for use by other network protocols in the deployment. Cisco ISE checks if the multicast address that you enter is a valid and allowed multicast address. It does not allow 224.0.0.0 to be used as a multicast address, but does not check for the reserved list of multicast addresses. For a list of reserved multicast addresses that you should not use, see http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create a node group, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

Step 2 Click **Deployment** from the navigation pane on the left.

Step 3 From the Deployment navigation pane on the left, click the action icon, and click **Create Node Group**.

The Create Node Group page appears.

Step 4 Enter a unique name for your node group.

Step 5 You can also enter an optional description.

Step 6 Enter a unique multicast address. The multicast address must be between 224.0.0.1 and 239.255.255.255.

Note The multicast address that you assign to a node group should not be reserved for use by other network protocols in the deployment. For a list of reserved multicast addresses, see http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml.

The multicast address is used to communicate between nodes in a group to monitor the health of the nodes and for session cleanup.

Step 7 Click **Submit** to save the node group.

Results

After you save the node group, it should appear in the navigation pane on the left. If you do not see the node group in the left pane, it may be hidden. Click the Expand button on the navigation pane to view the hidden objects.

Optional Steps:

- To add a node to a node group, you must edit the node and choose the node group from the Member of Node Group drop-down list box.
- To remove a node from a node group, you must edit the node and choose <none> from the Member of Node Group drop-down list box.

Troubleshooting Topics

- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7

To edit a node group, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

Step 2 From the Deployment navigation pane on the left, click the node group that you want to edit.

Note If you do not see the node group in the left pane, it may be hidden. Click the Expand button on the navigation pane to view the hidden objects.

The Edit Node Group page appears. You can only edit the description and multicast address.

Step 3 (Optional) Enter the new description.

Step 4 Enter the new multicast address. The multicast address should be unique.

Step 5 Click **Submit** to save the changes.

Optional Steps:

- To add a node to a node group, you must edit the node and choose the node group from the Member of Node Group drop-down list box.
- To remove a node from a node group, you must edit the node and choose <none> from the Member of Node Group drop-down list box.

Troubleshooting Topics

- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7

To delete a node group, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

Step 2 From the Deployment navigation pane on the left, click the node group that you want to delete.

The Edit Node Group page appears.

Step 3 Click the action icon from the navigation pane on the left and click **Delete Node Group**.

The following message appears:

Are you sure you want to delete?

Step 4 Click **OK** to delete the node group.

A confirmation message appears on your screen after the node group is deleted. Deleting a node group does not delete any of the nodes that belong to it. The nodes are simply dissociated from the group.

Troubleshooting Topics

- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7

Changing Node Personas and Services

You can edit the Cisco ISE node configuration to change the personas and services that run on the node. For example, on a node that profiles your devices, you can disable the services and enable them. However, you cannot add any services or roles to a node that is designated as an Inline Posture node.

Prerequisites:

- If you want to reuse an Inline Posture node, first deregister the node and reset the configuration of the node using the **application reset-config ise** command. Then, reregister the node as a new node.

  When an Inline Posture node is deregistered, it defaults to the Administration, Policy Service, and Monitoring personas that are in effect in a standalone state, and then restarts. When the node comes back up, it is returned to an Inline Posture node configuration.

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Note When you enable or disable any of the services that run on a Policy Service ISE node or make any changes to a Policy Service ISE node, you will be restarting the application server processes on which these services run. You must expect a delay while these services restart.

To change the roles and services of an ISE node, complete the following steps:

Step 1 Log into the primary Administration ISE node.

Step 2 Choose **Administration > System > Deployment**.

Step 3 Click **Deployment** from the navigation pane on the left.

The Deployment Nodes List page appears.

Step 4 Check the check box next to the node whose personas or services you want to change, then click **Edit**.

Step 5 Edit the node personas and services. See Table 9-3 for a description of the fields in the ISE Edit Node page.

Step 6 Click **Save** to save the changes.

After the persona or service change is saved successfully, an alarm is generated on your primary Administration ISE node that confirms the persona or service change. If the persona or service change is not saved successfully, the alarm is not generated.

Troubleshooting Topics

- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7
- Lost Monitoring and Troubleshooting Data After Registering Policy Service ISE Node to Administration ISE Node, page D-10

Configuring Monitoring ISE Nodes for Automatic Failover

The term automatic failover is used because high availability is not supported on Monitoring ISE nodes in the true sense. For Monitoring ISE nodes, operation audit data is duplicated by the Policy Service ISE node(s), which then sends copies to both the primary and secondary Monitoring ISE nodes.

Note Monitoring is served from the primary (active) Monitoring ISE node. Monitoring data is only served from the secondary (standby) Monitoring ISE node when the active node is down. The secondary Monitoring ISE node is read-only. For this reason, you are not allowed to make any configuration changes to a secondary Monitoring ISE node.

Automatic Failover Process

When a primary Monitoring ISE node goes down, the secondary Monitoring ISE node takes over all monitoring and troubleshooting information. The secondary node provides read-only capabilities, which means you cannot make configuration changes to that node.

To make configuration changes on the secondary node, the administrator must first manually promote the secondary node to a primary role. If the primary node comes back up after the secondary node has been promoted, it assumes the secondary role. If the secondary node was not promoted, the primary Monitoring ISE node will resume its role after it comes back up.

Warning **When the primary node comes back up after a failover, a manual backup and restore is required to update the primary node so it can reclaim the data that was lost.**

Configuring Primary and Secondary Monitoring ISE Nodes

You can specify two Monitoring ISE nodes on an ISE network and create an active-standby pair. Once the active-standby pair is defined, the following rules apply:

- All configuration changes must be made on the primary Monitoring ISE node. The secondary node is read-only.
- Configuration changes made to the primary node are automatically replicated on the secondary node.
- Both the primary and secondary nodes are listed as log collectors to which all other nodes send logs.
- The ISE dashboard is the main entry point for monitoring and troubleshooting. Monitoring information is displayed on the dashboard from the primary Monitoring ISE node. If the primary node goes down, the information is served from the secondary node.
- Backing up and purging monitoring data is not part of a standard ISE node backup process. You must configure repositories for backup and data purging on both the primary and secondary Monitoring ISE nodes, using the same repositories for each.

Note When you register a secondary Monitoring ISE node, it is recommended that you back up the primary Monitoring ISE node and then restore the data to the new secondary Monitoring ISE node. This ensures that the history of the primary Monitoring ISE node is in sync with the new secondary node as new changes are replicated. For more information, see Performing On-Demand Backups, page 23-50 and Restoring the Monitoring Database, page 23-51.

Prerequisites:

- Before you can configure two Monitoring ISE nodes for automatic failover, they must first be registered as ISE nodes, as described in Guidelines for Setting Up a Distributed Deployment, page 9-6 and Configuring a Cisco ISE Node, page 9-7.
- Specify monitoring roles and services on both nodes and name them for their primary and secondary roles, as appropriate.
- You must configure repositories for backup and data purging on both the primary and secondary Monitoring ISE nodes, using the same repositories for each. This is important for the backup and purging features to work properly. Purging takes place on both the primary and secondary nodes of a redundant pair. For example, if the primary Monitoring ISE node uses two repositories for backup and purging, you must specify the same repositories for the secondary node.

  You can configure a data repository for a Monitoring ISE node using the **repository** command in the system command line interface (CLI). For more information, see Backing Up and Restoring the Monitoring Database, page 23-45 and the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

Warning **For scheduled backup and purge to work properly on the nodes of a Monitoring redundant pair, you must configure the same repository, or repositories, on both the primary and secondary nodes using the CLI. The repositories are not automatically synced between the two nodes.**

To configure Monitoring ISE nodes for automatic failover, complete the following steps:

Step 1 From the ISE dashboard, verify that the Monitoring ISE nodes are ready.

The System Summary dashlet shows the Monitoring ISE nodes with a green check mark to the left when their services are ready.

Note Deployment changes may require the start of services. It can take a minute for the services to come up.

Step 2 Select **Administration > System > Deployment**.

Step 3 In the left panel, click **Deployment**.

Step 4 From the Deployment Nodes list, check the check box next to the Monitoring ISE node that you want to specify as active.

Step 5 Click the **Edit** icon.

Step 6 In the Personas panel, from the Role drop-down menu, choose **Primary**.

Note When you choose a Monitoring ISE node as primary, the other Monitoring ISE node automatically becomes secondary. In the case of a standalone deployment, primary and secondary role configuration is disabled.

Step 7 Click **Save**. The active and standby nodes restart.

Removing a Node from Deployment

To remove a node from the deployment, you must deregister it.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To remove a node from deployment, complete the following steps:

Note Before you remove any secondary node from the deployment, we recommend that you run a backup of Cisco ISE configuration, which you can then restore later on, if needed.

Step 1 Choose **Administration > System > Deployment**.

Step 2 Click **Deployment** from the navigation pane on the left.

Step 3 Check the check box next to the secondary node that you want to remove, then click **Deregister**.

The system prompts you with the following message:

Are you sure you want to deregister the selected items?

Step 4 Click **OK** to remove the node from the deployment.

The deregistered node now becomes a standalone ISE node. It retains the last configuration that it received from the primary Administration ISE node and assumes the default personas of a standalone node (Administration, Policy Service (session and profiling services), and Monitoring).

If you deregister a Monitoring ISE node, this node will not be listed as a syslog target in this page: Administration > System > Logging > Logging Targets.

After a secondary node is deregistered successfully, an alarm is generated on your primary Administration ISE node that confirms a successful node deregistration. If the secondary node fails to deregister from the primary Administration ISE node, the alarm is not generated.

Troubleshooting Topics

- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7

Changing the IP Address of the Monitoring Node

You must follow the procedure described in this section to change the IP address of the Monitoring node.

Prerequisite

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To change the IP Address of the Monitoring node, complete the following tasks:

Step 1 Remove the Monitoring node from the deployment. See the "Removing a Node from Deployment" section on page 9-26 for more information.

Step 2 Change the IP address of the Monitoring node.

Step 3 Register the Monitoring node as a secondary server with the primary Administration ISE node. See the "Registering and Configuring a Secondary Node" section on page 9-13 for more information.

Note If you are using the hostname while registering the Monitoring node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *ise1.cisco.com* must be DNS-resolvable from the primary Administration ISE node. Otherwise, node registration will fail. You must enter the IP addresses and FQDNs of the ISE nodes that are part of your distributed deployment in the DNS server.

The primary Administration node replicates the change in the Monitoring node's IP address to the other ISE nodes in your deployment.

Replacing the Cisco ISE Appliance Hardware

You should choose to replace the Cisco ISE appliance hardware only if there is an issue with the hardware. For any software issues, you can re-image the appliance and reinstall the Cisco ISE software.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To replace a Cisco ISE appliance hardware in your distributed deployment, complete the following tasks:

Step 1 Remove the node from the deployment. See the "Removing a Node from Deployment" section on page 9-26 for more information.

Step 2 Register the new node as a secondary server with the primary Administration ISE node. See the "Registering and Configuring a Secondary Node" section on page 9-13 for more information.

Step 3 Configure the same personas and services that were running on the node that was removed. See the "Changing Node Personas and Services" section on page 9-23 for more information.



CHAPTER 10

Setting Up Inline Posture

This chapter describes how to set up and configure Inline Posture nodes in standalone mode, or as a high availability pair, and covers the following topics:

- Inline Posture Known Limitations, page 10-1
- Understanding the Role of Inline Posture, page 10-1
- Planning an Inline Posture Deployment, page 10-4
- Deploying an Inline Posture Node, page 10-12
- Configuring Inline Posture for High Availability, page 10-24
- Adding Inline Posture as a RADIUS Client, page 10-29
- Monitoring an Inline Posture Node, page 10-30
- Removing an Inline Posture Node from Deployment, page 10-31
- Remote Access VPN Use Case, page 10-31

Inline Posture Known Limitations

This section describes known limitations for Inline Posture in Cisco ISE:

- Inline Posture is not supported in a virtual environment, such as VMware.
- Backup and restore is not available for Inline Posture nodes in Cisco ISE, Release 1.1.
- The Simple Network Management Protocol (SNMP) Agent is not supported by Inline Posture.
- The Cisco Discovery Protocol (CDP) is not supported by Inline Posture.

For more information on these and other known issues, see the "Known Issues" section of the *Release Notes for the Cisco Identity Services Engine, Release 1.1*.

Understanding the Role of Inline Posture

An Inline Posture node is a gatekeeper that enforces access policies and handles change of authorization (CoA) requests. An Inline Posture node is positioned behind the network access devices on your network that are unable to accommodate CoA, such as wireless LAN controllers (WLC) and virtual private network (VPN) devices.

After the initial authentication of a client (using EAP/802.1x and RADIUS), the client must still go through posture assessment. The posture assessment process determines whether the client should be restricted, denied, or allowed full access to the network. When a client accesses the network through a WLC or VPN device, Inline Posture is responsible for the policy enforcement and CoA that these devices are unable to accommodate.

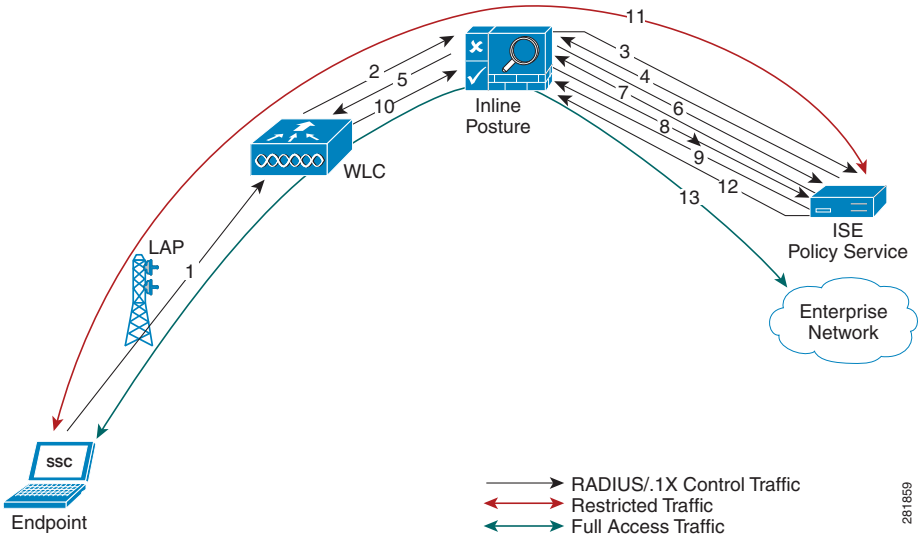
Inline Posture Policy Enforcement

Inline Posture uses RADIUS proxy and URL redirect capabilities in the control plane to manage data plane traffic for endpoints. As a RADIUS proxy, Inline Posture is able to tap into RADIUS sessions between network access devices (NADs) and RADIUS servers. NADs can open full gate to client traffic. However, Inline Posture opens only enough to allow limited traffic from clients. The restricted bandwidth allows clients the ability to have an agent provisioned, have posture assessed, and have remediation done. This restriction is accomplished by downloading and installing DACLs that are tailored for specific client flow.

Upon full compliance, a CoA is sent to the Inline Posture node by the Policy Service ISE node, and full gate is opened by the Inline Posture node for the compliant client endpoint. The RADIUS proxy downloads the full-access DACL, installs it, and associates the client IP address to it. The installed DACL can be common for a number of user groups, so that duplicate downloads are not necessary as long as the DACL content does not change at the Cisco ISE servers.

Figure 10-1 illustrates the Inline Posture policy enforcement process. This example shows the flow for WLC enforcement for traffic to the Policy Service ISE node. However, the access steps are similar for an inline deployment with VPN gateways.

Figure 10-1 Inline Posture Policy Enforcement Flow



The Inline Posture policy enforcement flow illustrated in Figure 10-1 follows these steps:

1. The endpoint initiates a .1X connection to the wireless network.
2. The WLC, which is a NAD, sends a RADIUS Access-Request message to the RADIUS server (usually the Policy Service ISE node).
3. Inline Posture node, acting as a RADIUS proxy, relays the Access-Request message to the RADIUS server.

4. After authenticating the user, the RADIUS server sends a RADIUS Access-Accept message back to the Inline Posture node.

   There can be a number of RADIUS transactions between the Endpoint, WLC, Inline Posture node, and the Cisco ISE RADIUS server before the Access-Accept message is sent. The process described in this example has been simplified for the sake of brevity.

5. The Inline Posture node passes the Access-Accept message to the WLC, which in turn authorizes the endpoint access, in accordance with the profile that accompanied the message.

6. The proxied Access-Accept message triggers Inline Posture to send an Authorization-Only request to the Policy Service ISE node, to retrieve the profile for the session.

7. The Policy Service ISE node returns an Access-Accept message, along with the necessary Inline Posture profile.

8. If the access control list (ACL) that is defined in the profile is not already available on the Inline Posture node, Inline Posture downloads it from the Policy Service ISE node using a RADIUS request (to the Cisco ISE RADIUS server).

9. The Cisco ISE RADIUS server sends the complete ACL in response. It is then installed in the Inline Posture data plane so that endpoint traffic passes through it.

   There may be a number of transactions before the complete ACL is downloaded, especially if the ACL is too large for one transaction.

10. As the endpoint traffic arrives at the WLC, the WLC sends out a RADIUS Accounting-Start message for the session to the Inline Posture node.

    The actual data traffic from the endpoint may arrive at the Inline Posture untrusted side before the Accounting-Start message is received by the Inline Posture node. Upon receiving the RADIUS Accounting-Start message, the Inline Posture node learns the IP address of the endpoint involved in the session and associates the endpoint with the ACL (downloaded and installed earlier in the session). The initial profile for this client endpoint could be restrictive, to posture the client before being given full access.

11. Assuming the restrictive ACL allows only access to Cisco ISE servers, the endpoint is only allowed actions such as agent downloading and posture assessment over the data plane.

12. If the client endpoint is posture compliant (as part of the restricted communication with Cisco ISE services earlier), the Policy Service ISE node initiates a RADIUS Change of Authorization (CoA) with the new profile. Hence, a new ACL is applied at the Inline Posture node for the session. The new ACL is installed immediately and applied to the endpoint traffic.

13. The endpoint is then capable of full access to the enterprise network, as a result of the new profile that was applied to Inline Posture.

    A RADIUS stop message for a given session that is issued from the WLC, resets the corresponding endpoint access at the Inline Posture node.

In a deployment, such as outlined in the example, when more endpoints connect to the wireless network they are likely to fall into one of the identity groups that already have authenticated and authorized users connected to the network.

For instance, there may be an employee, executive, and guest that have been granted access through the outlined steps. This situation means that the respective restrictive or full-access profiles for those ID groups have already been installed on the Inline Posture node. The subsequent endpoint authentication and authorization uses the existing installed profiles on the Inline Posture node, unless the original profiles have been modified at the Cisco ISE policy configuration. In the latter case, the modified profile with ACL is downloaded and installed on the Inline Posture node, replacing the previous version.

Trusted and Untrusted Interfaces

The following terminology plays a significant role in an Inline Posture deployment. For this reason, it is important that you understand the definitions as they relate to Inline Posture:

- Trusted—The interface that talks to the Policy Service ISE node and other trusted devices *inside* the Cisco ISE network. The trusted interface is always designated to Eth0.
- Untrusted—The interface that talks to the WLC, VPN, and other devices *outside* the Cisco ISE network. The untrusted interface is always designated to Eth1.

Inline Posture Dedicated Nodes

Unlike other persona services, Inline Posture is unable to share a node with other services. This inability to share a node means that Inline Posture must be a dedicated node that is registered to the primary Administration ISE node on your network.

Cisco ISE allows you to have up to two Inline Posture nodes configured as an active-standby pair for high availability.

For information on Cisco ISE distributed deployments, see Chapter 9, "Setting Up Cisco ISE in a Distributed Environment."

Planning an Inline Posture Deployment

Before you begin configuring Inline Posture for your network, you should understand the Inline Posture operating modes, deployment options, as well as the basics of filters and managed subnets as they apply to Inline Posture.

This section provides information on the following topics:

- About Inline Posture Configuration, page 10-4
- Choosing an Inline Posture Operating Mode, page 10-5
- Best Practices for Inline Posture, page 10-7
- Configuring Managed Subnets and Static Routes, page 10-8
- Standalone Mode or High Availability, page 10-8
- Configuring Inline Posture for High Availability, page 10-24
- Inline Posture Guidelines for Distributed Deployment, page 10-11

Note For information on how to install a Cisco ISE node, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

About Inline Posture Configuration

Inline Posture is a dedicated node registered to the Administration ISE node. You configure Inline Posture from the administration console, and that configuration is then pushed to the Inline Posture node. A copy of the configuration is stored locally in the administration database. Registration results in the Inline Posture node being rebooted.

If you have an Inline Posture high availability (HA) pair, the configuration automatically pushes to both Inline Posture nodes. If the secondary node is down during a configuration change, you can click a database sync button on the primary node that automatically applies the latest configuration to the secondary node when it comes up. A local database maintains the configurations.

Note Registering an Inline Posture node results in system restart. Changes to infrastructure configurations, such as eth1 IP address, Inline Posture mode, and high availability changes also require a system restart.

After you register an Inline Posture node to the Administration ISE node, you are not allowed to change the eth0 (Trusted) IP address through the Admin user interface. The reason for this is that, if you change the eth0 IP address of a registered Inline Posture node, it no longer can communicate with the Administration ISE node. Any attempted communication between the Inline Posture node and Administration ISE node then fails, leading to a potential exception.

Warning **It is highly recommended that you not change the IP address of an Inline Posture node from the CLI after it has been registered on the Cisco ISE network.**

Choosing an Inline Posture Operating Mode

The Inline Posture operating mode you choose depends largely on the architecture of your existing network. However, this choice sets a precedent for many of the other configuration options you have to specify for the deployment. For this reason, it is important that you understand the functions of each of the following Inline Posture operating modes:

- Routed mode—This mode acts as a Layer 3 “hop” in the wire, selectively forwarding packets to specified addresses. This mode provides the ability to segregate network traffic, allowing you to specify users who have access to selected destination addresses.
- Bridged mode—This mode acts as a Layer 2 “bump” in the wire, forwarding packets without regard to the destination address.
- Maintenance mode—This mode takes the node offline so that you can perform administrative procedures. This mode is also the default mode of a node when it first comes onto the network, before you perform other configurations.

Bridged mode and routed mode are discussed in greater detail throughout the rest of this section.

Inline Posture Routed Mode

In routed mode, the Inline Posture node operates as a Layer 3 router, and becomes the default gateway for the untrusted network with its managed clients. All traffic between the untrusted and trusted networks passes through the Inline Posture node, which applies the IP filtering rules, access policies, and other traffic-handling mechanisms that you decide to configure.

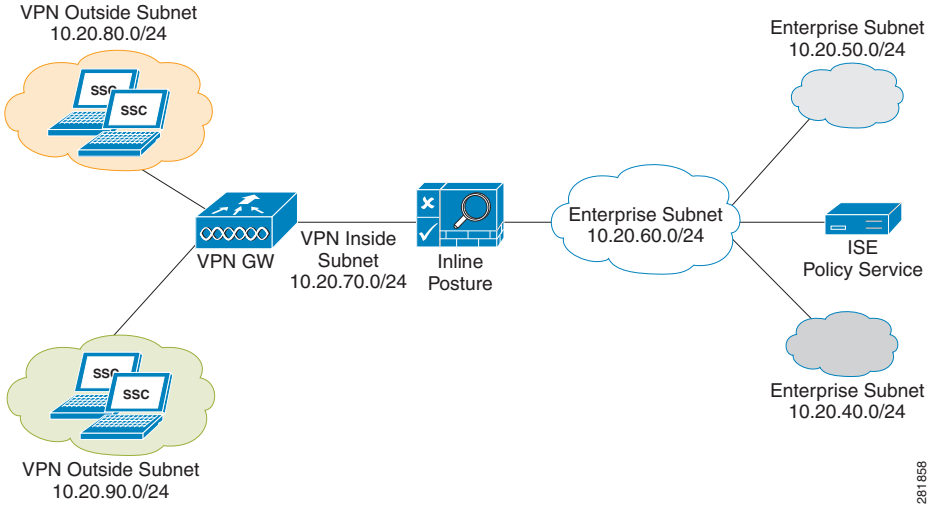
When you configure Inline Posture in routed mode, you need to specify the IP addresses of its two interfaces:

- Trusted (Eth0)
- Untrusted (Eth1)

The trusted and untrusted addresses should be on different subnets. Inline Posture can manage one or more subnets, with the untrusted interface acting as a gateway for the managed subnets.

Figure 10-2 illustrates an Inline Posture routed mode configuration. In the following routed mode example, Inline Posture is a hop for the client traffic from the VPN gateway (GW) en route to the Policy Service ISE node. Inline Posture requires that static routes be configured for subnets 10.20.80.0/24 and 10.20.90.0/24 toward the VPN gateway, just like any other router. The enterprise router on the trusted side of the network also requires that the static routes are configured for the same subnets toward the Inline Posture node.

Figure 10-2 Inline Posture Routed Mode Configuration

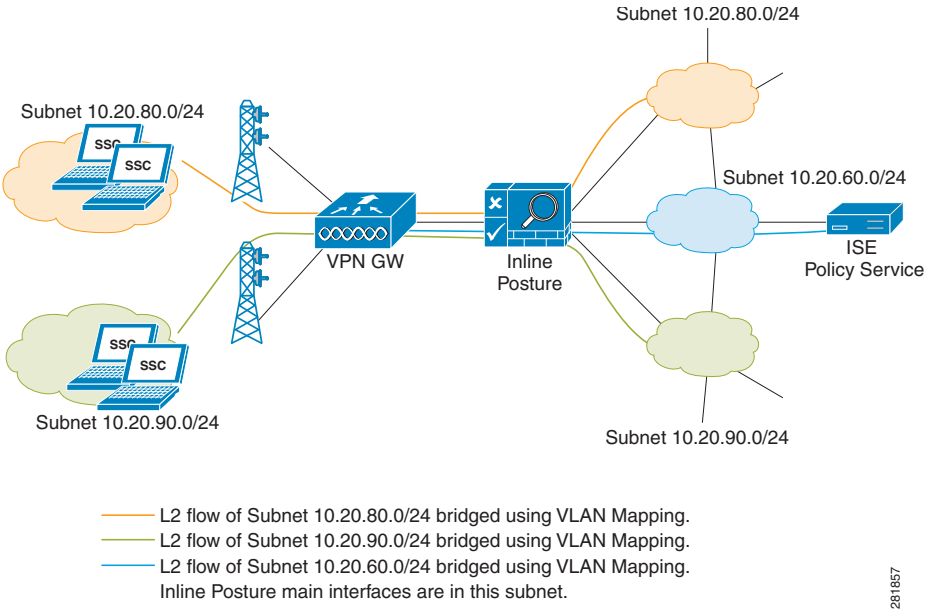


Inline Posture Bridged Mode

In bridged mode, the Inline Posture node operates as a standard Ethernet bridge. This configuration is typically used when the untrusted network already has a gateway, and you do not want to change the existing configuration.

Figure 10-3 shows the Inline Posture node acting as a bridge for the Layer 2 client traffic from the WLC into the Cisco ISE network, managed by the Policy Service ISE node. In this configuration, Inline Posture requires subnet entries for the 10.20.80.0/24 and 10.20.90.0/24 subnets to be able to respond to and send Address Resolution protocol (ARP) broadcasts to the correct VLANs.

Figure 10-3 Inline Posture Bridged Mode Configuration



When the Inline Posture node is in bridged mode, the following conditions apply:

- Inline Posture eth0 and eth1 can have the same IP address.
- All end devices in the bridged subnet must be on the untrusted network.

Best Practices for Inline Posture

This section introduces best practice concepts for deploying Inline Posture in a distributed environment.

Using Filters to Define Access Privileges

Consider the following when configuring filters:

- As typically implemented, Inline Posture enforces authentication requirements on endpoints that attempt to access the network. Device and subnet filters are used to validate or deny WLC and VPN devices.
- For certain devices, you may want to bypass authentication, posture assessment, role assignment, or any combination thereof. Common examples of bypassed device types include printers, IP phones, servers, nonclient machines, and network devices.

  Inline Posture matches the MAC address of a device, or a MAC and IP address combination, or a subnet address to determine whether the bypass function is enabled for a device. You can choose to bypass policy enforcement, or to forcibly block access.

Warning **Do not configure the MAC address in a MAC Filter for a directly connected adaptive security appliance (ASA) VPN device without also entering the IP address. Without the addition of the (optional) IP address, VPN clients are allowed to bypass policy enforcement. This bypass happens because the VPN is a Layer 3 hop for clients, and the device uses its own MAC address (as the source address) to send packets along the network toward the Inline Posture node.**

Configuring Managed Subnets and Static Routes

Consider the following when configuring managed subnets for Inline Posture:

- Configure managed subnets for endpoints in Layer 2 proximity of the Inline Posture node. For example, a WLC that delivers packets directly to the untrusted interface of the Inline Posture node.
- When configuring subnets for endpoints in Layer 2 proximity to an Inline Posture node, you must also configure a managed subnet for Inline Posture. This configuration ensures that the Inline Posture node can send Address Resolution protocol (ARP) queries with the appropriate VLAN IDs for the client devices on the untrusted interface. Configure the untrusted (authentication) VLAN in the VLAN ID field for the managed subnet.
- When configuring a managed subnet for Inline Posture, configure an IP address and not a subnet address. This configuration ensures that the ARP requests that Inline Posture sends have a valid source IP address.
- Subnets on the trusted side of the Inline Posture node should be dissimilar to subnets on the untrusted side.
- An Administration ISE node and Inline Posture node should not be on the same subnet, unless you have defined a static route.

Consider the following when configuring static routes for Inline Posture:

- Configure static routes for endpoints that are more than one hop away (Layer 3) from the Inline Posture node.
- Static routes should be configured for all downstream host networks that are typical of VPN address pools.

High Availability

Consider the following when configuring Inline Posture for high availability:

- Assign a service IP (also known as a virtual IP) for each side of the Inline Posture interfaces, trusted (eth0) and untrusted (eth1).
- Specify link-detect IP addresses for the trusted (eth0) and untrusted (eth1) interfaces. Link-detect appears as an optional setting in the user interface, but is highly recommended.

Standalone Mode or High Availability

One of the most important decisions you will make with regard to your Inline Posture deployment, is whether to deploy a single, standalone node, or an active-standby pair to ensure high availability.

A standalone Inline Posture node is simply a single Inline Posture node that provides services and works independently of all other nodes. You might choose to deploy a single standalone Inline Posture node for a network that serves a small facility, where redundancy is not a major concern.

An Inline Posture high availability deployment consists of two Inline Posture nodes that are configured as an active-standby pair. The active node acts as the RADIUS proxy, forwarding all the network packets until such time that it fails, then the standby node takes over. As long as the active node is functioning properly, the standby node remains passive. However, should the active node falter, the standby node takes over to perform Inline Posture functionality.

Figure 10-2 illustrates a simple Inline Posture standalone configuration, with client access through WLC and VPN devices. Figure 10-4 illustrates a routed mode high availability Inline Posture configuration.

Inline Posture High Availability

Inline Posture stateless high availability deployment has an active-standby pair node configuration, where the standby node acts as a backup unit and does not forward any packets between the interfaces. Stateless means that sessions that have been authenticated and authorized by an active node are automatically authorized again after a failover occurs.

The standby node monitors the active node using the heartbeat protocol (using eth2 and eth3 interfaces), which requires that messages are sent at regular intervals between the two nodes. If the heartbeat stops or does not receive a response back in the allotted time, failover occurs and recovery action takes place.

Note The heartbeat protocol that is active in an Inline Posture high availability configuration requires a direct Ethernet cable connection between the eth2 interfaces of both nodes of a high availability pair. Likewise, there must be a direct Ethernet cable connection between the eth3 interfaces of the two nodes. Figure 10-4 illustrates this principle.

In addition to the heartbeat monitor, an optional (but highly recommended) link-detect mechanism is available. With the use of link-detect, Inline Posture trusted and untrusted interfaces ping an external IP address from their respective interfaces. If both nodes are unable to ping the external IP address, then failover does not occur. However, if either of the nodes becomes unreachable, the node that is functional automatically becomes the active node.

Upon failover, the following occurs:

1. The standby Inline Posture node takes over the service IP address (SIP).
2. Once the failover happens, the administrator corrects the failed node and reverts to an earlier configuration, as needed.

   When a failed node is brought back online, a manual sync operation to update the node with the most current information is required. For information on how to perform an Inline Posture node sync operation, see Syncing an Inline Posture Node, page 10-28.
3. Active sessions are automatically reauthenticated and authorized.

Key Points for High Availability

- The terms primary and secondary have different meanings with regard to Inline Posture high availability than they do in relation to Cisco ISE nodes. For Inline Posture high availability, primary and secondary denote the device that takes over the active state and the device that takes the standby role in case there is a contention, such as when both nodes boot up at the same time.
- The terms active and standby are representative of high availability states. A primary or secondary Inline Posture node can be in either an active or standby state.
- If the heartbeats simultaneously go down for both Inline Posture high availability nodes, a partitioning state may ensue. A partitioning state is a condition where both nodes assume that the other has totally failed, and both try to take over active control.
- The secondary Inline Posture node is read-only, and cannot be used for configuration of any kind, even high availability.
- The eth2 and eth3 interfaces of both nodes in an Inline Posture high availability pair (primary and secondary) communicate with heartbeat protocol exchanges to determine the health of the nodes. For the heartbeat to work, you must connect the eth2 interface of the primary Inline Posture node to

the eth2 interface of the secondary node using an Ethernet cable. Likewise, the eth3 interface of the primary Inline Posture node must be connected to the eth3 interface of the secondary node with an Ethernet cable. Figure 10-4 illustrates this principle.

Note A heartbeat is a message that is sent from one node in an Inline Posture high availability pair to the other member of the pair at regular intervals. If a heartbeat is not received for an extended period of time, usually several heartbeat intervals, the node that should have sent the heartbeat is assumed to have failed. If it is the primary Inline Posture node that fails, the secondary node takes over so there is no disruption in service.

- When a node in a high availability pair is down and configuration changes are made to the single active node, there is no mechanism that automatically populates the failed node with the new configuration when it comes back up. The Sync-up Peer Node button that appears in the Inline Posture high availability user interface on the active node, allows you to manually sync the standby node with the latest Inline Posture database from the active node.
- For high availability, you register two Inline Posture nodes, then choose one node to be primary and enable high availability. For more information, see Configuring Inline Posture for High Availability, page 10-24.

Configuring Inline Posture High Availability in Routed Mode

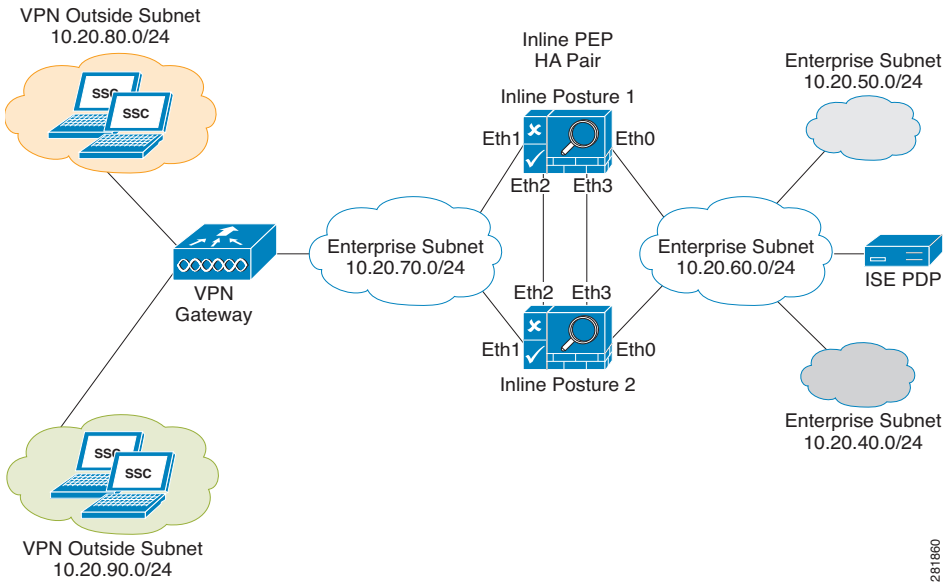
An Inline Posture high availability (HA) pair consists of two physical Inline Posture nodes configured as a cluster that have heartbeat links on the eth2 and eth3 interfaces, connected by dedicated cables. Each Inline Posture node has its own physical IP addresses on the trusted and untrusted Ethernet interfaces, but a separate service IP address must be assigned to the cluster as a whole.

Note The service IP address, also called a virtual IP address, is required for RADIUS authentication purposes. You assign the SIP to both the trusted and untrusted interfaces for both nodes of the active-standby pair, thus making the SIP the address of the cluster, representing it as a single entity to the rest of the network.

For example, the untrusted IP address for IPEP1 can be10.20.70.101, and the untrusted IP address for IPEP2 can be 10.20.70.102. However, the service IP address for both nodes on the untrusted side of the network would be10.20.70.100. The active Inline Posture node in the pair, at any point of time, assumes the service IP address on the untrusted side of the network. The same holds true for the trusted side of the network.

Figure 10-4 shows an example of an Inline Posture high availability routed mode configuration. Note the dedicated cables that connect the eth2 and eth3 interfaces between the two nodes to facilitate the heartbeat communication that checks for failure in the active node.

Figure 10-4 Inline Posture Routed Mode High Availability Example



Configuring Inline Posture High Availability in Bridged Mode

The following guidelines apply to an Inline Posture bridged mode high availability configuration:

- Inline Posture eth0 and eth1 should have IP addresses in the same subnet. Having the same IP address is recommended.
- Any devices on the trusted side of the network that have IP addresses in the subnets that are managed by an Inline Posture in bridged mode, must have an explicit static route configured at the Inline Posture node. This configuration is necessary because by default, Inline Posture assumes that the subnet that it manages (as configured on the Managed Subnets user interface page) lies entirely on the untrusted side of the network.

Inline Posture Guidelines for Distributed Deployment

Before you begin configuring an Inline Posture node in a distributed deployment, be sure you understand the following statements:

1. Inline Posture is unable to run concurrently with Administration, Policy Service, or Monitoring personas, and therefore is a dedicated node.
2. An Inline Posture node must be registered as a secondary node to the primary Administration ISE node on your network.
3. You can deploy a standalone Inline Posture node, or an active-standby pair.
4. You can have up to two Inline Posture nodes configured on your network at any one time. For an Inline Posture high availability active-standby pair, two nodes are configured. One node is designated as the primary node and the other as the secondary node. The primary node has the preference for being the active node when both nodes come up at the same time.
5. For an Inline Posture active-standby pair configuration, all configuration related to functionality must be done from the active node of the pair. The user interface for the standby node, on the Cisco ISE user interface, shows only basic configuration tables.

6. You can sync an Inline Posture active node configuration to its peer standby node from the Failover tab of the active node. For more information, see Syncing an Inline Posture Node, page 10-28.

Note If you have a WLC authentication, authorization, and accounting (AAA) server (Cisco 2100 or 4400 Series Wireless LAN Controllers) on your network, the RADIUS authentication server timeout value needs to be set to a minimum of 30 seconds. This minimum value ensures that RADIUS failover will work in conjunction with Inline Posture. See the WLC server hardware documentation for more information.

Deploying an Inline Posture Node

The initial process for configuring an Inline Posture node is the same, whether it is intended to be a standalone node or part of an active-standby pair. This section covers the series of tasks you must complete to configure an Inline Posture node on your Cisco ISE network.

To configure an Inline Posture node, complete the following tasks:

1. Configuring Inline Posture in Bridged or Routed Mode, page 10-12
2. Creating Inline Posture Downloadable Access Control Lists, page 10-19
3. Creating Inline Posture Node Profiles, page 10-21
4. Creating an Inline Posture Authorization Policy, page 10-23

Configuring Inline Posture in Bridged or Routed Mode

To introduce an Inline Posture node in your Cisco ISE network you must first register the Inline Posture node with the primary Policy Service ISE node, configure the Inline Posture settings, and then create authorization profiles and policies that establish the Inline Posture gatekeeping policies.

The Inline Posture node is a RADIUS proxy that interfaces with NADs as their RADIUS server, making the NADs (VPN gateway, WLC) RADIUS clients. As a proxy, Inline Posture interfaces with the Policy Service ISE node as a client, making the Policy Service ISE node its RADIUS server.

Note Upon completing the following procedure, a NAD entry is automatically created for the Inline Posture node. For a standalone node, the IP address for that node is used. For an HA pair, the service IP address for the active node is used.

Guidelines for Configuring Certificates for Inline Posture

Secure communication between Administration and Inline Posture nodes requires mutual authentication. This means that not only must the Inline Posture node prove its identity to the Administration node, but the reverse is also true. Observe the following guidelines when configuring certificates on these nodes:

- The presence of certain combinations of attributes in the local certificates of the Administration and Inline Posture nodes can prevent mutual authentication from working.

  The attributes are:

  - Extended Key Usage (EKU)—Server Authentication
  - Extended Key Usage (EKU)—Client Authentication
  - Netscape Cert Type—SSL Server Authentication
  - Netscape Cert Type—SSL Client Authentication

The following combinations are recommended for the Administration certificate:

- Both EKU attributes should be disabled, if both EKU attributes are disabled in the Inline Posture certificate, or both EKU attributes should be enabled, if the server attribute is enabled in the Inline Posture certificate.
- Both Netscape Cert Type attributes should be disabled, or both should be enabled.

The following combinations are recommended for the Inline Posture certificate:

- Both EKU attributes should be disabled, or both should be enabled, or the server attribute alone should be enabled.
- Both Netscape Cert Type attributes should be disabled, or both should be enabled, or the server attribute alone should be enabled.

- Where self-signed local certificates are used on the Administration and Inline Posture nodes, you must install the self-signed certificate of the Administration node in the trust list of the Inline Posture node. In addition, if you have both primary and secondary Administration nodes in your deployment, you must install the self-signed certificate of both Administration nodes in the trust list of the Inline Posture node.
- Where CA-signed local certificates are used on the Administration and Inline Posture nodes, mutual authentication should work correctly. In this case, the certificate of the signing CA is installed on the Administration node prior to registration, and this certificate is replicated to the Inline Posture node.
- If CA-issued keys are used for securing communication between the Administration and Inline Posture nodes, before you register the Inline Posture node, you must add the public key (CA certificate) from the Administration node to the CA certificate list of the Inline Posture node.

Prerequisites

- You should have administrative permissions on the primary Administration ISE node.
- Follow and apply the Guidelines for Configuring Certificates for Inline Posture, page 10-12.
- Register the Inline Posture node with the primary Administration ISE node, as described in Registering and Configuring a Secondary Node, page 9-13. All nodes must be registered with the primary Administration ISE node to function as a member of the Cisco ISE distributed system. Be sure to check the Inline Posture check box. The Administration, Monitoring, and Policy Service check boxes are automatically unchecked.

Note Registering an Inline Posture node results in a system restart. Likewise, changes to infrastructure configurations, such as the eth1 IP address, Inline Posture mode, and high availability changes also require a system restart. The restart is automatic. However to manually restart the node from the CLI, use the **application stop ise** and **application start ise** commands.

- RADIUS configuration is mandatory. At least one client and one server configuration is necessary. You need the corresponding shared secret information for both sides to complete this procedure.
- Have all necessary configuration information for your installation on hand. For example, you might need the trusted and untrusted IP addresses, service IP address, the IP addresses for other Cisco ISE nodes, shared secret for RADIUS configuration, management VLAN ID, WLC, or VPN IP address, and so on. Check with your system architect for a complete list of the information you will need.

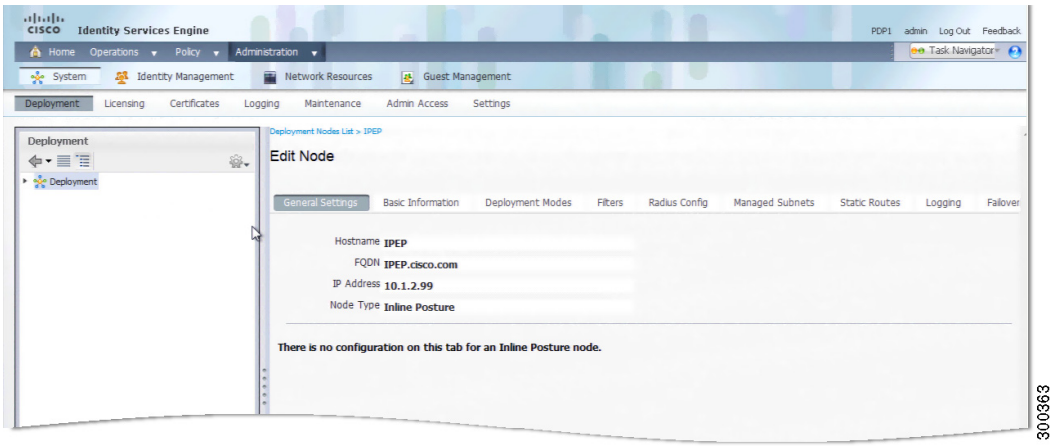
Warning **Do not configure the MAC address in a MAC Filter for a directly connected ASA VPN device without also entering the IP address. Without the addition of the (optional) IP address, VPN clients are allowed to bypass policy enforcement. This access happens because the VPN is a Layer 3 hop for clients, and the device uses its own MAC address (as the source address) to send packets along the network toward the Inline Posture node.**

To configure Inline Posture in bridged or routed mode, complete the following steps:

Step 1 From the primary Administration ISE node choose **Administration > System > Deployment**, click the **Deployment** link in the left-hand panel, and then in the Deployment Nodes list, check the **Inline Posture node** check box and click the **Edit** icon.

Step 2 On the General Settings page, check the **Inline PEP** check box. The Administration, Monitoring, and Policy Service check boxes are automatically unchecked.

Figure 10-5 Edit Inline Posture Node



The tabs change to General Settings, Basic Information, Deployment Modes, Filters, Radius Config, Managed Subnets, Static Routes, Logging, and Failover.

Note A newly registered Inline Posture node comes up with a default IP address of 192.168.1.100, a subnet mask of 255.255.255.0, and a default gateway of 192.168.1.1. Change these values to fit your deployment in the following step.

Step 3 Click the **Basic Information** tab and enter the appropriate information for the following options:

- Time Sync Server: Primary, Secondary, Tertiary
- DNS Server: Primary, Secondary, Tertiary
- Trusted Interface (to protected network): Set Management VLAN ID (all the other information is automatically populated for these options)
- Untrusted Interface (to management network): IP Address, Subnet Mask, Default Gateway, Set Management VLAN ID

Figure 10-6 is an example of a bridged mode configuration. Figure 10-7 is an example of a routed mode configuration.

Figure 10-6 Basic Information (Bridged)

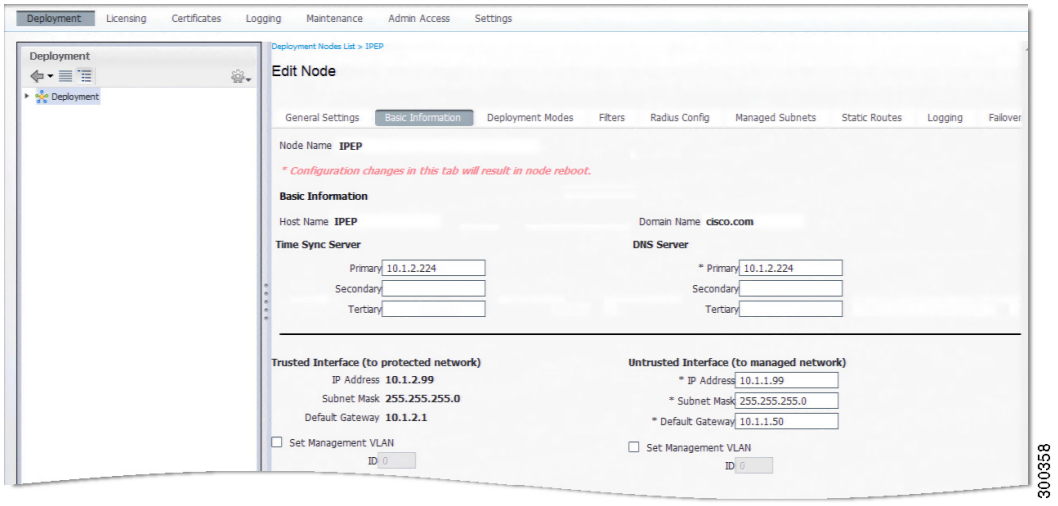
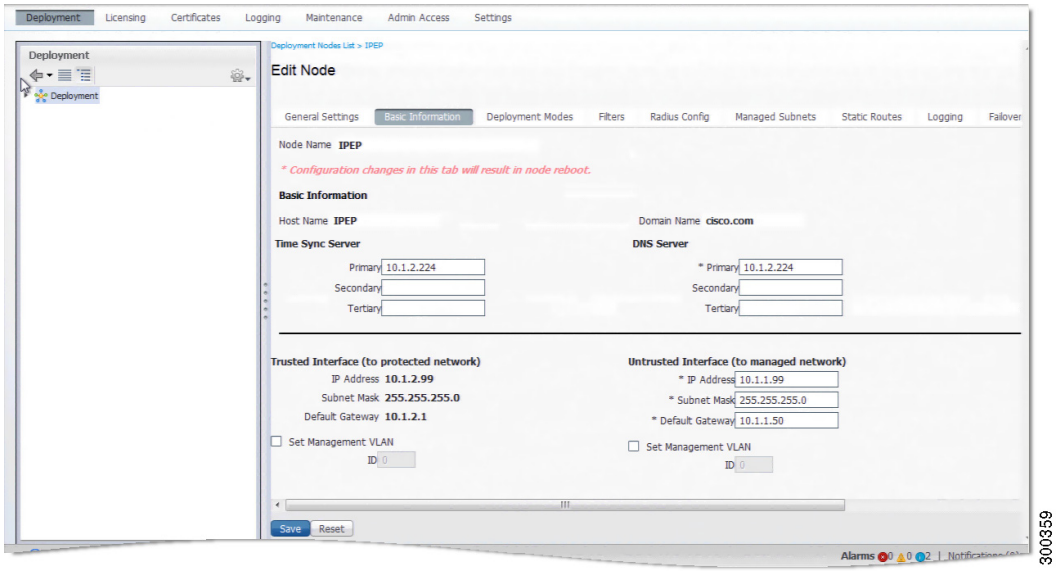


Figure 10-7 Basic Information (Routed)



Step 4 Choose the **Deployment Modes** tab. A newly registered Inline Posture node comes up in maintenance mode. For production purposes, choose one of the following:

- Routed Mode—Provides router (hop in the wire) functionality for Inline Posture. Figure 10-8 provides an example for routed mode.
- Bridged Mode—Provides VLAN mapping functionality for the subnets to be managed by Inline Posture. After checking the Bridged Mode check box, enter the Untrusted Network and Trusted Network VLAN ID information. Figure 10-9 provides an example for bridged mode.

  For VLAN mapping, you should also do the following:

  – Add a mapping for management traffic by entering the appropriate VLAN ID for the trusted and untrusted networks.

– Add a mapping for client traffic by entering the appropriate VLAN ID for the trusted and untrusted networks.

Figure 10-8 Deployment Modes (Routed)

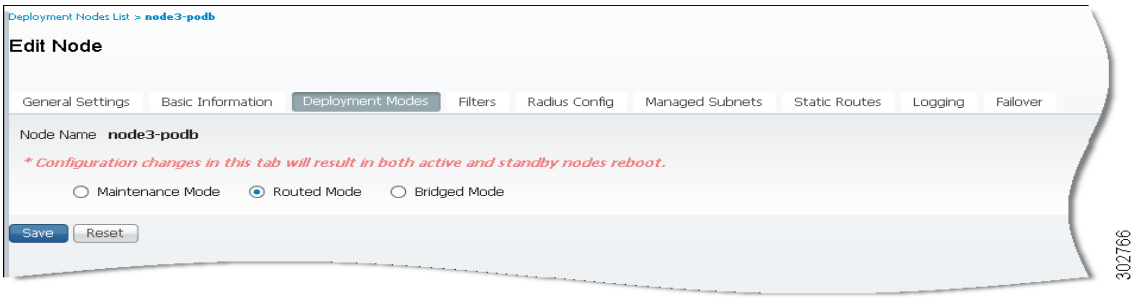


Figure 10-9 Deployment Modes (Bridged)

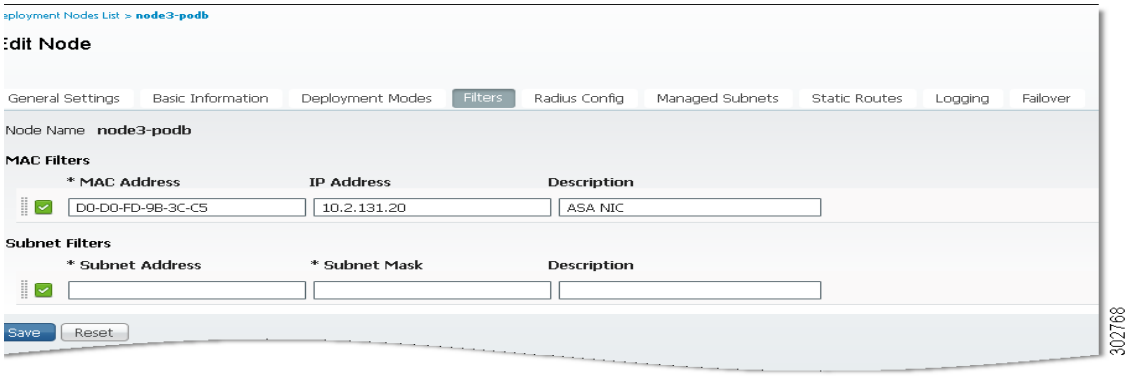
Step 5 Choose the **Filters** tab and enter the subnet address and subnet mask for the client device, or the MAC address and IP address of the device on which to filter.

You can use MAC and subnet filters to bypass Inline Posture enforcement to certain endpoints or devices on the untrusted side of the network. For example, if VPN or WLC management traffic is required to pass through Inline Posture, you would not want to subject those particular NADs to Cisco ISE policy enforcement. By providing the MAC address and IP address for these NADs on a filter, you can then access the user interface or configuration terminal by way of Inline Posture without restrictions.

- MAC filters—MAC Address and/or IP Address on which to avoid policies
- Subnet Filters—Subnet Address and Subnet Mask on which to avoid policies

Note For security reasons, it is recommended that you always include the IP address along with the MAC address in a MAC filter entry. For more information, see the Warning in Prerequisites, page 10-13.

Figure 10-10 Filters



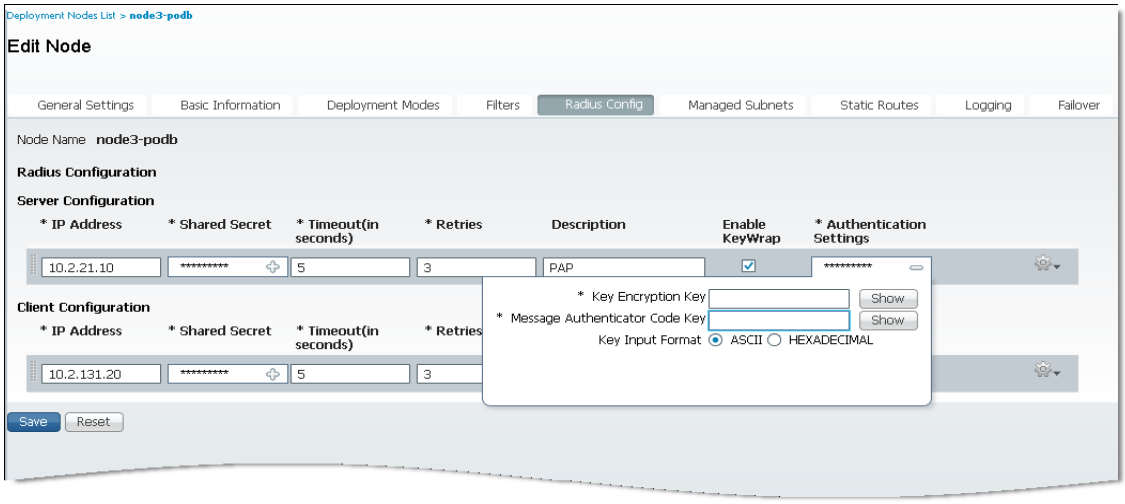
Step 6 Choose the **RADIUS Config** tab and enter the IP Address and Shared Secret for the following:

- Primary Server—Primary RADIUS server, usually the Policy Service ISE node
- Secondary Server—Optional
- Client—Device that requests access on behalf of clients, WLC or VPN

Note WLC roaming is not supported in Cisco ISE, Release 1.1.

RADIUS configuration is mandatory. At least one client and one server configuration is necessary for Inline Posture. For more information on RADIUS proxy services, see Proxy Service, page 16-21.

Figure 10-11 RADIUS Configuration



Step 7 (Optional) Check the Enable KeyWrap check box and specify the following Authentication Settings:

- Key Encryption Key
- Message Authenticator Code Key
- Key Input Format: ASCI or Hexidecimal

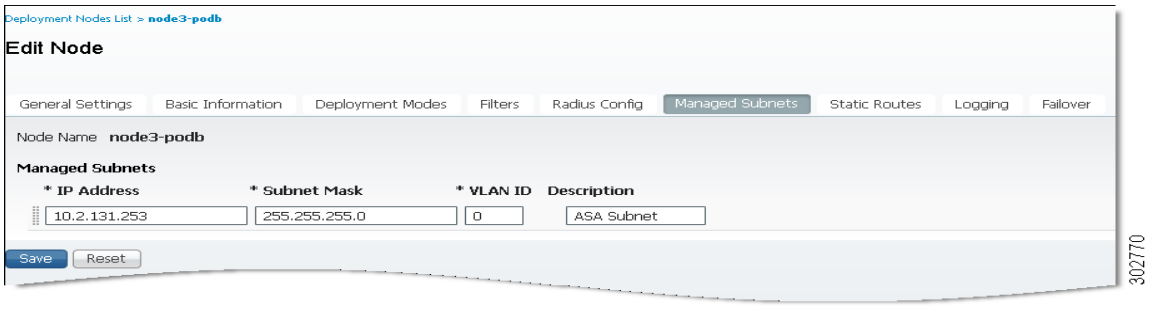
Deployments that utilize wireless LAN technology require secure transmission from a RADIUS server to a network access point. KeyWrap attributes provide stronger protection and more flexibility.

Step 8 Click the **Managed Subnets** tab, and enter the following information for each Managed Subnet:

- IP Address
- Subnet Mask
- VLAN ID
- Description

For subnets of endpoints that are in Layer 2 proximity to the Inline Posture node (such as a WLC), you must configure managed subnets. This configuration requires an unused IP address in the same subnet as the managed subnet, along with the VLAN (if any) of the subnet. You can have multiple managed subnet entries.

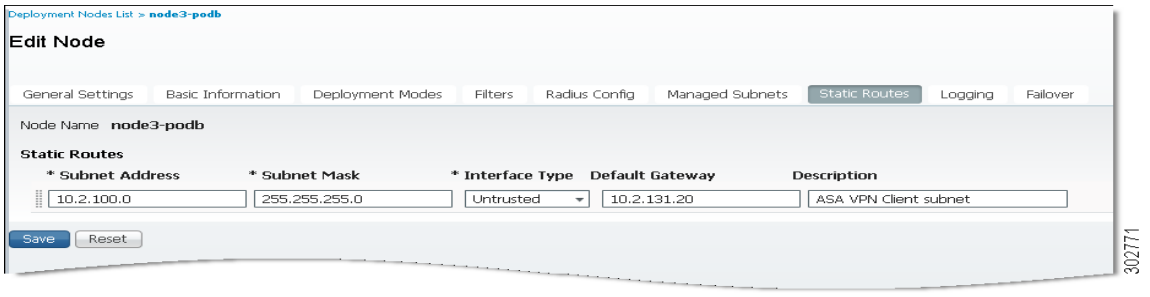
Figure 10-12 Managed Subnets



Step 9 Click the **Static Routes** tab, then enter the Subnet Address, Subnet Mask, and choose **Trusted** or **Untrusted** from the Interface Type drop-down menu. Repeat this step as needed for your configuration.

When the subnets of the endpoints under Cisco ISE control are Layer 3 away from the Inline Posture node, a static route entry is needed. For example, if a VPN gateway device (that sends managed subnet traffic to the Inline Posture untrusted interface) is two hops away, its client subnet needs to have a static route defined for Inline Posture. The network on the trusted side should know to send traffic to the Inline Posture trusted interface.

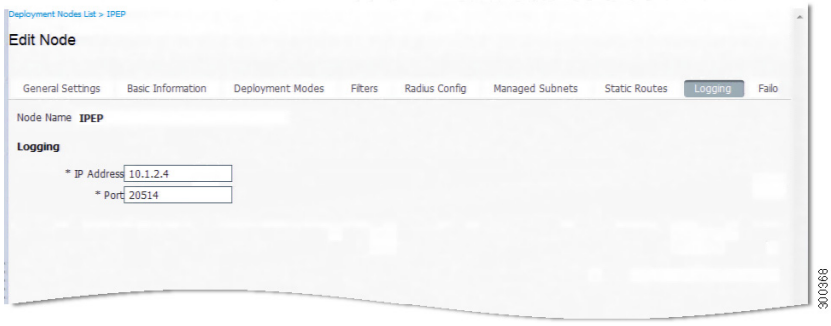
Figure 10-13 Static Routes



Step 10 Click the **Logging** tab and enter the IP Address and Port number for the logging server, which is typically the Monitoring ISE node.

An IP address and port (default 20514) for logging Inline Posture events are mandatory. This requirement ensures that the viable status of the Inline Posture node is displayed on the Cisco ISE dashboard in the System Summary dashlet, and that other log information regarding the nodes is available.

Figure 10-14 Logging



Step 11 Click **Save**. The node restarts.

Step 12 To verify the automatically generated Inline Posture NAD listing, go to **Administration > Network Resources > Default Device**.

For a standalone node, the IP address for that node is used. For an HA pair, the service IP address for the active node is used.

Next Steps

To complete the configuration setup of the Inline Posture node, complete the following tasks, creating three DACLs, authorization profiles, and authorization policy rules: unknown, compliant, and noncompliant.

1. Creating Inline Posture Downloadable Access Control Lists, page 10-19
2. Creating Inline Posture Node Profiles, page 10-21

Note It is important to associate the appropriate downloadable access control list (DACL) with the corresponding profile. For example, the unknown DACL should be associated with the unknown authorization profile.

3. Creating an Inline Posture Authorization Policy, page 10-23

Troubleshooting Topics

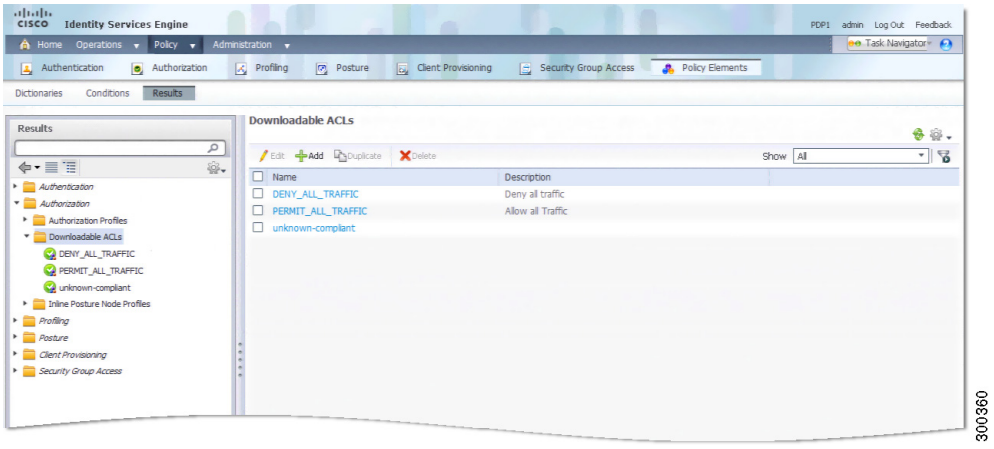
- Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working, page D-7

Creating Inline Posture Downloadable Access Control Lists

Downloadable access control lists (DACLs) are building blocks for authorization profiles, and they provide the rules for the profiles to follow. Access control lists (ACLs) prevent unwanted traffic from entering the network by filtering source and destination IP addresses, transport protocols, and other variables, using the RADIUS protocol.

After you create DACLs as named permission objects, add them to authorization profiles, which you then specify as the result of an authorization policy. For more information on DACLs, see Understanding Authorization Policies, page 17-1.

Figure 10-15 Inline Posture DACLs



Note Every administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure.

To create a DACL for Inline Posture, complete the following steps:

Step 1 Following the instructions as described in Configuring Permissions for Downloadable ACLs, page 17-33, create the following DACLs:

- ipep-unknown (Pre-Posture): Use at least one ACL to allow supplicants and the Policy Service to have access to each other for posture evaluation. This DACL can be used to block or quarantine users until they pass authentication. See Figure 10-16 for an example.
- ipep-compliant (Permit All): Use the following: permit ip any any
- ipep-noncompliant (Deny All): Use the following: deny ip any any

Figure 10-16 Inline Posture DACL Compliance Unknown

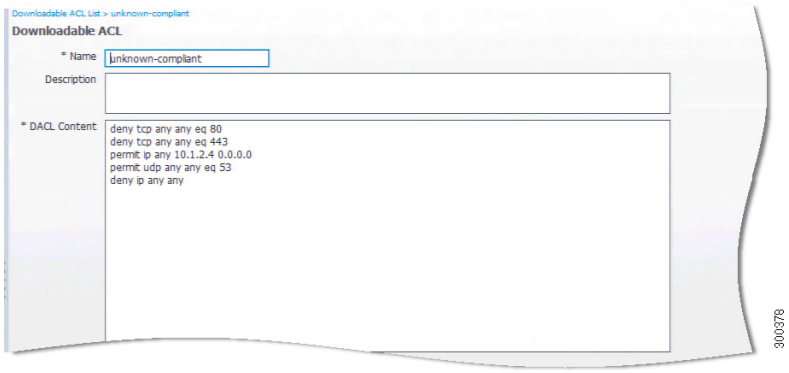
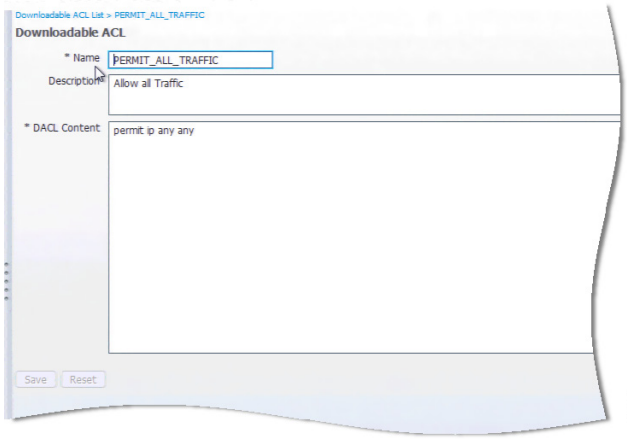


Figure 10-17 Inline Posture DACL Compliant



Step 2 Save the DACLs, and then go to Creating Inline Posture Node Profiles, page 10-21.

Troubleshooting Topics

- Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working, page D-7

Creating Inline Posture Node Profiles

This section describes how to create authorization profiles for Inline Posture. You create three Inline Posture authorization profiles, as well an authorization profile for a NAD. For more information, see Cisco ISE Authorization Policies and Profiles, page 17-5.

All Inline Posture inbound profiles are automatically set to cisco-av-pair=ipep-authz=true so that the Inline Posture node is sure to apply these rules, instead of proxying them on to the NADs. The URL redirect is essential for client provisioning, as well as agent discovery redirection.

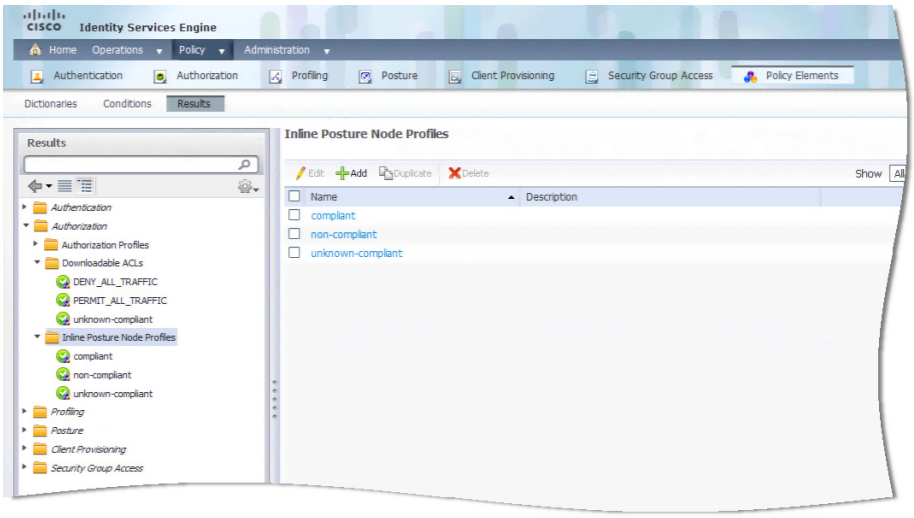
To create authorization profiles for NAD and Inline Posture, complete the following steps:

Step 1 Create a NAD authorization profile as described in Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28.

Note You can configure a RADIUS Reply Message = NAD Profile, to see *NAD Profile* in the RADIUS log messages for Inline Posture. This configuration can be helpful for troubleshooting at a later time.

Step 2 Create authorization profiles to Inline Posture that correspond to the DACLs you created in Creating Inline Posture Downloadable Access Control Lists, page 10-19.

Figure 10-18 Inline Posture Profiles



Specify the appropriate DACL for each of the following authorization profiles:

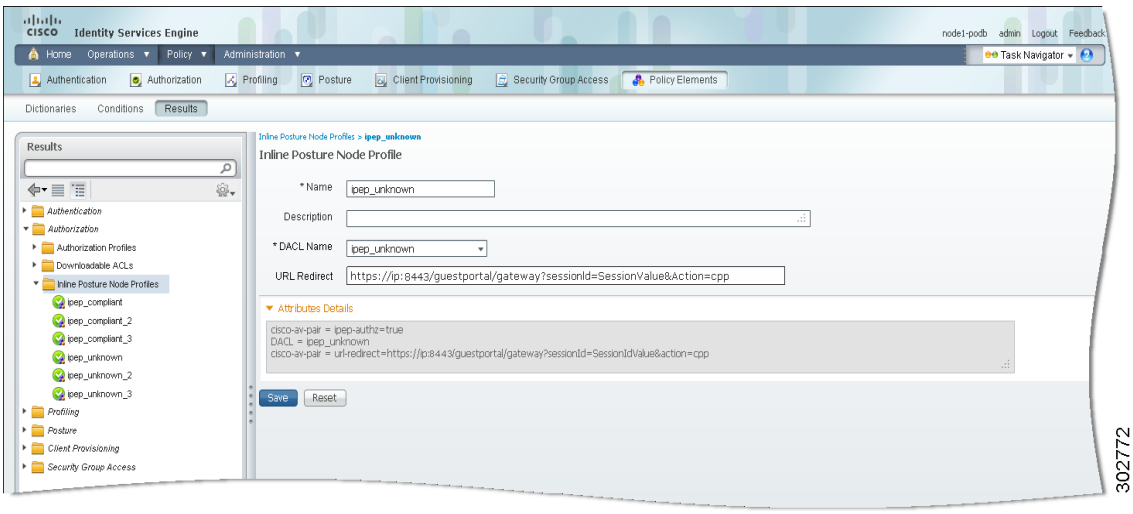
- Unknown-Compliant (Pre-Posture): This profile requires that you enter a URL redirect.

  From the Inline Posture Authorization Profiles page, select the Unknown-Compliant DACL name from the drop-down menu, enter the following URL redirect in the text field, and click **Submit**:

  url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionValue&Action=cpp

  The URL redirect appears in the Attributes Details field.

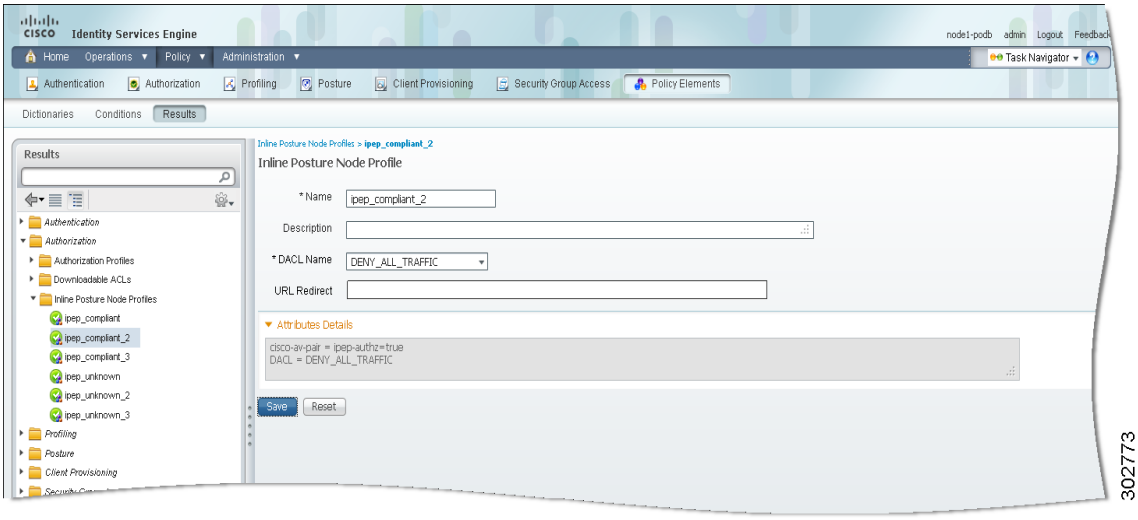
Figure 10-19 Unknown-Compliant Authorization Profile



You are redirected to a web page where you download and install an agent. The agent then scans your system. If your system passes, you are automatically granted full access. If your system does not pass, you are denied access.

- IPEP-Compliant (Permit Any)
- IPEP-Noncompliant (Deny All)

Figure 10-20 Non-Compliant Authorization Profile



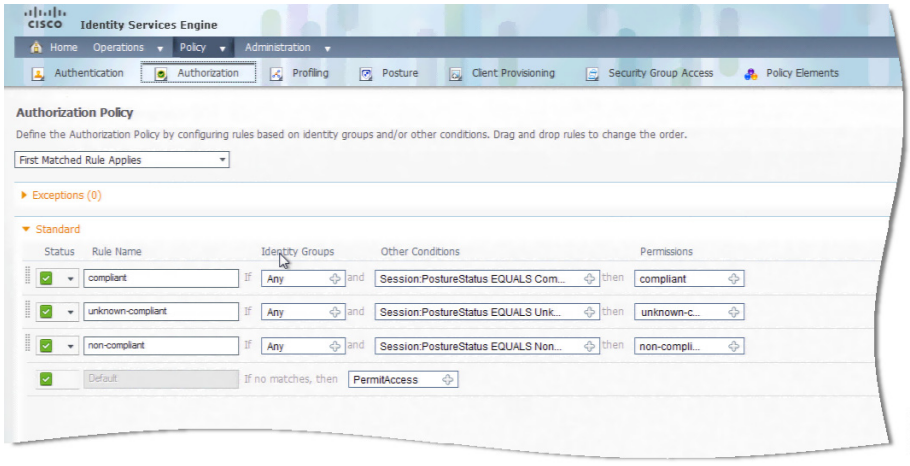
Step 3 After you have saved each of the authorization profiles, continue with Creating an Inline Posture Authorization Policy, page 10-23.

Creating an Inline Posture Authorization Policy

Authorization policies provide the means for controlling access to the network and its resources. Cisco ISE lets you define a number of different authorization policies.

The elements that define the authorization policy are referenced when you create policy rules. Your choice of conditions and attributes defines the authorization profile. Figure 10-21 shows the authorization rules that are necessary for VPN and WLC access.

Figure 10-21 Authorization Rules for VPN and WLC Access



For more information on authorization policies, see Cisco ISE Authorization Policies and Profiles, page 17-5.

To create authorization policies, complete the following steps:

Step 1 Create an authorization policy as described in Creating a New Authorization Policy, page 17-14, leaving the default rule as is. Then, continue with the following steps.

Step 2 Create the following Unknown Posture Status Rule:

- Identity Group: Any
- Condition: Session:PostureStatus EQUALS = Unknown
- Permissions: ipep-unknown-compliant + nad-authorization-profile

Step 3 Create the following Compliant Posture Rule:

- Identity Group: Any
- Condition: Session:PostureStatus EQUALS = Compliant
- Permissions: ipep-compliant + nad-authorization-profile

Step 4 Create the following Noncompliant Posture Rule:

- Identity Group: Any
- Condition: Session:PostureStatus EQUALS = Noncompliant
- Permissions: ipep-noncompliant + nad-authorization-profile

Step 5 Save the policy. The Inline Posture node configuration process is now complete.

Next Step

Complete the following task: Adding Inline Posture as a RADIUS Client, page 10-29.

Configuring Inline Posture for High Availability

This section explains how to configure two Inline Posture nodes for high availability. One node is specified as the primary unit in the pair and becomes the active node by default. The other becomes the secondary node, which is a standby unit in case of default.

A high availability node failover prompts the standby node to take over the service IP address. After this process occurs, an administrator must correct the failed Inline Posture node and revert it to the earlier configuration, as needed. Since high availability failover is stateless, all active sessions are automatically reauthorized after a failover occurs.

This section covers the following topics:

- Configuring a High Availability Pair, page 10-25
- Syncing an Inline Posture Node, page 10-28

Configuring a High Availability Pair

This section shows you how to define a high availability relationship between two registered Inline Posture nodes.

In the example that is presented, the service IP address used for the bridged mode high availability pair is different from the physical IP addresses of the Inline Posture nodes, effectively creating a cluster. The WLC interacts with the cluster as a single unit, using the service IP address. For this reason, the service IP is defined for the trusted and untrusted networks.

Configuring Primary and Secondary Inline Posture Nodes

Warning **Both nodes in a high availability pair must use the same mode, either bridged or router. Mixed modes are not supported on Inline Posture high availability pairs.**

Prerequisites

- You should have administrative permissions on the primary Administration ISE node.
- You should have successfully configured two (2) Inline Posture nodes, and registered them on the Cisco ISE network as described in Configuring Inline Posture in Bridged or Routed Mode, page 10-12.
- The eth2 and eth3 interfaces of both nodes in an Inline Posture high availability pair (primary and secondary) communicate with heartbeat protocol exchanges to determine the health of the nodes. For the heartbeat to work, you must connect the eth2 interface of the primary Inline Posture node to the eth2 interface of the secondary node using an Ethernet cable. Likewise, the eth3 interface of the primary Inline Posture node must be connected to the eth3 interface of the secondary node with an Ethernet cable. Figure 10-4 illustrates this principle.
- For RADIUS purposes, you need a service IP address that you will assign to both the trusted and untrusted interfaces of the Inline Posture active-standby cluster during in the course of this procedure.
- Have all necessary network configuration information for your installation on hand. For example, you will need the IP addresses for both Inline Posture nodes, a service IP address for the cluster, the IP address for the Policy Service ISE node, and the shared secret for RADIUS configuration. You might also need the management VLAN ID, WLC IP address, VLAN IP address, and so on. Check with your system architect for a complete list of the information you will need.

To configure an Inline Posture high availability pair, complete the following steps:

Step 1 From the primary Administration ISE node, choose **Administration > System > Deployment**.

Step 2 Click the **Deployment** link in the left panel. Then, in the Deployment Nodes list, check the check box next to the Inline Posture node that you want to designate as the primary node and click the **Edit** icon.

Step 3 On the General Settings tab, verify the node name, that the Inline PEP check box is selected, then choose **Active** as the HA Role from the drop-down menu.

Step 4 Click the **Failover** tab to bring it forward, and check the **HA Enabled** check box.

Step 5 Choose the **HA Peer Node** from the drop-down menu. A list of eligible standalone Inline Posture nodes appears from which to choose.

Step 6 Specify the following for the active node:

a. Enter the Trusted Service IP address (eth0) and the Untrusted Service IP address (eth1) for the traffic interfaces of the primary node. In the bridged mode example that follows, the service IP address is the same for both trusted and untrusted networks.

b. Optionally (but recommended as a best practice), enter the IP address for the Link-Detect system for both the trusted and untrusted sides. This address is usually the IP address for the Policy Service ISE node, because both the active and standby nodes should always be able to reach the Policy Service ISE node.

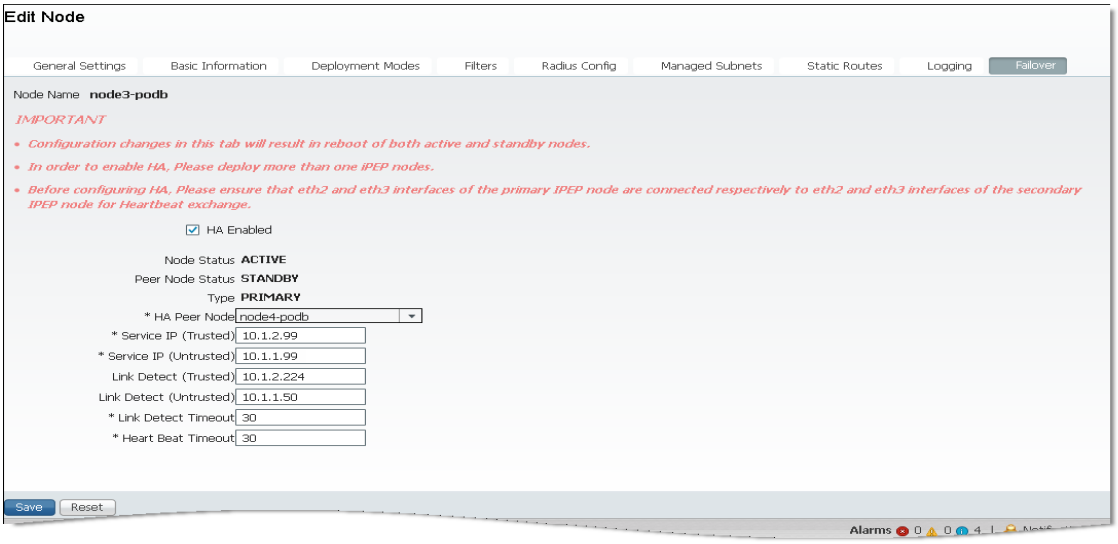
Then, Enter a Link-Detect Timeout value. The default value of 30 seconds is recommended. However, there is no maximum value.

Link-detect ensures that the Inline Posture node maintains communication with the Policy Service ISE node. If the active node does not receive notification (ping) from the Policy Service ISE node at the specified intervals, the active node fails over to the standby node.

Step 7 Enter a Heart Beat Timeout value. The default value of 30 seconds is recommended. However, there is no maximum value.

The heartbeat is a message that is sent between the two Inline Posture nodes at specified intervals. The heartbeat happens on eth2 and eth3 interfaces. If the heartbeat stops or does not receive a response in the allotted time, failover occurs.

Figure 10-22 Failover



Step 8 Choose the **HA Peer Node** from the drop-down menu. The secondary node syncs to the primary node.

- Replication Status—(Only appears for secondary nodes) Indicates whether incremental replication from the primary node to the secondary node is complete or not. You will see one of the following states:
  - Failed—Incremental database replication has failed.
  - In-Progress—Incremental database replication is currently in progress.
  - Complete—Incremental database replication is complete.
  - Not Applicable—Displayed if the ISE node is a standalone or primary node.

- Sync Status—(Only appears for secondary ISE nodes) Indicates whether replication from the primary node to the secondary node is complete or not. A replication happens when a node is registered as secondary or when you click Syncup to force a replication. You will see one of the following states:
  - Sync Completed—Full database replication is complete.
  - Sync in Progress—Database replication is currently in progress.
  - Out of Sync—Database was down when the secondary node was registered with the primary ISE node.
  - Not Applicable—Displayed if the ISE node is a standalone node.

Step 9 If the sync status for any secondary node is out of sync, check the check box next to that node and click **Syncup** to force a full database replication.

Note You must use the Syncup option to force a full replication if the Sync Status is *Out of Sync* or the Replication Status is *Failed*.

Step 10 Click **Save**. Both Inline Posture nodes restart.

When the nodes come back up, they are configured as primary and secondary, according to the settings you specified. You can view the state of a node by selecting the node to edit, as described in Step 2, and then clicking the Failover tab.

Note that the primary node has more options available for editing. That is because you make all configuration changes on the primary node. Configuration changes made to the primary node are automatically populated onto the secondary node. For this reason, the secondary node is read-only.

The following screenshots compare the Failover tabs of the active primary and standby secondary Inline Posture nodes.

Figure 10-23 Inline Posture Active Options

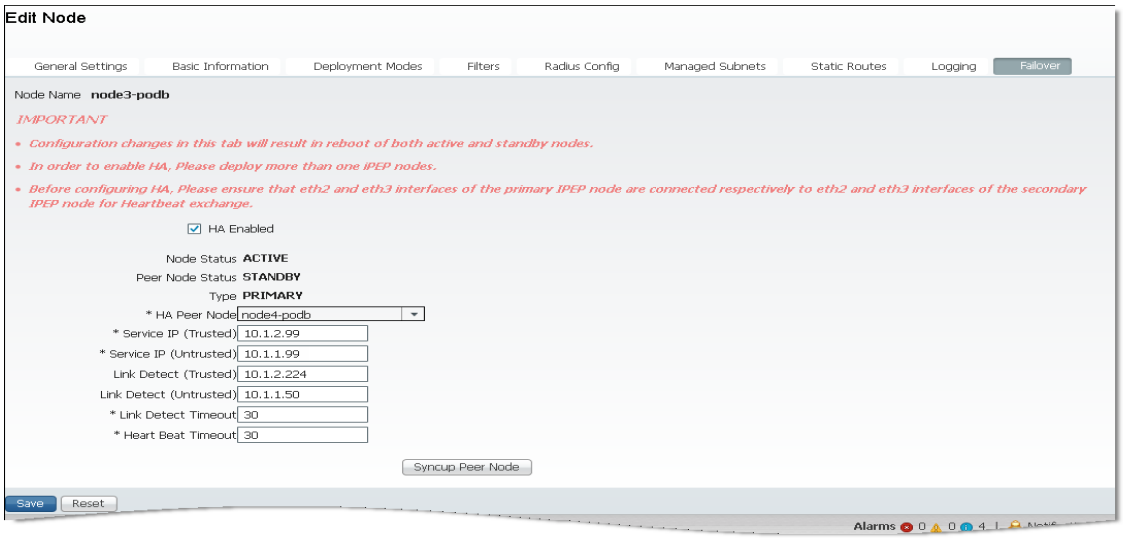
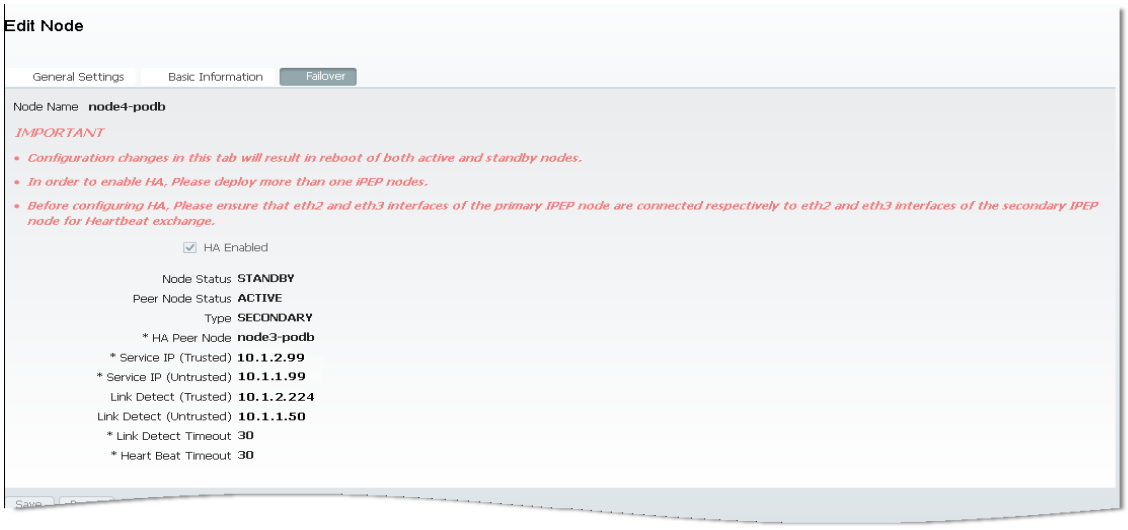


Figure 10-24 Inline Posture Standby Options



Next Step

Complete the following task: Adding Inline Posture as a RADIUS Client, page 10-29.

Troubleshooting Topics

- Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working, page D-7

Syncing an Inline Posture Node

The procedure that is covered in this section assumes that you have already configured two Inline Posture nodes in an active-standby pair. The purpose of this section is to show you how to sync one node in an active-standby pair to the other node.

Prerequisites

- You should have successfully configured two Inline Posture nodes, as described in Configuring Inline Posture in Bridged or Routed Mode, page 10-12.
- You should have successfully established the relationship between the two nodes, as described in Configuring a High Availability Pair, page 10-25.
- You should have administrative permissions on the primary Administration ISE node.

To sync one Inline Posture node to another, complete the following steps:

Step 1 From the primary Administration ISE node, choose **Administration > System > Deployment**.

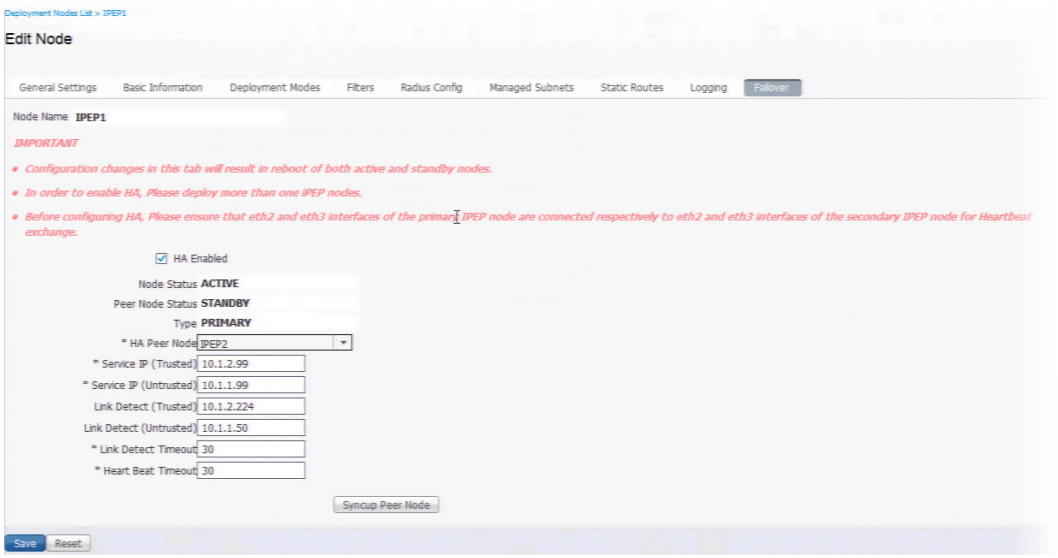
Step 2 Click the **Deployment** link in the left panel. Then, in the Deployment Nodes list, check the check box next to the Inline Posture node to which you want to sync the other node (usually the active node), and click the **Edit** icon.

Step 3 Click the **Failover** tab to bring it forward.

Step 4 Click **Sync Peer Node**.

Data from the selected node is automatically transferred to its peer node.

Figure 10-25 Sync Peer Node



Troubleshooting Topics

- Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working, page D-7

Adding Inline Posture as a RADIUS Client

For a standalone Inline Posture node, you need to add the trusted IP address as a RADIUS client. For a high availability pair, add the service IP address for the trusted interface as a RADIUS client. This section covers the basic steps for this task. For more in-depth information, see Chapter 6, "Managing Network Devices."

Prerequisites

You must have completed the tasks in the appropriate section:

- Deploying an Inline Posture Node, page 10-12
- Configuring Inline Posture for High Availability, page 10-24

To add Inline Posture as a RADIUS client, complete the following steps:

Step 1 Select **Administration > Network Resources > Network Devices**.

Step 2 In the Network Devices navigation panel, choose Network **Devices**.

Step 3 Enter a Name and Description for the device.

Step 4 Do one of the following:

- For a standalone Inline Posture node, enter the IP address for the trusted interface.
- For a high availability pair, enter the service IP address for the trusted interface.

Step 5 Enter a Model Name and Software Version, as necessary

Step 6 For the Network Device Group, specify a Location and Device Type, as necessary.

Step 7 Check the **Authentication Settings** check box, and enter the Shared Secret.

Step 8 Click **Save**.

Next Step

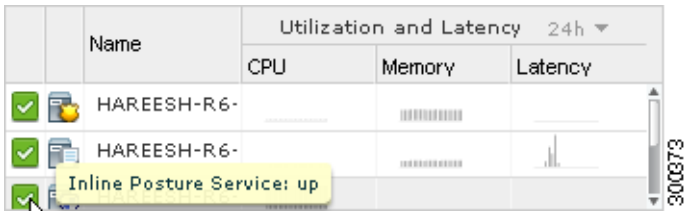
- Monitoring an Inline Posture Node, page 10-30

Monitoring an Inline Posture Node

You can monitor the health of a deployed Inline Posture node from the Cisco ISE dashboard, that is running on the Administration ISE node. The Inline Posture node appears on the System Summary dashlet. A green icon with a check mark means that the system is healthy. A yellow icon indicates a warning, and a red icon indicates of a critical system failure. Sparklines indicate the utilization of CPU, memory, and latency over time. You can choose to display data for the past 24 hours or the last 60 minutes.

When you hover the cursor over the health icon, a quick view dialog appears showing detailed information on system health.

Figure 10-26 System Summary Quick View Status



For more information, see Cisco ISE Dashboard Monitoring, page 23-3.

Removing an Inline Posture Node from Deployment

To remove an Inline Posture node from the deployment, you must first change it to maintenance mode, and then you can deregister it. Maintenance mode is a neutral state that allows the node to smoothly transition to the network or from a deployment.

Prerequisites

- You should have administrative permissions on the primary Administration ISE node.

To remove a node from deployment, complete the following steps:

Step 1 From the primary Administration ISE node, select **Administration > System > Deployment**.

Step 2 Click **Deployment** on the left pane, and then check the check box next to the Inline Posture node that you want to remove from the deployment, and click **Edit**.

Step 3 Click the **Deployment Modes** tab to bring it forward.

Step 4 Click the **Maintenance Mode** radio button, and then click **Save**.

Step 5 Click **Deployment** on the left pane, and then check the check box next to the Inline Posture node that you want to remove from the deployment, and then click **Deregister**.

You are prompted with the following message: Are you sure you want to deregister the selected items?

Step 6 Click **OK** to remove the node from the deployment.

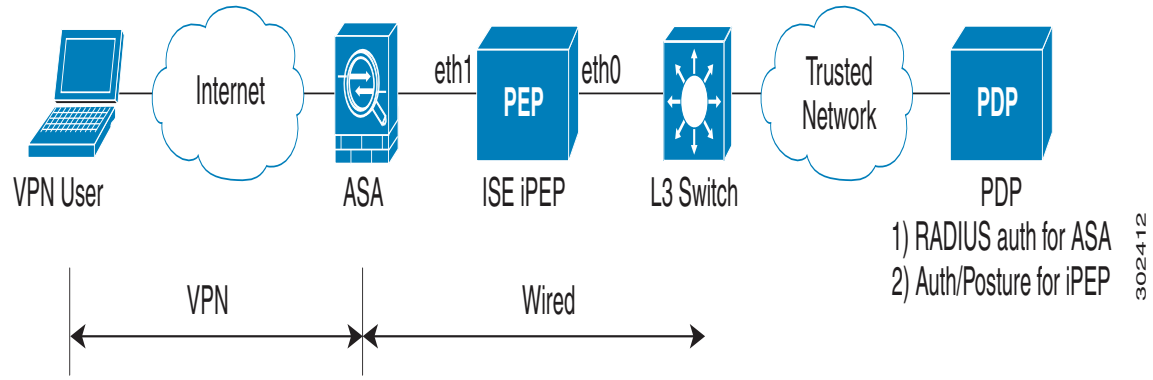
Troubleshooting Topics

- Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working, page D-7

Remote Access VPN Use Case

This section describes how to use an Inline Posture node with a VPN device such as ASA in a Cisco ISE network. Figure 10-27 shows a Cisco ISE deployment that uses an Inline Posture node for remote VPN access. The term iPEP in this illustration refers to the Inline Posture node and PDP refers to the Policy Service node. All the traffic from the VPN gateway must go through the Inline Posture node to ensure that Cisco ISE can apply policies and secure a network.

Figure 10-27 Cisco ISE Deployment with Inline Posture Node



Process Flow

1. Remote user authenticates to VPN gateway (ASA) using the RADIUS protocol.
2. As a RADIUS client, the ASA sends an authentication request to the AAA server (Inline Posture node).
3. As a RADIUS proxy, the Inline Posture node relays the RADIUS authentication request to the Cisco ISE node that acts as the RADIUS Server (Policy Service node).
4. The Cisco ISE Policy Service node authenticates the remote user using the configured identity store and returns the RADIUS response to the Inline Posture node which in turn relays it to the ASA (the network access device (NAD)).
5. Based on the authorization policy that is applicable for the user, the Policy Service node returns the appropriate attributes to the Inline Posture node and optionally to the ASA.
6. Each authorization policy rule entry can reference separate authorization profiles for both the Inline Posture node profile and the NAD (standard authorization profile).
   a. Inline Posture Node Profile: Specifies RADIUS attributes to be applied to the Inline Posture node such as a URL for redirection to the Client Provisioning service and downloadable ACLs (dACLs) for policy enforcement by the Inline Posture node.
   b. Standard Authorization Profile: Specifies any RADIUS attributes intended for NAD, or ASA in this example.
7. If the authorization policy determines that the endpoint is NonCompliant with the posture policy, or if the posture status is Unknown, then the Policy Service node returns a URL redirect attribute value to the Inline Posture node along with a dACL to specify the traffic to be allowed. All HTTP/HTTPS traffic denied by the dACL is redirected to the specified URL.
8. When the posture becomes Compliant, a reauthorization occurs and the Policy Service node sends a new dACL to the Inline Posture node, which provides the user privileged access to the internal network.

Configuring a Cisco ISE Deployment Using an Inline Posture Node

Prerequisite

Ensure that your network infrastructure is configured correctly to route or switch traffic to and from the Inline Posture node and its downstream networks.

To configure your Cisco ISE deployment with an Inline Posture node for remote VPN access, complete the following steps:

Step 1 Configure a standalone Cisco ISE node. For more information, refer to Configuring a Cisco ISE Node, page 9-7.

Step 2 Register the standalone Cisco ISE node as an Inline Posture node to an existing primary Administration ISE node, and configure the Inline Posture node from the primary Administration ISE node. For more information, refer to Deploying an Inline Posture Node, page 10-12.

Step 3 Optionally, you can configure a second Inline Posture node and configure an Active/Standby pair. For more information, refer to Configuring Inline Posture for High Availability, page 10-24.

Step 4 Set up a Policy Service ISE node (PDP) to be the RADIUS server for the Inline Posture node. Configure the Policy Service ISE node with the same RADIUS shared secret that is configured on the Inline Posture node.

Step 5 Add the Inline Posture node as a network access device in the primary Administration ISE node. For more information, refer to Adding Inline Posture as a RADIUS Client, page 10-29.

Step 6 Configure authorization profiles (Inline Posture node profiles) for use by the Inline Posture node. You can optionally configure standard authorization profiles for the NAD's use. For more information, refer to Creating Inline Posture Node Profiles, page 10-21 and Creating Inline Posture Downloadable Access Control Lists, page 10-19.

Step 7 Configure authorization policy to apply the Inline Posture node profiles to remote VPN users based on identity and posture status. For more information, refer to Creating an Inline Posture Authorization Policy, page 10-23.

Step 8 Add the VPN gateway's inside IP address as a RADIUS client in the Inline Posture node's RADIUS configuration along with the NAD's (ASA in this example) RADIUS shared secret.

Step 9 Configure the VPN gateway (ASA) for RADIUS authentication and accounting with the Inline Posture node configured as the RADIUS server. To do this:

a. Choose **Policy > Authentication**.

b. Ensure that the Default Rule is configured to authenticate users against the identity source that contains the user records.

c. Click **Save**.



CHAPTER 11

Setting Up Endpoint Protection Services

This chapter describes how to set up and configure Endpoint Protection Services (EPS), and covers the following topics:

- About Endpoint Protection Services, page 11-1
- EPS Functional Overview, page 11-1
- Enabling and Disabling EPS, page 11-3
- EPS Authorization, page 11-4
- Controlling Endpoints, page 11-6
- Monitoring EPS Data, page 11-8

About Endpoint Protection Services

Endpoint Protection Services (EPS) is a service that runs on the Cisco Identity Services Engine Administration node to extend the monitoring and controlling of endpoints. You can use EPS to monitor and change the authorization state of an endpoint without having to modify the overall Authorization Policy of the system. EPS supports both wired and wireless deployments.

Note EPS is available only with an ISE Advanced license. If you do not have an ISE Advanced license installed, the EPS functionality is not available. For more information, see Chapter 12, "Managing Licenses."

EPS Functional Overview

This section provides an overview of the functional aspects of EPS in Cisco ISE, Release 1.1. EPS operations are supported on both wired and wireless deployments.

EPS allows administrators to manage endpoints through the following actions:

- Quarantine—uses policies to disallow an endpoint access to the network, or limits its access. Policies can be created to assign different authorization profiles depending on the status.
- Unquarantine—reverses the quarantine status, and allowing the endpoint full access to the network.
- Shutdown—deactivates a port on the network attached system (NAS). Once a port is shutdown, you must manually reset the port.

Note Because you must manually reset the port, the shutdown operation is not available for wireless access and devices.

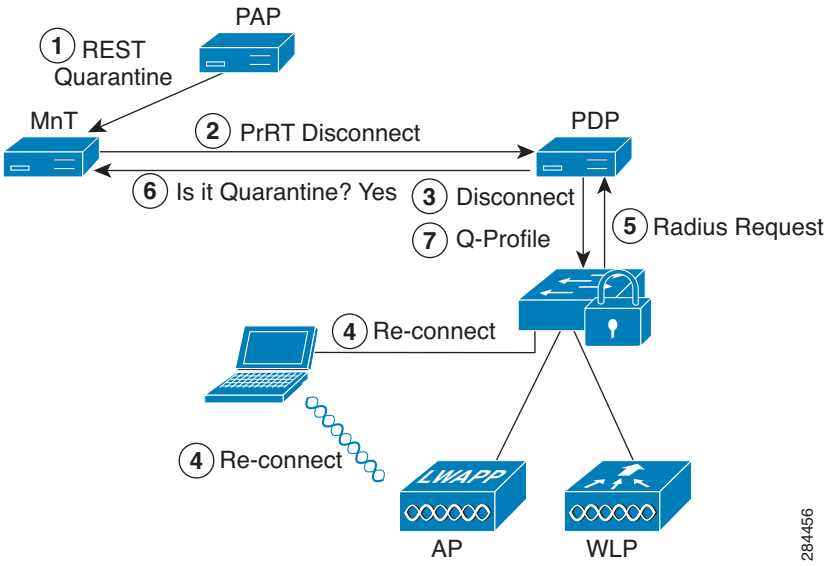
Quarantine and Unquarantine

You can set endpoint protection status to quarantine, and establish policies that assign different authorization profiles, depending on the status of the endpoint.

Quarantine essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. The The Quarantine VLAN must be previously defined by a network administrator and supported on the same NAS as the endpoint. Unquarantine reverses the quarantine action, returning the endpoint to its original VLAN.

The quarantine and unquarantine actions are performed as a result of established Authorization Rules that are defined to check for EPSStatus. In Figure 11-1, the quarantine flow assumes that rules have been configured and the EPS session has been established.

Figure 11-1 EPS Quarantine Flow

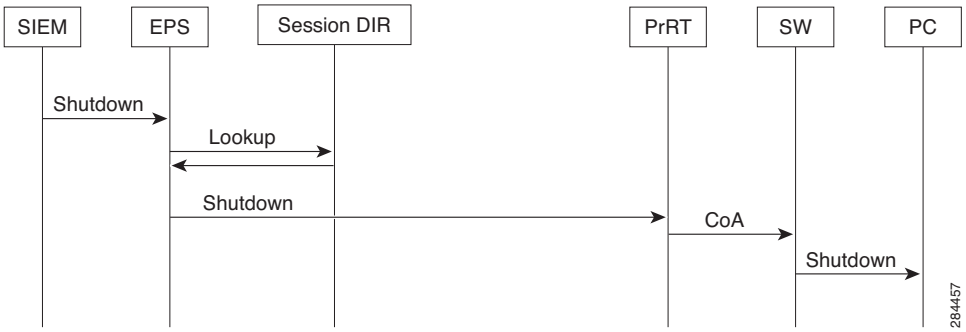


1. A PC endpoint logs onto the network through a wireless device (WLC), and a quarantine REST API call is issued from the Administration ISE node to the Monitoring ISE node.
2. The Monitoring ISE node then calls PrRT through the Policy Services ISE node to invoke a CoA.
3. The PC endpoint is disconnected.
4. The PC then reauthenticates and reconnects.
5. A RADIUS request for the PC endpoint is sent back to the Monitoring ISE node.
6. The PC endpoint is quarantined while the check is made.
7. The Q-Profile authorization policy is applied, and the endpoint is validated.
8. The PC endpoint is unquarantined, and allowed full access to the network.

Shutdown

The shutdown function gives the administrator the ability to close a port based on a specified IP address for MAC address. This function may not be supported on all devices. Figure 11-2 illustrates the EPS shutdown flow.

Figure 11-2 EPS Shutdown Flow



For the PC in the illustration, the shutdown operation is performed on the switch that the PC uses to access the network.

Warning **When you shutdown a port in this manner, you must manually reset the port to make it active again.**

Enabling and Disabling EPS

Endpoint Protection Services (EPS) is disabled by default. You must have Super Admin and Policy Admin role privileges to enable the service, as described in the following procedure.

Note EPS is only available with an ISE Advanced license. If you do not have an ISE Advanced license installed, the EPS functionality is not available. For more information, see Chapter 12, "Managing Licenses."

To enable and disable EPS, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Administration > System > Settings**.

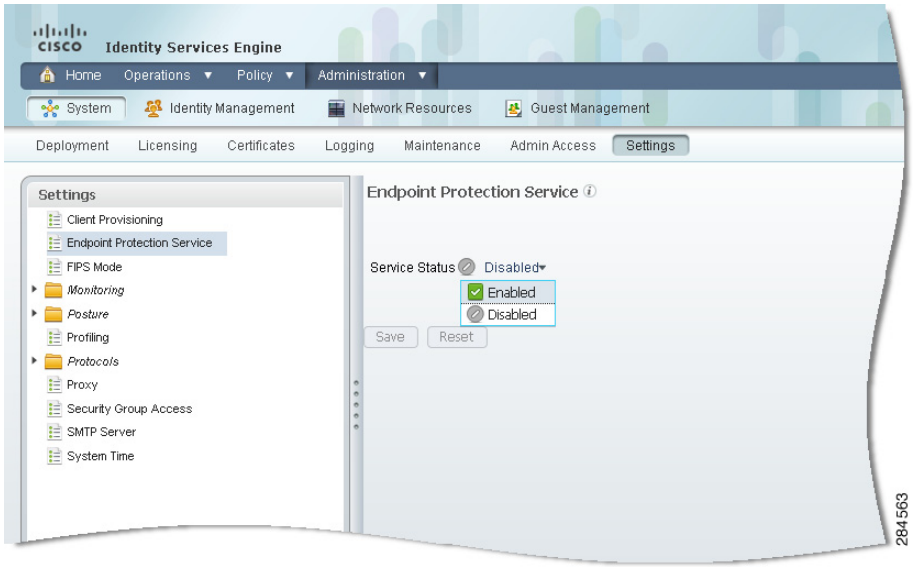
Step 2 In the Settings panel on the left, select **Endpoint Protection Service**.

Step 3 To enable EPS, from the Service Status drop-down menu select **Enabled** and click **Save**.

The service remains enabled until it is manually disabled.

Step 4 To disable EPS, from the Service Status drop-down menu select **Disabled** and click **Save**.

Figure 11-3 Enable and Disable EPS



For information on how to verify that EPS is enabled or disabled using the command line interface (CLI), see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

EPS Authorization

EPS allows you to reset the access status of an endpoint to quarantine, unquarantine, or shutdown. For this to occur, you must create an EPS authorization profile and policy rule.

This section covers the following topics:

- Creating a Quarantine Authorization Profile, page 11-4
- Creating an EPS Policy and Rule, page 11-5

Creating a Quarantine Authorization Profile

An authorization profile acts as a container for permissions that you define to allow access to specified network services. When authorization is complete, the permissions are granted for a network access request. For more information, see Cisco ISE Authorization Policies and Profiles, page 17-5.

This section provides an example of how to create a quarantine authorization profile for use with EPS.

To create a quarantine authorization profile, complete the following steps:

Step 1 In the Cisco ISE Admin user interface, go to **Policy > Policy Elements > Results**.

Step 2 In the Results panel on the left, select **Authorization > Authorization Profiles**.

The Standard Authorization Profiles panel appears on the right.

Step 3 In the Standard Authorization Profiles panel, click **Add**.

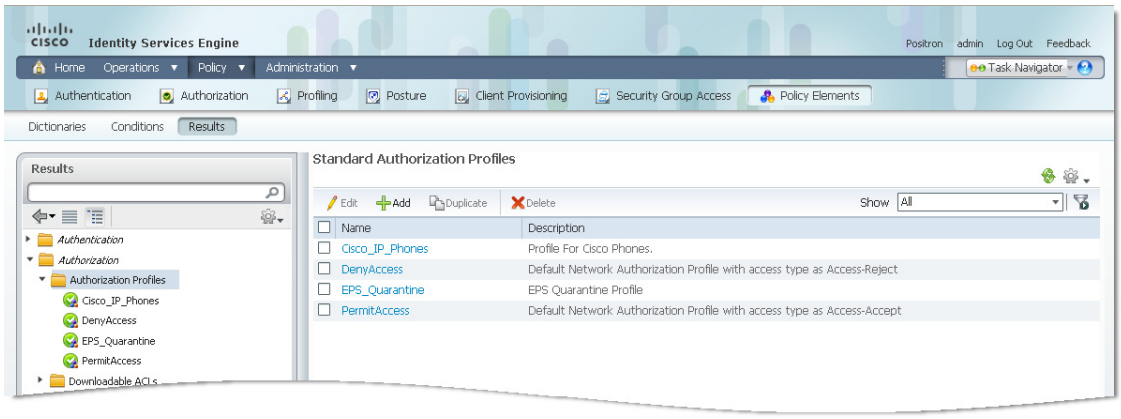
Step 4 Enter a unique **Name** and **Description**, and leave the Access Type as ACCESS_ACCEPT.

Step 5 Check the DACL Name check box and choose **DENY_ALL_ACCESS** from the drop-down list.

Step 6 Click **Save**.

The quarantine profile appears in the list of Standard Authorization Profiles, as shown in Figure 11-4.

Figure 11-4 EPS Quarantine Profile



Creating an EPS Policy and Rule

There are two types of authorization policies: standard and exception. Standard policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges.

By contrast, exception policies act as exceptions to standard policies. Exception polices are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement.

For EPS authorization, it is recommended that you create a quarantine status exception rule that is processed before the standard policies are processed. For more information on both of these types of policies, see Understanding Authorization Policies, page 17-1.

Prerequisite

You should have successfully completed Creating a Quarantine Authorization Profile, page 11-4.

To create an EPS exception policy and rule, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Policy > Authorization**, and expand the **Exceptions** panel.

Step 2 Click **Create New Rule** and enter a **Rule Name** in the text field, such as EPS Exception Rule.

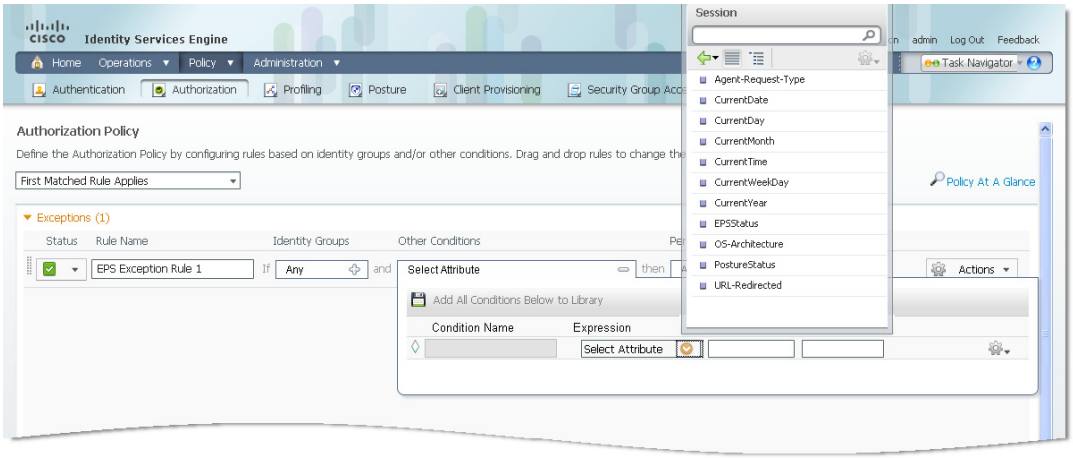
Step 3 Click the **Identity Group** plus sign (**+**) and choose an identity group, or leave the default, Any, as desired.

Step 4 Click the **Conditions** plus sign (**+**), and then click **Create New Condition (Advanced Option)**.

Step 5 Under Expression click **Select Attribute**, and then from the Dictionaries list choose **Session**.

Step 6 From the Session list, choose **EPSStatus**, then choose **Equals** from the first drop-down list on the right, and choose **Quarantine** from the second drop-down list.

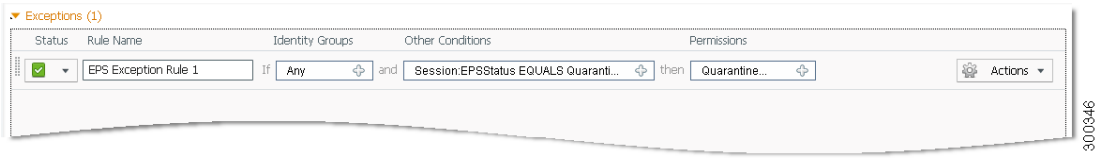
Figure 11-5 Set EPSStatus



Step 7 Scroll down and click **Save**.

The EPS exception rule appears in the Exception list, as shown in Figure 11-6.

Figure 11-6 EPS Exception Rule



Controlling Endpoints

You can quarantine selected endpoints with EPS, to limit their access to the network. If the endpoint is then validated, you can unquarantine the endpoint to allow it full access to the network. If you discover a hostile endpoint on your network, you can shutdown the endpoint's access, using EPS to close the port.

Note Shutdown may not be supported on all devices. Most switches should support the shutdown command, however. You can use the getResult() command to verify that the shutdown executed successfully.

Quarantine and Unquarantine Endpoints

You can quarantine and unquarantine an endpoint using the endpoint IP address or MAC address.

Prerequisites

- EPS must be enabled, as described in Enabling and Disabling EPS, page 11-3.
- You should have established EPS Authorization, page 11-4.

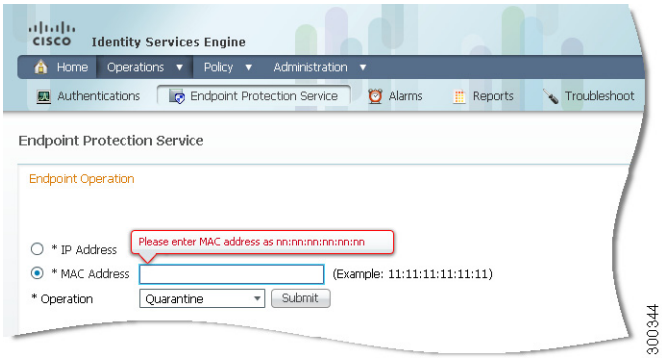
To quarantine and unquarantine an endpoint, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Endpoint Protection Service**.

Step 2 Click the **IP Address** or **MAC address** radio button, then enter the address for the endpoint in the text field, following the designated format.

Note If an active session does not contain information about the IP address of an endpoint, then an EPS operation with that IP address fails in Cisco ISE. This also applies to the MAC address and session ID for that endpoint. Cisco ISE throws the following error message: No active session found for this MAC address, IP Address, or Session ID when an EPS operation is performed with that IP address, MAC address, or session ID not found in the active session.

Figure 11-7 Endpoint Operation



Step 3 From the Operation drop-down menu, select one of the following:

- Quarantine — isolates the endpoint, restricting access on the network
- Unquarantine — reverses the quarantine process, allowing full access to the network

Note Cisco ISE allows you to perform quarantine and unquarantine operations on the same endpoint multiple times, provided they are not performed simultaneously.

Step 4 Click **Submit.**

Port Shutdown

You can shutdown the switch port that an endpoint is connected to using the endpoint IP address or MAC address.

Warning **The shutdown operation closes the switch port. Once this occurs, you have to manually reinstate the port to bring the endpoint back onto the network.**

The shutdown operation is effective only for endpoints that are connected through wired media.

To shutdown an endpoint, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Endpoint Protection Service**.

Step 2 Click the **IP Address** or **MAC address** radio button, then enter the address for the endpoint in the text field, following the designated format.

Step 3 From the Operation drop-down menu, select **Shutdown.**

Step 4 Click **Submit**.

Note You can also verify that a port is shutdown using the getResult() command on the CLI. For more information, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

Monitoring EPS Data

You can view EPS data in the following formats:

- Endpoint Protection Services Report
- Session Directory Reports

This section walks you through the process of running each of these reports. For more information on Cisco ISE reports, see Chapter 24, “Reporting.”

Endpoint Protection Services Report

To view EPS report data, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Endpoint Protection Services**.

Step 3 In the Reports panel on the right, click the **Endpoint Operations History** check box.

Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last 30 minutes
- Last hour
- Last 12 hours

- Today
- Yesterday
- Last 7 days
- Last 30 days
- Query and run

The report runs upon choosing the time period, and the Endpoint Operations History data appears.

Session Directory Reports

Quarantine and unquarantine operations can be triggered from session directory reports as well for active endpoints.

RADIUS Session Directory reports can also be used to track EPS data. There are no limits to the number of users that can be quarantined at one time, and there are no time constraints on the length of the quarantine period.

Note If a quarantined session is unquarantined, the initiation method for a newly unquarantined session depends on the authentication method that is specified by the switch configuration.

To track EPS data using Session Directory reports, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Session Directory**.

Step 3 In the Reports panel on the right, click one of the following radio buttons:

- RADIUS Active Sessions—Provides information on RADIUS authenticated, authorized, and started sessions.
- RADIUS Session History—Provides a summary of RADIUS session history, such as total authenticated and terminated sessions, as well as total and average session duration and throughput for a selected time period.
- RADIUS Terminated Sessions—Provides all the RADIUS terminated session information for a selected time period.

Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last 30 minutes
- Last hour
- Last 12 hours
- Today
- Yesterday
- Last 7 days

- Last 30 days
- Query and run

The report runs upon choosing the time period, and the report data appears.



CHAPTER 12

Managing Licenses

This chapter describes the licensing mechanism and licensing schemes that are available in the Cisco Identity Services Engine (ISE) and how to add or upgrade a license. The following topics are covered:

- Understanding Licensing, page 12-1
- Viewing Current Licenses, page 12-2
- Adding and Upgrading Licenses, page 12-3
- Removing Licenses, page 12-4

Understanding Licensing

In Cisco ISE, licensing enables you to provide coverage for increasing numbers of endpoints and offer more complex policy services, depending on the capabilities of the license or licenses that you choose to apply.

Cisco ISE licenses are available in Base, Advanced, and Wireless packages. Each package includes THE number of SKUs that is equal to the number of licenses that are included in the package. To use Cisco ISE, you must have a valid Base, Base and Advanced, or Wireless License package.

A single endpoint with multiple network connections may consume more than one Base or Advanced License. This situation can occur, for example, if an endpoint has both a wired and a wireless network connection. Each unique authenticated connection will require its own license.

The Base package includes all of the base services that are required to enable authentication and authorization, Guest services, and link encryption. The Advanced package includes Posture, Profiler, Device Registration and Supplicant Provisioning, and Security Group Access services.

The Base License is consumed whenever an authentication notification is received by Cisco ISE. A single Advanced License is consumed when any one or more of the following services or conditions are applied to the endpoint session:

- Posture
- Security Group Tag assignment
- Authorization using profile information
- Endpoint is registered in the MyDevices Portal

Cisco ISE is bundled with a licensing mechanism that has the following important features:

- **Built-in License**—Cisco ISE comes with a built-in evaluation license, which is valid for 90 days. The evaluation license includes both Base and Advanced packages and limits the number of endpoints to 100 for both the Base and Advanced packages. Therefore, you are not required to install a regular license immediately upon installation.
- **Central Management**—Licenses are centrally managed by the ISE administration node. In a distributed deployment, where two ISE nodes assume the Administration persona (primary and secondary), upon successful installation of the license file, the licensing information from the primary Administration node is propagated to the secondary Administration node. So there is no need to install the same license on each Administration node within the deployment.
- **License Count**—The Cisco ISE license is counted as follows:
  - A Base or Advanced license is consumed based on the feature that is utilized.
  - An endpoint with multiple network connections can consume more than one license per MAC address. For example, a laptop connected to wired and also to wireless at the same time. Licenses for VPN connections are based on the IP address.
  - Licenses are counted against concurrent, active sessions. An active session is one for which a RADIUS Accounting Start is received but RADIUS Accounting Stop has not yet been received.

Note Sessions without RADIUS activity are automatically purged from Active Session list every 5 days or if the endpoint is deleted from the system.

The following license types are available in Cisco ISE:

- Evaluation License
- Base License
- Advanced License
- Wireless License

Note Wireless Licenses cannot coexist on an Administration ISE node with Base or Base and Advanced Licenses.

Refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*, for more information about the license types available in the Cisco ISE license scheme.

Viewing Current Licenses

To view current licenses in Cisco ISE, choose **Administration > System > Licensing > Current Licenses**. The Current License page appears, which contains the following information:

- Administration Node—Name of the Cisco ISE server instance where the primary node is installed.
- ID—Administration node ID which is obtained from the licensing information.
- Version—Version number of the Cisco ISE.
- Base Type—The status/type of the Base License that is currently installed on the Administration node.
- Advanced Type—The status or type of the Advanced License that is currently installed on the Administration node.

- Wireless Type—The status or type of the Wireless License that is currently installed on the Administration node.

  After the 90-day evaluation license expires and you install a Wireless License, the Current Licenses page indicates that the Base and Advanced Licenses are "Not Installed."

- Wireless Upgrade Type—The status or type of the Wireless Upgrade License that is currently installed on the Administration node.

  After installing a Wireless Upgrade License, the Current Licenses page indicates that there is now an "Eval (0 Days)" Base License and that the Advanced License is "Not Installed."

- Licensed To—Name of the organization to which the license has been allotted.
- Base—The ratio in this number represents the number of utilized endpoints versus the number of allowed endpoints that are supported under the current Base licensing scheme. For example, if you are using an evaluation license and have identified only one endpoint, this number is 1/100.
- Advanced—The ratio in this number represents the number of utilized endpoints versus the number of allowed endpoints that are supported under the current Advanced licensing scheme. For example, if you are using an evaluation license and have identified only one endpoint, this number is 1/100.

Viewing Licensing History

You can obtain reports about the license types and actions taken (such as when the license was installed, upgraded, deleted, and so on) from the Licensing History page. To view the licensing history, choose **Operations > System > Reports > Licensing History**. The Licensing History page appears, which provides the following licensing information:

- Time Stamp—The time at which a particular license was added, updated, or deleted.
- Admin User Name—Name of the Admin User who took the particular action.
- Admin IP Address—IP address of the Cisco ISE node where the license is installed.
- Action—Action taken, such as created, upgraded, deleted, and so on.
- License File—Name of the license file that has been added, updated, or deleted. This column remains blank if the license is an evaluation license.
- Description—A short description of the action taken.

See System Reports, page 24-11 for information on how to generate a licensing history report.

Adding and Upgrading Licenses

You can add a license only on a standalone or primary Administration ISE node. You can upgrade your existing evaluation license on or before the expiration of the 90-day evaluation period. You have two options for upgrading or replacing your evaluation license. You must take either of these actions:

- Install a Base License and then choose whether or not to also install an Advanced License
- Install a Wireless License

Prerequisite

Make sure that you have obtained and installed appropriate license on your Cisco ISE node. Refer to the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*, for more information about how to obtain a valid license and how to install it.

To add or upgrade a license, complete the following steps:

Step 1 From the ISE Administration interface, select **Administration > System > Licensing > Current Licenses**. The Current Licenses page appears with a list of available deployment licenses and their configuration.

Step 2 Click the radio button next to the license name that you want to upgrade, and click **Edit**.

The Licensed Service page appears, which contains the following information:

- Service—The services that are available on the Cisco ISE node.
- Installations—The services that are currently installed on the Cisco ISE node.
- License File—Type of license that is currently activated on the Cisco ISE node.
- End Points—The number of endpoints that are supported under the current licensing scheme.
- Updated Time—Time at which the license was updated.
- Counter—The number of licenses that are installed in the Cisco ISE node and the number of endpoints that are supported under the current licensing scheme.

Step 3 Click **Add Services**. The Import New License File page appears.

Step 4 Click **Browse** to import the new license file that supports the added service.

Step 5 Click **Save**.

Go back to the Current Licenses page to verify the addition of the upgraded license. For further confirmation, check the features of the respective services for which the license has been upgraded.

Removing Licenses

You can add a license only on a standalone or primary Administration ISE node. You cannot remove evaluation licenses. If you remove the production licenses within the evaluation period, the evaluation license is restored upon deletion.

If Base, Advanced, or Wireless packages are installed, you can remove each of them individually. If you have installed a combined license, all related installations in the Base and Advanced packages are removed.

Note

- If the Advanced package count is greater than the Base package count, then the Base package cannot be deleted.
- If you have installed a Wireless Upgrade License after a Wireless License, you must remove the Wireless Upgrade License before you can remove the underlying Wireless License.

To remove a license, complete the following steps:

Step 1 From the Cisco ISE Administration interface, select **Administration > System > Licensing > Current Licenses**. The Current Licenses page appears with a list of available deployment licenses and their configuration.

Step 2 Click the radio button next to the node name, and click **Edit**. The Licensed Services page appears.

Step 3 Click the radio button next to the license name that you want to delete, and click **Remove**.

Step 4 Click **OK** in the confirmation dialog box to confirm that you want to delete this licensing package.

The Licensed Services page appears, showing the modified status.



CHAPTER 13

Managing Certificates

The Cisco Identity Services Engine (ISE) relies on public key infrastructure (PKI) to provide secure communication for the following:

- Client and server authentication for Transport Layer Security (TLS)-related Extensible Authentication Protocol (EAP) protocols
- HTTPS communication between your client browser and the management server

ISE provides a web interface for managing PKI credentials. There are two types of credentials:

- Local certificates—Used to identify the ISE server to other entities such as EAP supplicants, external policy servers, or management clients. Local certificates are also known as identity certificates. Along with the local certificate, a private key is stored in ISE to prove its authenticity.

  Cisco ISE identifies when a local certificate is about to expire and logs a warning in the audit logs. The expiration date also appears in the local certificate list page (Administration > System > Certificates > Local Certificates). The audit log message is logged in the *catalina.out* file. You can download this file as part of the support bundle (Operations > Troubleshoot > Download Logs). The *catalina.out* file will be available in this directory: support\apache_logs. There are two types of audit log messages that provide information on local certificate expiration warnings:

  - Certificate expiring in < 90 days—AuditMessage: 34100: Certificate.ExpirationInDays, Certificate.IssuedBy, Certificate.CertificateName, Certificate.IssuedTo
  - Certificate has expired—AuditMessage: 34101: Certificate.ExpirationDate, Certificate.IssuedBy, Certificate.CertificateName, Certificate.IssuedTo

- Certificate authority certificates—Used to verify remote certificates that are presented to ISE. Certificate authority certificates have a dependency relation that forms a Certificate Trust List (CTL) hierarchy. This hierarchy connects a certificate with its ultimate root certificate authority (CA) and verifies the authenticity of the certificate.

In a distributed deployment, at the time of registering a secondary node to the primary node, the secondary node should present a valid certificate. Usually, the secondary node will present its local HTTPS certificate. To provide authentication for deployment operations that require direct contact with the secondary node, the CTL of the primary node should be populated with the appropriate trust certificates, which can be used to validate the HTTPS certificate of the secondary node. Before you register a secondary node in a deployment, you must populate the CTL of the primary node. If you do not populate the CTL of the primary node, node registration fails. Node registration also fails if certificate validation fails for some reason.

Note After you obtain the backup from your standalone ISE node or primary Administration ISE node, if you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data. Otherwise, if you try to restore data using the older backup, the communication between the nodes might fail.

This chapter contains the following sections:

- Local Server Certificates, page 13-2
- Certificate Signing Requests, page 13-15
- Certificate Authority Certificates, page 13-16
- OCSP Services, page 13-25

Local Server Certificates

After installation, ISE generates, by default, a self-signed local certificate and private key, and stores them on the server. For certificate-based authentications, ISE authenticates itself to clients using the default self-signed certificate that is created at the time of installation. This self-signed certificate is used for both HTTPS and EAP protocols to authenticate clients. This self-signed certificate is valid for one year and its key length is set to 1024 bits. At the time of generation, this certificate is used for both EAP and HTTPS protocols. You can change this definition after you have imported or generated other local certificates. In a self-signed certificate, the hostname of ISE is used as the common name (CN) because it is required for HTTPS communication.

Note When you change the HTTPS local certificate on a node, existing browser sessions that are connected to that node do not automatically switch over to the new certificate. You must restart your browser in order to see the new certificate. This note applies for both Firefox and Internet Explorer 8 browsers.

Currently, Cisco ISE automatically creates self-signed certificates after initial installation. Cisco strongly recommends installing a CA-signed certificate and configuring it for use by HTTPS or EAP or both. You can import a CA certificate and its private key or request a CA for a CA-signed certificate. To request a CA-signed certificate, you must generate a certificate signing request (CSR) from the Cisco ISE user interface, export it, and send it to a CA. The CA will sign the certificate and return it to you. You must then bind the certificate that the CA returned with the private key that is stored with the CSR in ISE. After you bind this certificate with the private key, you can configure it for HTTPS or EAP or both.

The ISE provides a web interface that allows you to do the following:

- Import a local certificate and its private key from files residing on the system that is running the client browser. The private key can be encrypted or unencrypted. If the private key is encrypted, you must specify the password to decrypt it. After importing it into ISE, you can designate it as the certificate for Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) mutual authentication, or HTTPS communication between browser clients and the management server, or both. ISE checks the certificate for basic X509 certificate format, checks if the private key matches the public key in the certificate, and prevents duplicate certificates.

Note You can also choose the import option when you have exported the certificate and private key from another ISE server. You must specify a password to encrypt the private key while exporting it from another ISE server. You can import certificates only in privacy-enhanced mail (PEM) and Distinguished Encoding Rules (DER) formats.

- View a list of local certificates that are stored on ISE and their expiration dates.
- Edit a local certificate. You can change the friendly name and description and the protocol associations (HTTPS or EAP or both). You can request a renewal of self-signed certificates and thereby extend the expiration date.
- Delete a local certificate.
- Generate a self-signed certificate.
- Generate a CSR.
- Export a CSR to a file that resides on the system that is running the client browser to forward the CSR to a CA that will sign the certificate.
- Delete a CSR.
- Bind a CA certificate to its private key.
- Replace a local certificate with a duplicate certificate.

Note To plan your Inline Posture deployment and to know more about the Extended Key Usage (EKU) requirements for Inline Posture, see the "Guidelines for Configuring Certificates for Inline Posture" section on page 10-12.

This section covers the following topics:

- Viewing Local Certificates, page 13-3
- Adding a Local Certificate, page 13-4
- Editing a Local Certificate, page 13-11
- Deleting a Local Certificate, page 13-13
- Exporting a Local Certificate, page 13-13

Viewing Local Certificates

The Local Certificate page lists all the local certificates added to the ISE.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To view the local certificate list, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

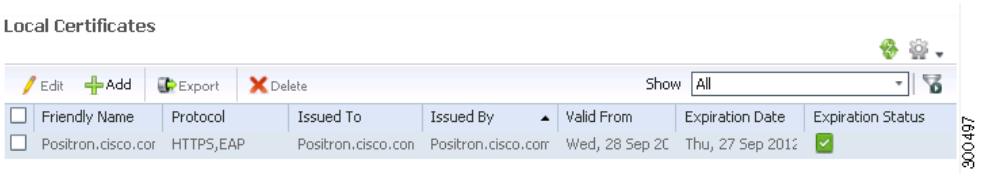
Step 2 From the Certificate Operations navigation pane on the left, click **Local Certificates**.

The Local Certificate page appears and provides the following information for the local certificates as shown in Figure 13-1:

- Friendly Name—Name of the certificate.
- Protocol—Protocols for which to use this certificate.
- Issued To—Certificate subject or the CN to which the certificate is issued.

  The common name is usually the fully qualified domain name of the ISE node.
- Issued By—Server that issued this certificate.
- Valid From—Date on which the certificate was created.
- Expiration Date—Expiration date of the certificate.
- Expiration Status—Provides information about the status of the certificate expiration. There are five icons and categories of informational message that appear in this column:
  1. Active (green icon)
  2. Expiring in less than 90 days (blue icon)
  3. Expiring in less than 60 days (yellow icon)
  4. Expiring in less than 30 days (orange icon)
  5. Expired (red icon)

Figure 13-1 Local Certificate List Page



Adding a Local Certificate

Note If your ISE deployment has multiple nodes in a distributed setup, you must add a local certificate to each node in your deployment individually because the private keys are not stored in the local database and are not copied from the relevant nodes.

You can add a local certificate to ISE in one of the following ways:

- Importing a Server Certificate, page 13-5
- Generating a Self-Signed Certificate, page 13-7
- Generating a Certificate Signing Request, page 13-8 and Binding a CA-Signed Certificate, page 13-10

Importing a Server Certificate

Before you import a local certificate, ensure that you have the local certificate and the private key file on the system that is running the client browser.

Note When you change the HTTPS local certificate on a node, existing browser sessions connected to that node do not automatically switch over to the new certificate. You must restart your browser in order to see the new certificate. This note applies for both Firefox and Internet Explorer 8 browsers.

Prerequisites:

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- If the local certificate that you import contains the basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.

To import a server certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Local Certificates**.

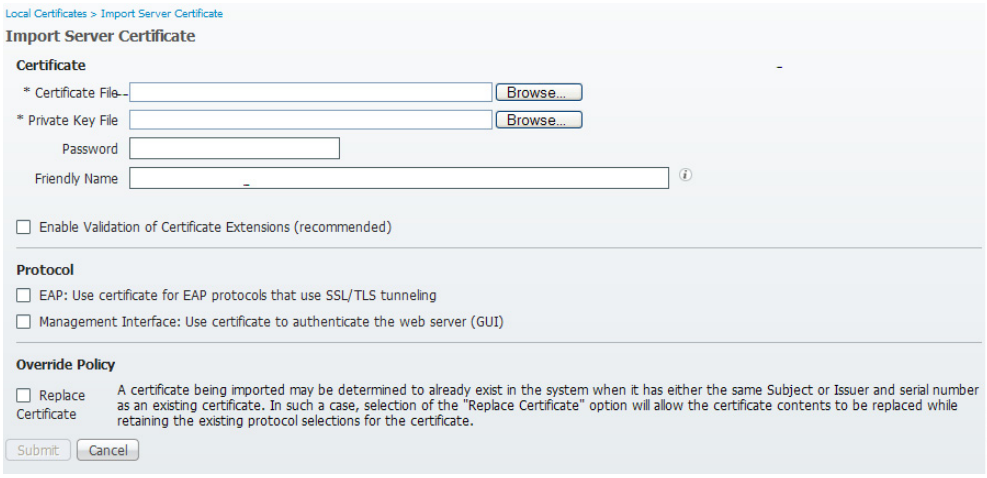
Note To import a local certificate to a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

Step 3 Choose **Add > Import Local Server Certificate**.

The Import Local Server Certificate page appears as shown in Figure 13-2.

Figure 13-2 Import Local Server Certificate Page



Step 4 Click **Browse** to choose the certificate file and the private key from the system that is running your client browser.

If the private key is encrypted, enter the **Password** to decrypt it.

Step 5 If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format <*common name*>#<*issuer*>#<*nnnnn*> where <*nnnnn*> is a unique five-digit number.

Step 6 If you want Cisco ISE to validate certificate extensions, enable the **Enable Validation of Certificate Extensions** option.

Note If you enable the **Enable Validation of Certificate Extensions** option, and the certificate that you are importing contains a basic constraints extension with the Certificate Authority (CA) flag set to true, ensure that the key usage extension is present, and that the "keyEncipherment" bit or the "keyAgreement" bit, or both, are also set.

Step 7 In the Protocol area:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the ISE node.
- Check the **Management Interface** check box to use this certificate to authenticate the web server (GUI).

Note If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the fully qualified domain name (FQDN) of the node. Otherwise, the import process will fail.

Step 8 In the Override Policy area, check the **Replace Certificate** check box to replace an existing certificate with a duplicate certificate. A certificate is considered a duplicate if it has the same subject or issuer and the same serial number as an existing certificate. This option updates the content of the certificate, but retains the existing protocol selections for the certificate.

Note If Cisco ISE is set to operate in FIPS mode, the certificate must be 2048 bits in size and use either SHA-1 or SHA-256 encryption.

Step 9 Click **Submit** to import the local certificate.

If you import a local certificate to your primary ISE node, and if the management interface option is enabled on the node in your deployment, Cisco ISE automatically restarts the application server on the node. Otherwise, you must restart the secondary nodes that are connected to your primary ISE node.

To restart the secondary nodes, from the command-line interface (CLI), enter the following commands:

a. **application stop ise**

b. **application start ise**

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on these commands.

Generating a Self-Signed Certificate

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To generate a self-signed certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Local Certificates**.

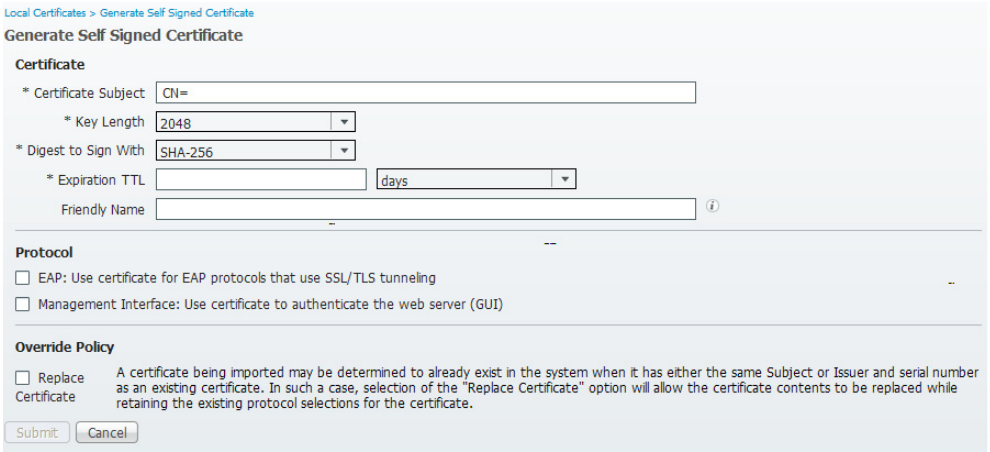
Note To generate a self-signed certificate from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

Step 3 Choose **Add > Generate Self-Signed Certificate**.

The Generate Self-Signed Certificate page appears, as shown in Figure 13-3.

Figure 13-3 Generating a Self-Signed Certificate Page



Step 4 Enter the following information:

- **Certificate Subject**—A distinguished name (DN) identifying the entity that is associated with the certificate. The DN must include a common name (CN) value.
- Required **Key Length**—Valid values are 512, 1024, 2048, 4096. (If you are deploying Cisco ISE as a FIPS-compliant policy management engine, you must specify a 2048 bit or larger key length).
- **Digest to Sign With**—You can choose to encrypt and decrypt certificates using either SHA-1 or SHA-256.
- Certificate **Expiration**. You can specify a time period in days, weeks, months, or years.

- If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format <*common name*>#<*issuer*>#<*nnnnn*> where <*nnnnn*> is a unique five-digit number.

Step 5 In the Protocol area:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the ISE node.
- Check the **Management Interface** check box to use this certificate to authenticate the web server (GUI). You must also reboot the Cisco ISE if you are turning on this function for the first time.

Note If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the FQDN of the node. Otherwise, the self-signed certificate will not be generated.

Step 6 In the Override Policy area, check the **Replace Certificate** check box to replace an existing certificate with a duplicate certificate. A certificate is considered a duplicate if it has the same subject or issuer and the same serial number as an existing certificate. This option updates the content of the certificate, but retains the existing protocol selections for the certificate.

Step 7 Click **Submit** to import the local certificate.

If you import a local certificate to your primary ISE node, and if the management interface option is enabled on the node in your deployment, Cisco ISE automatically restarts the application server on the node. Otherwise, you must restart the secondary nodes that are connected to your primary ISE node.

To restart the secondary nodes, from the command-line interface (CLI), enter the following commands:

a. **application stop ise**

b. **application start ise**

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on these commands.

Note If you are using a self-signed certificate and you need to change the hostname of your Cisco ISE node, ISE will continue to use the self-signed certificate with the old hostname after the hostname change. You must log into the administrative user interface of the Cisco ISE node, delete the existing self-signed certificate that has the old hostname, and generate a new self-signed certificate.

Generating a Certificate Signing Request

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To generate a certificate signing request (CSR), complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Local Certificates**.

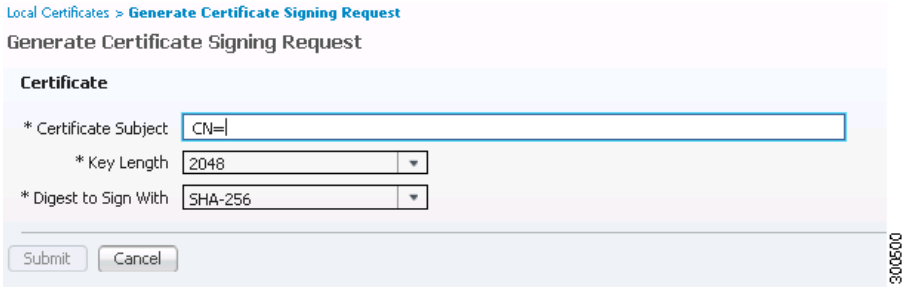
Note To generate a CSR from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

Step 3 Choose **Add > Generate Certificate Signing Request**.

The Generate Certificate Signing Request page appears as shown in Figure 13-4.

Figure 13-4 Generating a Certificate Signing Request



Step 4 Enter the certificate subject and the required key length. The certificate subject is a distinguished name (DN) identifying the entity that is associated with the certificate. The DN must include a common name value. Elements of the distinguished name are:

- C = Country
- S = Test State or Province
- L = Test Locality (City)
- O = Organization Name
- OU = Organizational Unit Name
- CN = Common Name
- E = Email Address

An example of Certificate Subject in a CSR should look like “CN=Host-ISE.cisco.com, OU=Cisco O=security, C=US, S=NC, L=RTP, e=test@test.com.”

Note When populating the Certificate Subject field, do not encapsulate the string in quotes.

Note If you intend to use the certificate generated from this CSR for HTTPS communication (Management Interface), ensure that the CN value in the Certificate Subject is the FQDN of the node. Otherwise, you will not be able to select Management Interface when binding the generated certificate.

Step 5 Choose to encrypt and decrypt certificates using either SHA-1 or SHA-256.

Note If Cisco ISE is set to operate in FIPS mode, the certificate must be 2048 bits in size and use either SHA-1 or SHA-256 encryption.

Step 6 Click **Submit** to generate a CSR.

A CSR and its private key are generated and stored in ISE. You can view this CSR in the Certificate Signing Requests page. You can export the CSR and send it to a CA to obtain a signature.

Binding a CA-Signed Certificate

After your CSR is signed by a CA and returned to you, use this process to bind the CA-signed certificate with its private key. You can also use the bind function to import a CA-signed certificate and its respective private key that you have exported from another Cisco ISE box in your deployment.

Prerequisites:

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- If the certificate that you bind contains the basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.

To bind a CA-signed certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Local Certificates**.

Note To bind a CA-signed certificate to a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

Step 3 Choose **Add > Bind CA Certificate**.

The Bind CA Signed Certificate page appears as shown in Figure 13-5.

Figure 13-5 Binding a CA-Signed Certificate



Step 4 Click **Browse** to choose the CA-signed certificate.

Step 5 If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format <*common name*>#<*issuer*>#<*nnnnn*> where <*nnnnn*> is a unique five-digit number.

Step 6 If you want Cisco ISE to validate certificate extensions, enable the **Enable Validation of Certificate Extensions** option.

Note If you enable the **Enable Validation of Certificate Extensions** option, and the certificate that you are importing contains a basic constraints extension with the Certificate Authority (CA) flag set to true, ensure that the key usage extension is present, and that the "keyEncipherment" bit or the "keyAgreement" bit, or both, are also set.

Step 7 In the Protocol area:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the ISE node.
- Check the **Management Interface** check box to use this certificate to authenticate the web server (GUI).

Note If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the FQDN of the node. Otherwise, the bind operation will fail.

Step 8 In the Override Policy area, check the **Replace Certificate** check box to replace an existing certificate with a duplicate certificate. A certificate is considered a duplicate if it has the same subject or issuer and the same serial number as an existing certificate. This option updates the content of the certificate, but retains the existing protocol selections for the certificate.

Step 9 Click **Submit** to bind the CA-signed certificate.

Editing a Local Certificate

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To edit a local certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Local Certificates**.

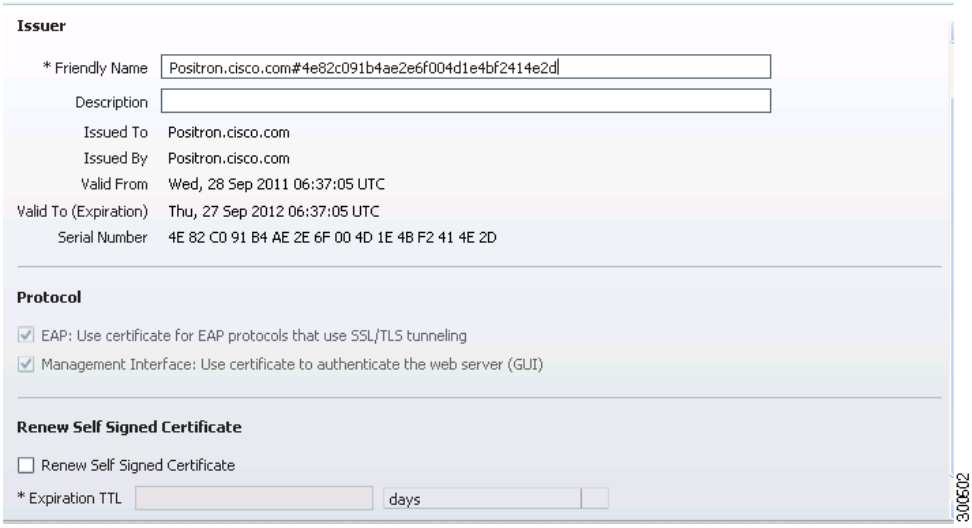
Note To edit a local certificate on a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

Step 3 Check the check box next to the certificate that you want to edit and click **Edit**.

The page refreshes and lists the information for the local certificate as shown in Figure 13-6.

Figure 13-6 Local Certificate Edit Page



You can edit the following:

- Friendly Name
- Description
- Protocols
- Expiration TTL (if the certificate is self-signed)

Step 4 Enter a friendly name to easily identify this certificate when you have many certificates with the same certificate subject.

Step 5 Enter an optional description.

Step 6 In the Protocol area:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the ISE node.
- Check the **Management Interface** check box to use this certificate to authenticate the web server (GUI).

Note If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the FQDN of the node. Otherwise, the edit operation will fail.

For example, if local_certificate_1 is currently designated for EAP and you check the EAP check box while editing local_certificate_2, then after you save the changes to local_certificate_2, local_certificate_1 will no longer be associated with EAP.

Step 7 To renew your self-signed certificate, check the **Renew Self Signed Certificate** check box and enter the expiration Time to Live (TTL) in days, weeks, months, or years.

Step 8 Click **Save** to save your changes.

If the management interface option is enabled on the node in your deployment, Cisco ISE automatically restarts the application server on the node. Otherwise, you must restart the secondary nodes that are connected to your primary ISE node.

To restart the secondary nodes, from the command-line interface (CLI), enter the following commands:

a. **application stop ise**

b. **application start ise**

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on these commands.

Deleting a Local Certificate

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete a local certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Local Certificates**.

Note To delete a local certificate from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

Step 3 Check the check box next to the certificate or certificates that you want to delete and click **Delete**.

Step 4 The following message appears in a pop-up dialog box.

Are you sure you want to delete the selected item(s)?

Step 5 Click **OK** to delete the local certificate or certificates.

Exporting a Local Certificate

You can export the selected local certificate, or the certificate and the private key.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To export a local certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Local Certificates**.

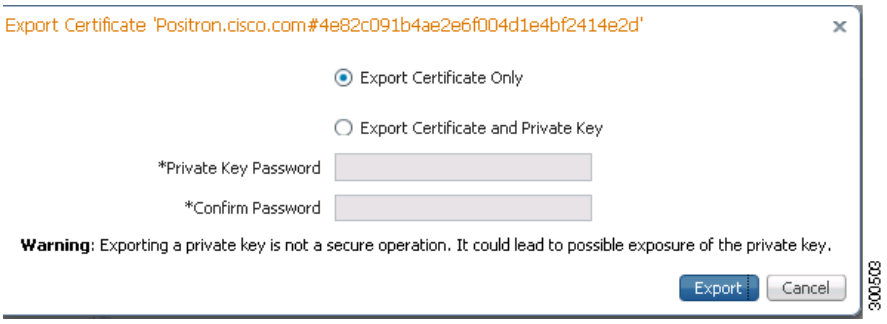
Note To export a local certificate from a secondary node, choose **Administration > System > Server Certificate**.

The Local Certificate page appears.

Step 3 Check the check box next to the certificate that you want to export, then click **Export**.

The Select Certificate Components to Export dialog box appears as shown in Figure 13-7.

Figure 13-7 Exporting a Local Certificate



You can choose to export only the certificate, or the certificate and the private key.

Cisco does not recommend exporting the private key associated with the certificate because its value may be exposed. If you must export the private key, you must specify an encryption password for the private key. You will need to specify this password while importing this certificate into another ISE server to decrypt the private key.

Note If the certificate being exported was previously imported into ISE with an encrypted private key, you do not have to use the same password again while exporting it a second time.

Step 4 Choose the certificate component that you want to export.

Step 5 Enter the password if you have chosen to export the private key. The password should be at least 8 characters long.

Step 6 Click **OK** to save the certificate to the file system that is running your client browser.

If you export only the certificate, the certificate is stored in the privacy-enhanced mail format. If you export both the certificate and the private key, the certificate is exported as a zip file that contains the certificate in the privacy-enhanced mail format and the encrypted private key file.

Certificate Signing Requests

The list of CSRs that you have created is available in the Certificate Signing Requests page. To obtain signatures from a CA, you must export the CSRs to the local file system that is running your client browser. You must then send the certificates to a CA. The CA will sign and return your certificates. The Certificate Signing Requests page allows you to export the CSRs to the local file system.

Note If your ISE deployment has multiple nodes in a distributed setup, you must export the CSRs from each node in your deployment individually.

This section contains the following topics:

- Viewing and Exporting Certificate Signing Requests, page 13-15
- Deleting a Certificate Signing Request, page 13-16

Viewing and Exporting Certificate Signing Requests

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To view the CSRs, complete the following steps:

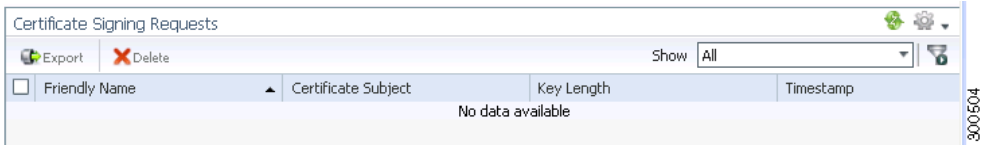
Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Signing Requests**.

Note If you want to view or export CSRs from a secondary node, choose **Administration > System > Certificate Signing Requests**.

The Certificate Signing Requests page appears with a list of CSRs as shown in Figure 13-8.

Figure 13-8 Certificate Signing Requests



Step 3 Check the check box next to the certificates that you want to export and click **Export**.

Step 4 Click **OK** to save the file to the file system that is running the client browser.

Deleting a Certificate Signing Request

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete a CSR, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Signing Requests**.

Note If you want to delete a CSR from a secondary node, choose **Administration > System > Certificate Signing Requests**.

The Certificate Signing Requests page appears with a list of CSRs.

Step 3 Check the check box next to the certificates that you want to delete and click **Delete**.

The following message appears:

Are you sure you want to delete the selected item(s)?

Step 4 Click **OK** to delete the CSR.

Certificate Authority Certificates

Certificate authority (CA) certificates are trusted certificates that are used to verify the identity of the client and server certificates that are presented to Cisco ISE. The digital certificates that are issued by a CA contain a public key and the identity of the user. You must request the certificate authority certificate from your CA and import it into ISE. When you import more than one certificate authority certificate, the certificate authority certificates form a Certificate Trust List (CTL). When a client sends an authentication request, ISE verifies the client certificate against the CTL. If the certificate of the client is issued by a CA that is present in the CTL, then ISE authenticates the client.

Cisco ISE does not support wildcard certificates.

ISE provides a web interface that allows you to do the following:

- Import a certificate authority certificate from a file residing on the system that is running the client browser. The certificate file must contain a privacy-enhanced mail or DER-formatted X509 certificate. After import, you can define the certificate as the Extensible Authentication Protocol-Certificate Trust List (EAP-CTL), which indicates that it is the immediate trust for TLS-related EAP protocols.
- Validate a certificate authority certificate.
- View the list of certificate authority certificates on the ISE node.
- Delete a certificate authority certificate.

- Edit the certificate authority certificate. You can edit the friendly name and description, the trust designation for EAP protocols, and the certificate revocation list (CRL) configuration.
- Export a certificate authority certificate to a file residing on the system that runs the client browser.

Note When deregistering a node whose status has changed (for example, a node status that reverts to standalone), you need to examine the Certificate Trust Store to verify if the certificate that is listed in the Certificate Authority Certificate table still applies or is still a valid certificate. Certificates that are no longer needed because the node is no longer part of a distributed deployment can be deleted. However, when a node is deregistered, the corresponding certificate stores are not automatically revised or updated by ISE. You would have to manually delete such certificates that you no longer need.

This section covers the following topics:

- Viewing Certificate Authority Certificates, page 13-17
- Adding a Certificate Authority Certificate, page 13-18
- Editing a Certificate Authority Certificate, page 13-19
- Deleting a Certificate Authority Certificate, page 13-22
- Exporting a Certificate Authority Certificate, page 13-22
- Importing Certificate Chains, page 13-23
- Creating Certificate Trust Lists in the Primary ISE Node, page 13-23

Viewing Certificate Authority Certificates

The certificate authority certificates page lists all the certificates that have been added to ISE.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

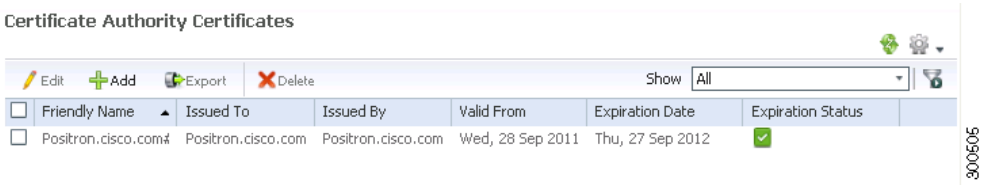
To view the certificate authority certificates, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Authority Certificates**.

The Certificate Authority Certificates page appears as shown in Figure 13-9.

Figure 13-9 Certificate Authority Certificate List Page



This page provides the following information for the certificate authority certificates:

- Friendly Name—Name of the certificate authority certificate.
- Issued To—Certificate subject or the company name to which the certificate has been issued.
- Issued By—CA that issued the certificate.
- Valid From—Date on which the certificate was issued.
- Expiration—The expiration date of the certificate authority certificate.
- Expiration Status—Provides information about the status of the certificate expiration. There are five icons and categories of informational message that appear in this column:
  1. Active (green icon)
  2. Expiring in less than 90 days (blue icon)
  3. Expiring in less than 60 days (yellow icon)
  4. Expiring in less than 30 days (orange icon)
  5. Expired (red icon)

Adding a Certificate Authority Certificate

Note Before you add a certificate authority certificate, ensure that the certificate authority certificate resides on the file system that is running the client browser.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To add a certificate authority certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

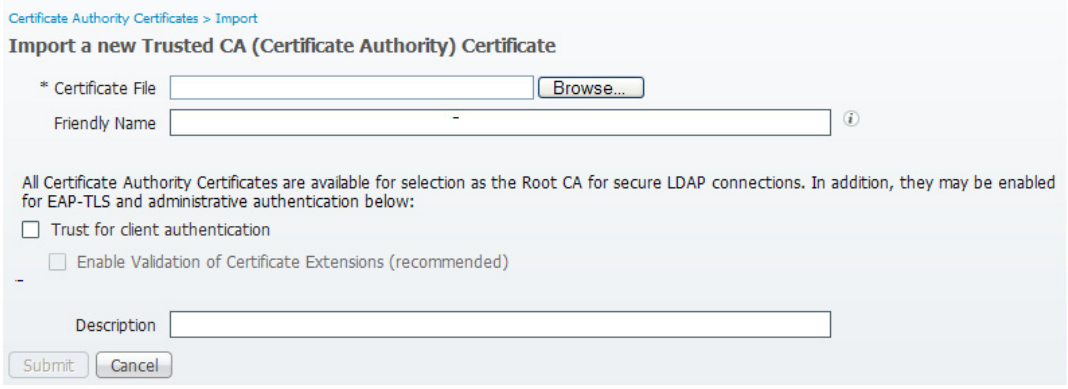
Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Authority Certificates**.

The Certificate Authority Certificates page appears.

Step 3 Click **Add**.

The Import a new Trusted CA (Certificate Authority) Certificate page appears as shown in Figure 13-10.

Figure 13-10 Import a Trusted CA Page



Step 4 Click **Browse** to choose the certificate authority certificate from the file system that is running the client browser.

Step 5 If you would like to specify a **Friendly Name** for the certificate, enter it in the field below the private key password. If you do not specify a name, Cisco ISE automatically creates a name in the format <*common name*>#<*issuer*>#<*nnnnn*> where <*nnnnn*> is a unique five-digit number.

Step 6 Check the **Trust for client authentication** check box if you want to use this certificate in the trust list.

Note If you check both the **Trust for client authentication** and **Enable Validation of Certificate Extensions** options, ensure that the "keyUsage" extension is present and the "keyCertSign" bit is set, and that the basic constraints extension is present with the CA flag set to true.

Step 7 Add an optional description.

Step 8 Click **Submit** to save the certificate authority certificate.

If client certificate-based authentication is enabled, then Cisco ISE will restart the application server on each node in your deployment, starting with the application server on the primary Administration node and followed, one-by-one, by each additional node.

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on these commands.

Editing a Certificate Authority Certificate

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To edit a certificate authority certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

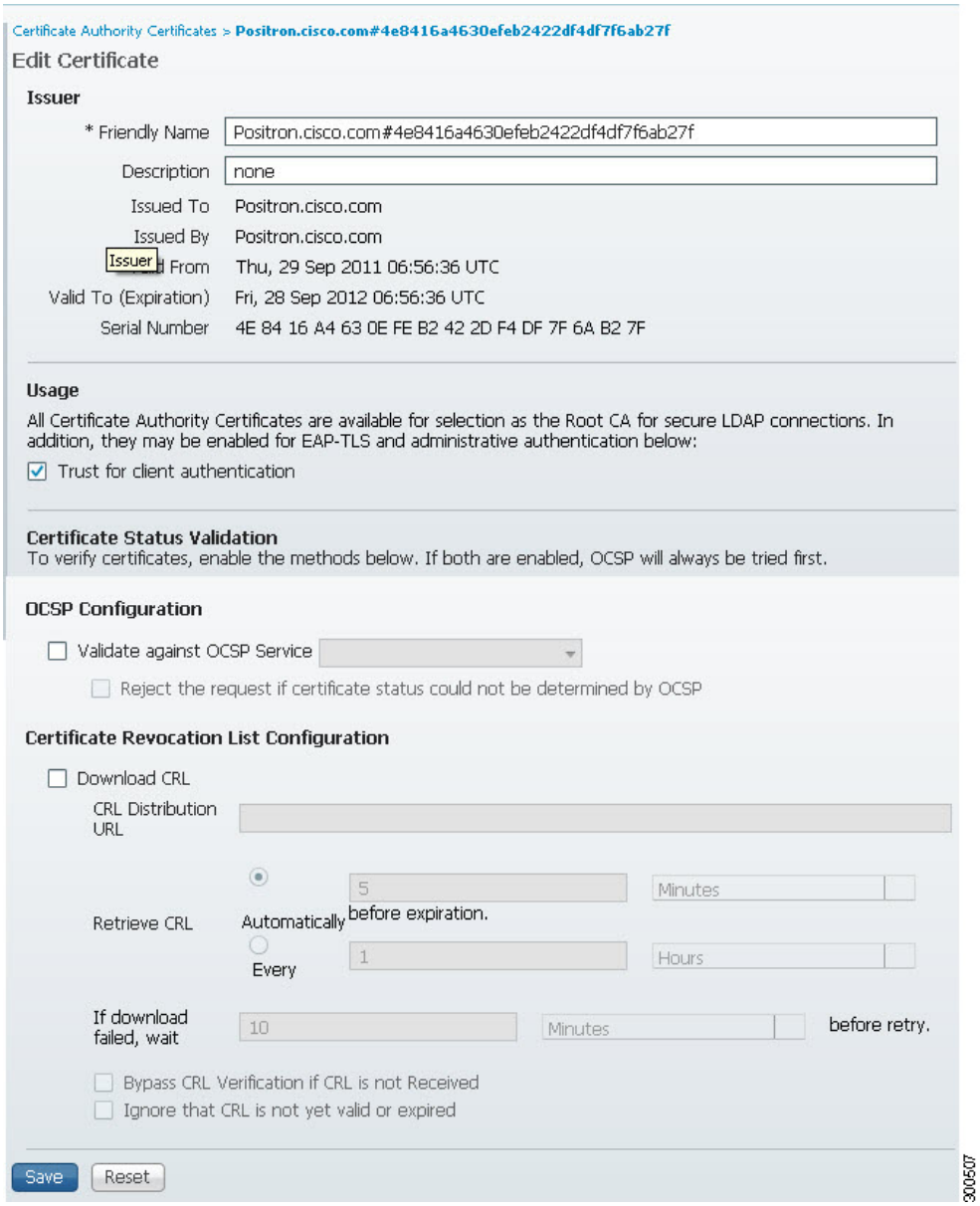
Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Authority Certificates**.

The Certificate Authority Certificates page appears.

Step 3 Check the check box next to the certificate that you want to edit and click **Edit**.

The page refreshes and the information for the certificate authority certificate is listed as shown in Figure 13-11.

Figure 13-11 Certificate Authority Certificate Edit Page



You can edit the following:

- Friendly Name
- Description
- Usage
- Certificate Revocation List Configuration

Step 4 Enter a friendly name to easily identify this certificate.

Step 5 Enter an optional description.

Step 6 Check the **Trust for client authentication** check box if you want to use this certificate in the trust list.

Note If you check both the **Trust for client authentication** and **Enable Validation of Certificate Extensions** options, ensure that the "keyUsage" extension is present and the "keyCertSign" bit is set, and that the basic constraints extension is present with the CA flag set to true.

Step 7 In the Certificate Status Validation area, check the following check boxes so that OCSP services are always tried first for certificate validation:

a. **Validate Against OCSP Service**

b. **Reject the request if certificate status could not be determined by OCSP**

See "OCSP Services" section on page 13-25 for more information on OCSP services.

Step 8 In the Certificate Revocation List Configuration area, do the following:

a. Check the **Download CRL** check box for the ISE to download a CRL.

b. Enter the URL to download the CRL from a CA in the URL Distribution text box. This field will be automatically populated if it is specified in the certificate authority certificate. The URL must begin with "http" or "https."

The CRL can be downloaded automatically or periodically.

c. You can configure the time interval between downloads in minutes, hours, days, or weeks if you want the CRL to be downloaded automatically before the previous CRL update expires.

d. Configure the time interval in minutes, hours, days, or weeks to wait before the ISE tries to download the CRL again.

e. If you uncheck the Bypass CRL Verification if CRL is not Received check box, all client requests that use certificates signed by the selected CA will be rejected until ISE receives the CRL file. If you check this check box, the client requests will be accepted before the CRL is received.

f. If you uncheck the Ignore CRL that is not yet valid or expired check box, ISE checks the CRL file for the start date in the Effective Date field and the expiration date in the Next Update field. If the CRL is not yet active or has expired, all authentications that use certificates signed by this CA are rejected. If you check this check box, ISE ignores the start date and expiration date and continues to use the not yet active or expired CRL and permits or rejects the EAP-TLS authentications based on the contents of the CRL.

Step 9 Click **Save** to save the changes you have made to the certificate authority certificate.

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on these commands.

Deleting a Certificate Authority Certificate

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete a certificate authority certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Authority Certificates**.

The Certificate Authority Certificates page appears.

Step 3 Check the check box next to the certificate that you want to delete and click **Delete**.

The following message appears.

Are you sure you want to delete?

Step 4 Click **OK** to delete the certificate authority certificate.

If client certificate-based authentication is enabled, then Cisco ISE will restart the application server on each node in your deployment, starting with the application server on the primary Administration node and followed, one-by-one, by each additional node.

Exporting a Certificate Authority Certificate

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To export a certificate authority certificate, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **Certificate Authority Certificates**.

The Certificate Authority Certificates page appears.

Step 3 Check the check box next to the certificate that you want to export and click **Export**.

Note You can export only one certificate at a time.

Step 4 Save the privacy-enhanced mail file to the file system that is running your client browser.

Importing Certificate Chains

You can import certificates from a file that contains a certificate chain. ISE supports the privacy-enhanced mail format for importing chains, where each privacy-enhanced-mail-encoded certificate is ordered with the root CA certificate appearing first to the last certificate (end entity) in the correct order. For example, if there are *n* certificates, then certificates 1 to *n* – 1 are assumed to be root or CA certificates that belong to the trust list, and the *n*th certificate is assumed to be an end entity certificate from the local certificate store. The associated private key file belongs to the *n*th (end entity) certificate. Ensure that this format and convention is strictly followed.

Importing the certificate chain is a two-step process:

- Import the certificate chain file to the certificate authority certificate list. See the "Adding a Certificate Authority Certificate" section on page 13-18 for information on how to import the certificate chain. Cisco ISE places all the certificates except the last one in the trusted certificate list.
- Import the certificate chain file to the local certificate store. See the "Importing a Server Certificate" section on page 13-5 for information on how to import the certificate chain. Cisco ISE places the last certificate (*n*th certificate) in the local certificate store.

Creating Certificate Trust Lists in the Primary ISE Node

In a distributed deployment, before registering a secondary node, you must populate the primary node's CTL with the appropriate CA certificates that can be used to validate the HTTPS certificate of the secondary node. The procedure to populate the CTL of the primary node is different for different scenarios:

- If the secondary node is using a CA-signed certificate for HTTPS communication, you can import the appropriate CA certificates into the CTL of the primary node. See "Importing Root and CA Certificates into the CTL of the Primary Node" section on page 13-23 for more information.
- If the secondary node is using a CA-signed certificate for HTTPS communication, you can alternatively import the CA-signed certificate of the secondary node into the CTL of the primary node, instead of relying on CA certificates for trust. See "Importing the CA-Signed Certificate from the Secondary Node into the Primary Node's CTL" section on page 13-24 for more information.
- If the secondary node is using a self-signed certificate for HTTPS communication, you can import the self-signed certificate of the secondary node into the CTL of the primary node. See "Importing the Self-Signed Certificate from the Secondary Node into the CTL of the Primary Node" section on page 13-24 for more information.

Note After registering your secondary node to the primary node, if you change the HTTPS certificate on the registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node's HTTPS certificate.

Importing Root and CA Certificates into the CTL of the Primary Node

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To import root and CA certificates into the CTL of the primary node, complete the following steps:

Step 1 You must obtain the appropriate CA certificates from the Certificate Authority that has signed the server certificate of the secondary node and import them into the CTL of the primary node. You do not have to obtain the root and all the intermediate CA certificates. You must obtain the CA certificate from the CA that directly signed the server certificate of the secondary node. You can optionally import additional higher-level signer CA certificates. For example, in a three-tier hierarchy, if the server certificate of the secondary node is signed by a CA and then by a Root CA, you must import the CA certificate of the CA that signed the server certificate of the secondary node and not the Root CA. The certificate validation software should be able to construct the path from the server certificate of the secondary node to the topmost signing certificate in the CA store.

Step 2 Log into the administrative user interface of your primary node, and import the appropriate CA certificates into the CTL of the primary node. See the "Adding a Certificate Authority Certificate" section on page 13-18 for more information. Repeat this process to add additional CA certificates, if required.

Importing the CA-Signed Certificate from the Secondary Node into the Primary Node's CTL

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To import the CA-signed certificate from the secondary node into the CTL of the primary node, complete the following steps:

Step 1 Log into the administrative user interface of the node that you are going to register as your secondary node, and export the CA-signed certificate that is used for HTTPS communication to the file system running your client browser. See the "Exporting a Certificate Authority Certificate" section on page 13-22 for more information.

Note In the Export dialog box, click the **Export Certificate Only** radio button.

Step 2 Log into the administrative user interface of your primary node, and import the CA-signed certificate of the secondary node into the CTL of the primary node. See the "Adding a Certificate Authority Certificate" section on page 13-18 for more information.

Importing the Self-Signed Certificate from the Secondary Node into the CTL of the Primary Node

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have the Super Admin or System Admin role assigned. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To import the self-signed certificate from the secondary node into the CTL of the primary node, complete the following steps:

Step 1 Log into the administrative user interface of the node that you are going to register as your secondary node and export the self-signed certificate that is used for HTTPS communication to the file system running your client browser. See the "Exporting a Local Certificate" section on page 13-13 for more information.

Note In the Export dialog box, click the **Export Certificate Only** radio button.

Step 2 Log into the administrative user interface of your primary node, and import the self-signed certificate of the secondary node into the CTL of the primary node. See the "Adding a Certificate Authority Certificate" section on page 13-18 for more information.

OCSP Services

The Online Certificate Status Protocol (OCSP) is a protocol that is used for checking the status of x.509 digital certificates. This protocol is an alternative to the CRL (Certificate Revocation List) and addresses issues that result in handling CRLs.

Cisco ISE has the capability to communicate with OCSP servers over HTTP to validate the status of certificates in authentications. The OCSP configuration is configured in a reusable configuration object that can be referenced from any certificate authority (CA) certificate that is configured in Cisco ISE. See Editing a Certificate Authority Certificate, page 13-19.

You can configure CRL and/or OCSP verification per CA. If both are selected, then Cisco ISE first performs verification over OCSP. If a communication problem is detected with both the primary and secondary OCSP servers, or if unknown status is returned for a given certificate, Cisco ISE will fail over to perform CRL checking.

This section contains the following topics:

- OCSP Certificate Status Values, page 13-25
- OCSP High Availability, page 13-26
- Viewing OCSP Services, page 13-27
- Adding, Editing, or Duplicating OCSP Services, page 13-27
- Deleting an OCSP Service, page 13-30
- OCSP Statistics Counters, page 13-30
- Monitoring OCSP, page 13-31

OCSP Certificate Status Values

OCSP services return the following values for a given certificate request:

- Good—Indicates a positive response to the status inquiry. It means that the certificate is not revoked, and the state is good only until the next time interval (time to live) value.

- Revoked—The certificate was revoked.
- Unknown—The certificate status is unknown. This can happen if the OCSP is not configured to handle the given certificate CA.
- Error—No response was received for the OCSP request.

Related Topics

OCSP Statistics Counters, page 13-30

OCSP High Availability

Cisco ISE has the capability to configure up to two OCSP servers per CA, called primary and secondary OCSP servers. Each OCSP server configuration contains the following parameters:

- URL—The OCSP server URL.
- Nonce—A random number that is sent in the request. This option ensures that old communications cannot be reused in reply attacks.
- Validate Response—ISE validates the response signature that is received from the OCSP server.

In case of timeout (5 seconds), when ISE communicates with the primary OCSP server, it falls over to the secondary OCSP server.

ISE uses the secondary OCSP server for a configurable amount of time before attempting to use the primary server again.

OCSP Failures

The three general OCSP failure scenarios are as follows:

1. Failed OCSP cache or OCSP client side (ISE) failures
2. Failed OCSP responder scenarios, for example:
   a. The first primary OCSP responder not responding, and the secondary OCSP responder responding to the ISE OCSP request.
   b. Errors, responses not received from ISE OCSP requests.

An OCSP responder may not provide a response to the ISE OCSP request or it may return an OCSP Response Status as “not successful.” OCSP Response Status values can be as follows:

- tryLater
- signRequired
- unauthorized
- internalError
- malformedRequest

There are many date-time checks, signature validity checks and so on, on the OCSP request. For more details, refer to *RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* which describes all the possible states, including the error states.

3. Failed OCSP reports

Viewing OCSP Services

To view OCSP services, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

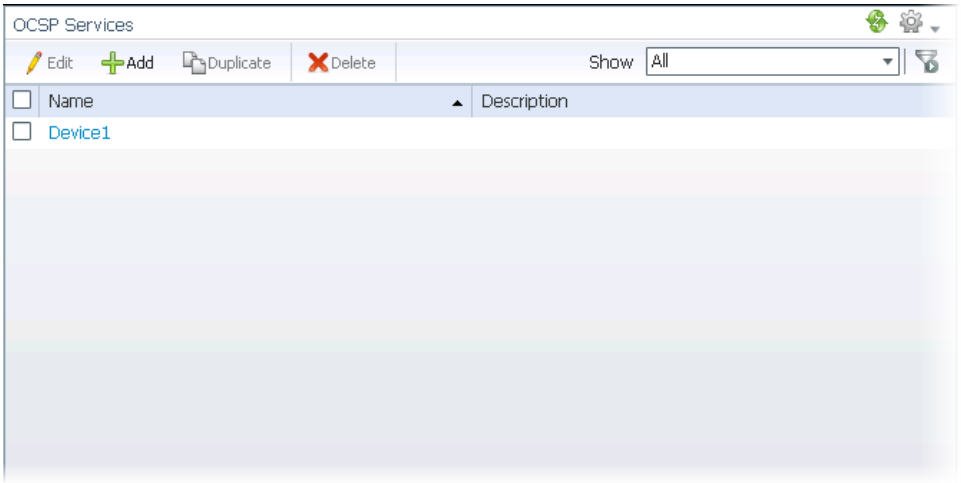
Step 2 From the Certificate Operations navigation pane on the left, click **OCSP Services**.

The OCSP Service List page appears, as shown in Figure 13-12.

Step 3 The OCSP Service List page displays the following information for the configured OCSP service:

- Name
- Description

Figure 13-12 OCSP Service List Page



Adding, Editing, or Duplicating OCSP Services

To add or edit OCSP services, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **OCSP Services**.

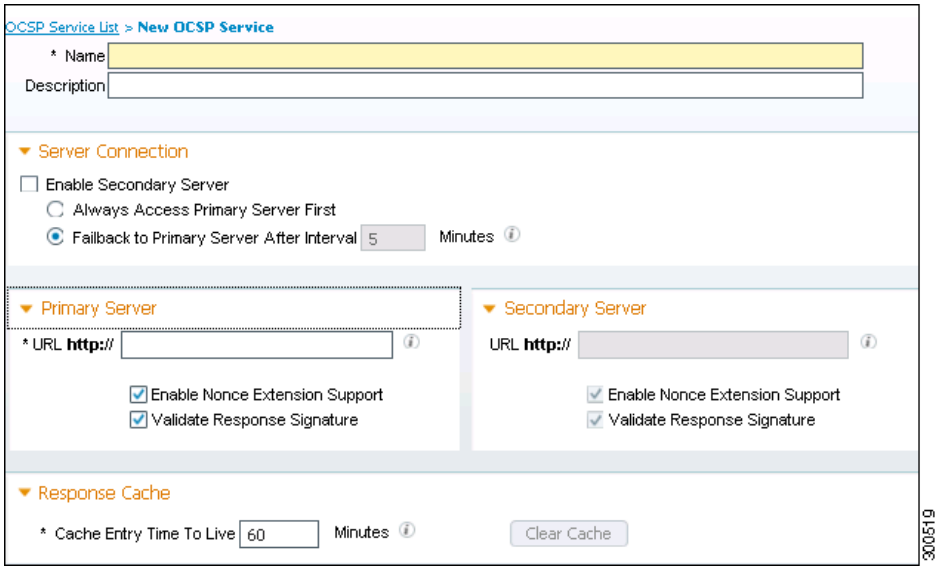
The OCSP Service List page appears. See Figure 13-12.

Step 3 Click one of the following:

- **Add**
- **Edit**
- **Duplicate**

The New OCSP Service page appears. See Figure 13-13.

Figure 13-13 OCSP Services Add or Edit Page



Step 4 Provide the following information for the OCSP service:

- Name
- Description

Step 5 Check the **Enable Secondary Server** check box if you want to enable high availability.

Step 6 Select one of the following options for high availability:

- Always Access Primary Server First —Use this option to check the primary server before trying to move to the secondary server. Even if the primary was checked earlier and found to be unresponsive, ISE will try to send a request to the primary server before moving to the secondary server.
- Fallback to Primary Server After Interval—Use this option when you want ISE to move to the secondary server and then fall back to the primary server again. In this case, all other requests are skipped, and the secondary server is used for the amount of time that is configured in the text box. The allowed time range is 1-999 minutes.

Step 7 Provide the URLs or IP addresses of the primary and secondary OCSP servers.

Step 8 Check or uncheck the following options:

- Nonce—You can configure a nonce to be sent as part of the OCSP request. This includes a pseudo-random number in the OCSP request. It is verified that the number that is received in the response is the same as the number that is included in the request. This option ensures that old communications cannot be reused in replay attacks.
- Validate Response Signature—The OCSP responder signs the response with one of the following signatures:
  - The CA certificate
  - A different certificate from the CA certificate

  In order for ISE to validate the response signature, the OCSP responder needs to send the response along with the certificate, otherwise the response verification fails, and the status of the certificate cannot be relied on. According to the RFC, OCSP can sign the response using different certificates.

This is true as long as OCSP sends the certificate that signed the response for ISE to validate it. If OCSP signs the response with a different certificate which is not configured in ISE, the response verification will fail.

Step 9 Provide the number of minutes for the Cache Entry Time to Live.

Each response from the OCSP server holds a "nextUpdate" value. This value shows when the status of this certificate will be updated next on the server. When the OCSP response is cached, the two values (one from the configuration and another from response) are compared, and the response is cached for the period of time that is the lowest value of these two. If the "nextUpdate" value is 0, the response is not cached at all.

Cisco ISE will cache OCSP responses for the configured time. The cache is not replicated nor persistent, thus when ISE restarts the cache is cleared.

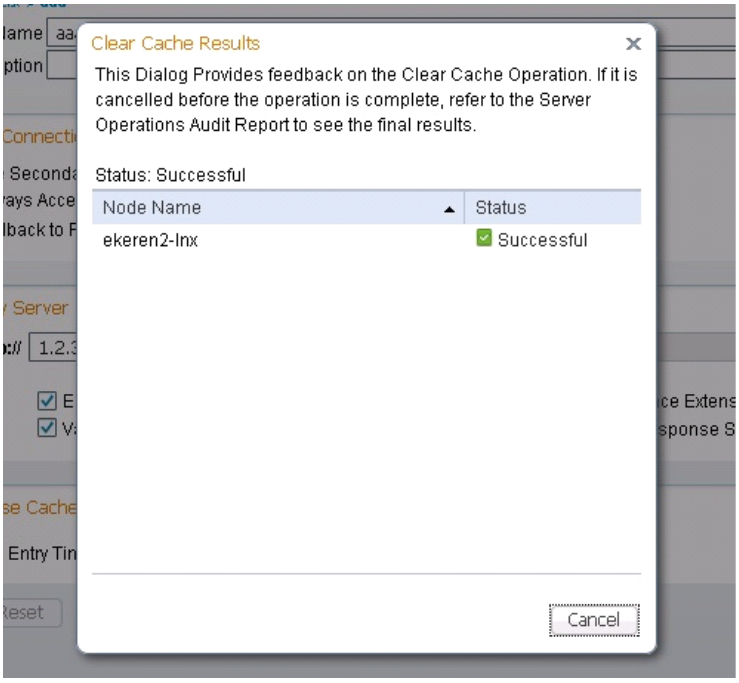
The OCSP cache is used in order to maintain the OCSP responses, for the following reasons:

- To reduce network traffic and load from the OCSP servers on an already known certificate
- To increase the performance of Cisco ISE by caching already known certificate statuses

Step 10 Click **Clear Cache** to clear entries of all the certificate authorities that are connected to the OCSP service.

In a deployment, Clear Cache interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment. Figure 13-14 shows the Clear Cache Status Message dialog box.

Figure 13-14 Clear Cache Status Message



Deleting an OCSP Service

To delete an OCSP service, complete the following steps:

Step 1 Choose **Administration > System > Certificates**.

Step 2 From the Certificate Operations navigation pane on the left, click **OCSP Services**.

The OCSP Service List page appears.

Step 3 Check the check box next to the OCSP service that you want to delete, and click **Delete**.

The following message appears: Are you sure you want to delete?

Step 4 Click **OK** to delete the OCSP service.

OCSP Statistics Counters

The OCSP counters are used for logging and monitoring the data and health of the OCSP servers. Logging occurs every five minutes. A syslog message is sent to the Cisco ISE Monitoring node and is preserved in the local store, which contains the data for the previous five minutes. After the message is sent, the counters are recalculated for the next interval. This means, after five minutes, a new five minute window interval starts again.

Table 13-1 lists the OCSP syslog messages and their descriptions.

Table 13-1 OCSP Syslog Messages

Attribute Name	Attribute Description
OCSPPrimaryNotResponsiveCount	The number of nonresponsive primary requests
OCSPSecondaryNotResponsiveCount	The number of nonresponsive secondary requests
OCSPPrimaryCertsGoodCount	The number of ‘good’ certificates that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsGoodCount	The number of ‘good’ statuses that are returned for a given CA using the primary OCSP server
OCSPPrimaryCertsRevokedCount	The number of ‘revoked’ statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsRevokedCount	The number of ‘revoked’ statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsUnknownCount	The number of ‘Unknown’ statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsUnknownCount	The number of ‘Unknown’ statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsFoundCount	The number of certificates that were found in cache from a primary origin
OCSPSecondaryCertsFoundCount	The number of certificates that were found in cache from a secondary origin

Table 13-1 OCSP Syslog Messages

Attribute Name	Attribute Description
ClearCacheInvokedCount	How many times clear cache was triggered since the interval
OCSPCertsCleanedUpCount	How many cached entries were cleaned since the t interval
NumOfCertsFoundInCache	Number of the fulfilled requests from the cache
OCSPCacheCertsCount	Number of certificates that were found in the OCSP cache

Monitoring OCSP

You can view the OCSP services data in the form of an OCSP Monitoring Report. The OCSP services data is stored in ocsp_notice database table.

This section describes the process of running this report. For more information on Cisco ISE reports, see Chapter 24, "Reporting."

OCSP Monitoring Report

To view OCSP services data, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Server Instance**.

Step 3 In the Reports panel on the right, click the **OCSP Monitoring** radio button.

Step 4 From the **Run** drop-down menu, choose a time period over which the report data will be collected:

- Last 30 minutes
- Last hour
- Last 12 hours
- Today
- Yesterday
- Last 7 days
- Last 30 days
- Query and run—Use this to get data of more than last 30 days.

The report runs upon choosing the time period, and the **Server Instance > OCSP Monitoring report** data appears.



CHAPTER 14

Logging

This chapter describes the logging mechanism implemented in the Cisco Identity Services Engine (ISE), including steps to configure logging targets, edit logging categories, and configuring logging settings. The following topics are covered:

- Understanding Logging, page 14-1
- Configuring Local Log Settings, page 14-2
- Understanding Remote Logging Targets, page 14-2
- Understanding Logging Categories, page 14-5
- Viewing Message Catalog, page 14-8
- Understanding Debug Log Configuration, page 14-8
- Viewing Log Collection Status, page 14-11

Understanding Logging

The Cisco ISE provides a logging mechanism that is used for auditing, fault management, and troubleshooting of the services provided by Cisco ISE. The logging mechanism helps you to identify fault conditions in deployed services and troubleshoot issues efficiently. It also produces logging output from the monitoring and troubleshooting primary node in a consistent fashion.

You can configure your Cisco ISE node to collect the logs in the local systems using a virtual loopback address. To collect logs externally, you configure external syslog servers, called targets. Logs are classified into various predefined categories, which are discussed in Understanding Logging Categories. You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

In the ISE administration interface, navigate to **Administration > System > Logging** to perform the following logging related tasks:

- To configure local log settings, see Configuring Local Log Settings, page 14-2
- To understand and create remote logging targets, see Understanding Remote Logging Targets, page 14-2
- To understand and edit logging categories, see Understanding Logging Categories, page 14-5
- To view message catalog, see Viewing Message Catalog, page 14-8
- To understand and configure debug logs, see Understanding Debug Log Configuration, page 14-8
- To view log collection status, see Viewing Log Collection Status, page 14-11

Configuring Local Log Settings

Use this process to set the local log storage period and to delete the local logs.

To configure the logging settings, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Local Log Settings**.

Step 2 Configure the following fields:

a. Local Log Storage Period—The maximum number of days to keep the log entries in the configuration source.

Note To avoid wasting disk space, logs can be deleted during the specified local log storage period. Click the **Delete Logs Now** button to delete the existing log files at any time before the expiration of the storage period.

Step 3 Click **Save**.

Understanding Remote Logging Targets

Logging targets are locations where the system logs are collected. In Cisco ISE, targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can FTP them to an external server. Cisco ISE has the following default targets, which are dynamically configured in the loopback addresses of the local system:

- LogCollector—Default syslog target for the Log Collector.
- ProfilerRadiusProbe—Default syslog target for the Profiler Radius Probe.

Configuring Remote Logging Targets

You can use the default logging targets that are configured locally at the end of the ISE installation or you can create external targets which store the logs.

This section contains the following topics:

- Viewing Remote Logging Targets, page 14-3
- Creating Remote Logging Targets, page 14-4
- Editing Remote Logging Targets, page 14-4
- Deleting Remote Logging Targets, page 14-5

Viewing Remote Logging Targets

You can view the predefined and user-defined remote logging targets. You can also search for a particular target using the filter.

To view remote logging targets, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Remote Logging Targets**.

The Remote Logging Targets page appears with a list of existing logging targets.

Step 2 Click Filter and choose one of the following options:

- Quick Filter
- Advanced Filter

To perform a quick filter, enter search criteria in one or more of the following attribute fields:

- Name
- IP Address
- Type
- Description

To perform an Advance filter, create a matching rule by performing the following:

- In the Filter drop-down list, select one of the following options:
  - Name
  - IP Address
  - Type
  - Description
- In the second drop-down list, select one of the following options:
  - Contains
  - Does not contain
  - Does not equal
  - Ends with
  - Is empty
  - Is exactly (or equals)
  - Is not empty
  - Starts with
- In the text box, enter your desired search value.
- Click Go to launch the filter process, or click plus (+) to add additional search criteria.
- Click Clear Filter to reset the filter process.

The desired remote logging targets are displayed.

Creating Remote Logging Targets

To create an external logging target, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Remote Logging Targets**.

The Remote Logging Targets page appears.

Click **Add**.

Step 2 The Log Collector page appears.

Step 3 Configure the following fields:

a. Name—Enter the name of the new target.

b. Target Type—By default it is set to Syslog. The value of this field cannot be changed.

c. Description— Enter a brief description of the new target.

d. IP Address—Enter the IP address of the destination machine where you want to store the logs.

e. Port—Enter the port number of the destination machine.

f. Facility Code—Choose the syslog facility code to be used for logging. Valid options are Local0 through Local7.

g. Maximum Length— Enter the maximum length of the remote log target messages. Valid options are from 200 to 1024 bytes.

Step 4 Click **Save**.

Step 5 Go to the Logging Targets page and verify the creation of the new target.

Editing Remote Logging Targets

To edit a remote logging target, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Remote Logging Targets**.

The Remote Logging Target page appears.

Click the radio button next to the logging target name that you want to edit and click **Edit**.

The Log Collector page appears.

Step 2 Modify the following field values as necessary:

- Name
- Target Type
- Description
- IP Address
- Port
- Facility Code
- Maximum Length

Step 3 Click **Save**.

The updating of the selected Log Collector is completed.

Deleting Remote Logging Targets

To edit a remote logging target, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Remote Logging Targets**.

The Log Collector page appears.

Step 2 Click the radio button next to the logging target that you want to delete and click **Delete**.

Step 3 Click **OK** in the confirmation dialog box to confirm that you want to delete the logging target.

Understanding Logging Categories

A logging category is a bundle of message codes that describe a function, a flow, or a use case. In Cisco ISE, each log is associated with a message code that is bundled with the logging categories according to the log message content. Logging categories help describe the content of the messages that they contain.

Logging categories promote logging configuration. Each category has a name, target, and severity level that you can set, as per your application requirement.

Cisco ISE provides predefined logging categories for services, such as Posture, Profiler, Guest, AAA (authentication, authorization, and accounting), and so on, to which you can assign log targets.

Table 14-1 lists the Cisco ISE predefined categories that are available in Cisco ISE by default:

Table 14-1 Logging Categories

Parent Category	Category
AAA Audit	• AAA Audit • Failed Attempts • Passed Authentication
AAA Diagnostics	• AAA Diagnostics • Administrator Authentication and Authorization • Authentication Flow Diagnostics • Identity Store Diagnostics • Policy Diagnostics • Radius Diagnostics • Guest
Accounting	• Accounting • Radius Accounting

Table 14-1 Logging Categories (continued)

Parent Category	Category
Administrative and Operational Audit	• Administrative and Operational Audit
Posture and Client Provisioning Audit	• Posture and Client Provisioning Audit
Posture and Client Provisioning Diagnostics	• Posture and Client Provisioning Diagnostics
Profiler	• Profiler
System Diagnostics	• System Diagnostics • Distributed Management • Internal Operations Diagnostics
System Statistics	• System Statistics

See Available Reports, page 24-42 for more information on the relevant troubleshooting reports per category.

This section contains the following topics:

- Searching Logging Categories, page 14-6
- Editing Logging Categories, page 14-7

Searching Logging Categories

You can use Filter to search for a particular category.

To search a category, complete the following steps:

Step 1 From the ISE Administration Interface, choose **Administration > System > Logging > Logging Categories**.

The Logging Categories page appears with a list of existing categories.

Step 2 Click Filter and choose one of the following options:

- Quick Filter
- Advanced Filter

To perform a quick filter, enter search criteria in one or more of the following attribute fields:

- Parent Category
- Category
- Targets
- Severity
- Local Log Level

To perform an Advance filter, create a matching rule by performing the following:

- In the Filter drop-down list, select one of the following options:
  - Parent Category
  - Category

- Targets
- Severity
- Local Log Level

• In the second drop-down list, select one of the following options:

- Contains
- Does not contain
- Does not equal
- Ends with
- Is empty
- Is exactly (or equals)
- Is not empty
- Starts with

• In the text box, enter your desired search value.
• Click Go to launch the filter process, or click plus (+) to add additional search criteria.
• Click Clear Filter to reset the filter process.

The desired remote logging categories are displayed.

Editing Logging Categories

This section shows you how to set the log severity level and choose logging targets where the logs of selected categories will be stored.

To edit the configuration of a specific logging category, complete the following steps:

Step 1 From the Cisco ISE Administration Interface, choose **Administration > System > Logging > Logging Categories**.

The Logging Categories page appears with a list of existing categories.

Step 2 Click the radio button next to the category that you want to edit and click **Edit**.

The edit page appears, showing the details of the selected category.

Step 3 Modify the following field values:

Note The Name field cannot be changed.

a. Log Severity Level— For diagnostic logging categories, use the drop-down list box to select the severity level. Valid options are:

- FATAL—Emergency. This option means that Cisco ISE cannot be used and you must take action immediately.
- ERROR—This option indicates a critical or error condition.
- WARN—This option indicates a normal but significant condition. This is the default condition.
- INFO—This option indicates an informational message.

  - DEBUG—This option indicates a diagnostic bug message.

b. Target—This section contains two boxes: Available and Selected. The Available box contains the existing logging targets, both local (predefined) and external (user-defined). The Selected box, which is initially empty, contains the selected targets for the specific category. You can change the targets for a category by transferring the targets between the Available and the Selected boxes using the left and right icons.

Step 4 Click **Save**.

Step 5 Go to the Logging Categories page and verify the configuration changes that were made to the specific category.

Viewing Message Catalog

You can use the Message Catalog page to view all possible log messages.

To view the message catalog, complete the following steps:

Step 1 Choose **Administration > System > Logging > Message Catalog**.

The Log Message Catalog page appears, from which you can view all possible log messages that can appear in your log files. The data available in this page are for display only.

Each message contains the following fields:

- Category Name—The logging category to which a message belongs
- Message Class—The group to which a message belongs
- Message Code—A unique message code identification number associated with a message
- Message Text—Name of the message
- Severity—The severity level associated with a message

Understanding Debug Log Configuration

Debug logs capture bootstrap, application configuration, runtime, deployment, monitoring and reporting, and public key infrastructure (PKI) information.

Use this process to configure the log severity level for individual components, and store the debug logs in the local server so that you can export to Cisco technical support for evaluation and troubleshooting.

Note The debug log configuration is not saved upon backup and restore operation and this configuration is not saved upon upgrade.

Configuring Debug Log Level

To configure debug logs via the Cisco ISE user interface, complete the following steps:

Step 1 Choose **Administration > System > Logging > Debug Log Configuration**. The Node List page appears, which contains a list of nodes and their personas.

Note You can use the Filter button to search for a specific node, particularly if the node list is large.

Step 2 Select the node and click **Edit**.

The Debug Level Configuration page appears, which contains a list of components that is based on the services that are running in the selected node and the current log level that is set for individual components.

Each node contains the following components:

- Active Directory
- CacheTracker
- NotificationTracker
- ReplicationTracker
- cisco-mnt
- client
- com-cisco-nm
- cpm-clustering
- cpm-mnt
- epm-pap
- epm-pap-api.services
- epm-pdp
- epm-pip
- guest
- guestadmin
- guestauth
- guestportal
- identity-store-AD
- mnt-alert
- mnt-collector
- org-apache
- org-apache-cxf
- org-apache-digester
- org-displaytag
- pep-auth-manager-test

- posture
- profiler
- provisioning
- prrt-JNI
- runtime-AAA
- runtime-config
- runtime-logging
- sponsorportal
- swiss

Note You can use the Filter button to search for a specific component from the list.

Step 3 Do one of the following to adjust the log severity level:

- Click on a component name, choose the desired log level from the combo box, and click **Save**.

  Valid options are:

  - FATAL—Emergency. This option means that Cisco ISE cannot be used and you must take action immediately.
  - ERROR—This option indicates a critical or error condition.
  - WARN—This option indicates a normal but significant condition. This is the default condition.
  - INFO—This option indicates an informational message.
  - DEBUG—This option indicates a diagnostic bug message.

- Choose a component name for which you want to configure the debug log level, and click **Edit**. In this page, choose the desired log level from the Log Level combo box, and click **Save**.

Note Changing the log severity level of *runtime-AAA* component changes the log level of its subcomponent *prrt-JNI* as well. A change in subcomponent log level does not affect its parent component.

The debug log configuration for the selected component is complete.

Related Topics

- Downloading Support Bundles, page 23-40
- Downloading Debug Logs, page 23-43

Viewing Log Collection Status

You can obtain reports on the log collection status for all Cisco ISE nodes. In the Cisco ISE administration interface, choose **Operations > System > Reports > Log Collection Status**. The Log Collection status page appears, which contains the following information:

- ISE Server: Name of the Cisco ISE node in which logs are collected
- Last Syslog Message: Arrival time of the most recent syslog message
- Last Error: Name of the most recent error message
- Last Error Time: Arrival time of the most recent error message

See System Reports, page 24-11, for information on how to generate the report on log collection status.

Viewing Log Collection Details

You can view server log details such as last syslog message, log configuration changes made, server errors, and so on using the Log Collection Details page. In the Cisco ISE administration interface, choose **Operations > System > Reports > Log Collection Status**. The Log Collection status page appears. Select a node to view the Log Collection Details page, which contains the following information pertaining to the selected node:

- Log Name: Name of the log category under which the logs are collected
- Last Syslog Message: Arrival time of the most recent syslog message
- Last Error: Name of the most recent error message
- Last Error Time: Arrival time of the most recent error message

See System Reports, page 24-11 for information on how to generate the report on log collection status.



CHAPTER 15

Managing Cisco ISE Backup and Restore Operations

This chapter describes the Cisco Identity Services Engine (ISE) database backup and restore operations, which include Cisco ISE application configuration and Cisco Application Deployment Engine operating system (ADE operating system) configuration. This chapter does not cover the Monitoring and Troubleshooting database backup and restore procedures. For information on the Monitoring and Troubleshooting database backup and restore, see Chapter 23, "Monitoring and Troubleshooting."

Note Backup and restore is not available for Inline Posture nodes in Cisco ISE, Release 1.1. For more information on this and other known issues, see the *Release Notes for the Cisco Identity Services Engine, Release 1.1.*

This chapter contains the following sections:

- Overview of Cisco ISE Backup and Restore, page 15-1
- Supported Scenarios for Backup, Restore, and Upgrade, page 15-2
- Configuring Repositories, page 15-3
- On-Demand Backup, page 15-5
- Scheduled Backups, page 15-6
- Viewing Backup History, page 15-10
- Restoring Data from a Backup, page 15-11
- Viewing Restore History, page 15-12
- Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 15-12
- Recovering Lost Nodes in Standalone and Distributed Deployments, page 15-13

Overview of Cisco ISE Backup and Restore

Cisco ISE allows you to back up data only from the primary or standalone Administration ISE node. Backup can be done either from the Cisco ISE command-line interface (CLI) or Cisco ISE user interface. The restore operation can only be done through the CLI.

Cisco ISE allows you to back up the following data:

- Application-specific configuration data—Contains only Cisco ISE configuration data from the Cisco ISE database
- Application and ADE operating system data—Contains both application-specific and Cisco ADE operating system configuration data

Backup and restore operation can be performed with the backup files of the previous versions of the Cisco ISE and restored on a later version. For example, if you have a backup that is taken from an ISE node (Cisco ISE, Release 1.0) before an upgrade, you can restore it on Cisco ISE, Release 1.1.

Cisco ISE allows you to restore Cisco ISE application and ADE operating system data on a primary or standalone administration node. After you restore data on the primary administration node, the changes are replicated to the secondary nodes in your deployment.

If you obtain the backup from your primary Administration ISE node in one timezone and try to restore it on another ISE node in another timezone, the restore process might fail. This failure happens if the timestamp in the backup file is later than the system time on the ISE node on which the backup is restored. If you restore the same backup a day after it was obtained, then the timestamp in the backup file is in the past and the restore process succeeds.

Note We recommend that you do not change the system timezone after the initial ISE installation and setup.

Note After you obtain the backup from your standalone ISE node or primary Administration ISE node, if you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data. Otherwise, if you try to restore data using the older backup, the communication between the nodes might fail.

Typically, you would need the application-specific backup to be scheduled more frequently, and the whole system backup infrequently. The whole system backup is required in case of a hardware failure that requires you to reimage your hardware.

You need a data repository, which is the location where Cisco ISE saves your backup file. You must create a repository before you can run an on-demand or scheduled backup.

Note If you have a standalone administration node that fails, then you need to run the full system backup to restore it. If your primary Administration ISE node fails, you can use the distributed setup to promote your secondary Administration ISE node to become the primary, and restore data on your primary Administration ISE node after it comes up.

You can perform a backup either through the CLI or through the Cisco ISE user interface.

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on the CLI backup commands.

Note Cisco ISE also provides another CLI command, **backup-logs**, that you can use to collect log and configuration files for troubleshooting purposes. For more information, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

Supported Scenarios for Backup, Restore, and Upgrade

For details on supported approaches to a previous backup on a newer build and upgrade scenarios, refer to the “Upgrading Cisco ISE” chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release1.1*.

Configuring Repositories

Cisco ISE allows you to create and delete repositories through the Cisco ISE user interface. You can use these repositories for various operations such as backup, restore, and so on. You can create the following types of repositories:

- DISK
- FTP
- SFTP
- TFTP
- NFS
- CDROM
- HTTP
- HTTPS

The Repositories page allows you to manage repositories from the Cisco ISE administrative user interface. You can create, and delete repositories through the administrative user interface.

Note Repositories are local to each device.

Note We recommend that you have a repository size of 10 GB for small deployments (100 endpoints or less), 100 GB for medium deployments, and 200 GB for large deployments.

This section contains the following topics:

- Creating Repositories
- Deleting Repositories

Creating Repositories

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create a repository, complete the following steps:

Step 1 Choose **Administration > System > Maintenance**.

Step 2 From the Operations navigation pane on the left, click **Repository**.

The Repository List page appears with a list of configured repositories. This page will be blank when you create repositories for the first time.

Step 3 Click **Add** to add a new repository.

The Repository Configuration page appears.

Step 4 Enter the values as described:

- Repository—(Required) Name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.

Note You cannot edit the name of a repository.

- Protocol—(Required) From the drop-down list box, choose one of the protocols.
- Path—(Required) Enter the path to your repository in this field. This value must start with a forward slash (/).

  The path must be valid and must exist at the time you create the repository. The following three fields are required depending on the protocol that you have chosen.

  - ServerName—(Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IPv4 address of the server where you want to create the repository.
  - Username—(Required for FTP, SFTP, and NFS) Enter the username that has write permission to the specified server. Only alphanumeric characters are allowed.
  - Password—(Required for FTP, SFTP, and NFS) Enter the password that will be used to access the specified server. Passwords can consist of the following characters: 0 through 9, a through z, A through Z, -, ., |, @, #,$, %, ^, &, *, (,), +, and =.

Step 5 Click **Submit** to create the repository.

A message similar to the following one appears:

Repository is created successfully.

Step 6 Click **Repository** from the Operations navigation pane on the left or click the **Repository List** link at the top of this page to go to the repository listing page.

Next Steps:

1. Ensure that the repository that you created is working by executing the following command from the Cisco ISE command line interface:

   show repository *repository_name*

   where *repository_name* is the name of the repository that you have created. For more information, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.*

Note If the path that you provided while creating the repository does not exist, then you will get the following error: %Invalid Directory.

2. Run an on-demand backup or schedule a backup. See Running On-Demand Backup and Scheduling a Backup for more information.

Deleting Repositories

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete a repository, complete the following steps:

Step 1 Choose **Administration > System > Maintenance**.

Step 2 From the Operations navigation pane on the left, click **Repository**.

The repositories listing page appears.

Step 3 Click the radio button next to the repository that you want to delete, then click **Delete**.

Cisco ISE prompts you with the following message:

Are you sure you want to delete this repository?

Step 4 Click **OK** to delete the repository.

The following message appears:

Repository was deleted successfully.

The Repository List page appears and the repository that you deleted will no longer be listed in this page.

On-Demand Backup

Cisco ISE provides an option to obtain an on-demand backup of the primary administration node. You can obtain a backup of the Cisco ISE application-specific configuration data, or application and Cisco ADE operating system data.

Running On-Demand Backup

Prerequisites:

1. Before you perform this task, you should have a basic understanding of the Backup and Restore operations in Cisco ISE.
2. Ensure that you have configured repositories. See the "Configuring Repositories" section on page 15 -3 for more information.
3. Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Note For backup and restore operations, you cannot choose the CDROM, HTTP, or HTTPS options because these are read-only repositories.

To perform an on-demand backup, complete the following steps:

Step 1 Choose **Administration > System > Maintenance**.

Step 2 From the Operations navigation pane on the left, choose **Data Management > Administration Node > Full Backup On Demand**.

The Backup On Demand page appears.

Step 3 Enter the name of your backup file.

Step 4 Select the repository where your backup file should be saved.

You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.

Step 5 Check the **Application-Only Backup, Excludes OS System Data** check box to obtain a Cisco ISE application data backup. Uncheck this check box if you want the Cisco ADE operating system data as well.

Step 6 Enter the **Encryption Key**. This key is used to encrypt and decrypt the backup file.

Step 7 Click **Backup Now** to run your backup.

Note In a distributed deployment, do not change the role of a node or promote a node when the backup is running. Changing node roles will shut down all the processes and might cause some inconsistency in data if backup is running concurrently. Wait for the backup to complete before you make any node role changes.

Step 8 Your screen will be refreshed and the following message will appear in the lower right corner of your screen, if you are viewing the Backup On Demand page:

Backup is done successfully.

If you have moved to other pages in the Cisco ISE user interface, to check the status of your backup, you must go to the Backup History page. See the "Viewing Backup History" section on page 15 -10 for more information.

Cisco ISE appends the backup filename with the timestamp and stores this file in the specified repository. Check if your backup file exists in the repository that you have specified.

For more information:

This procedure backs up your Cisco ISE application and Cisco ADE operating system data. To back up Monitoring and Troubleshooting database data, see the "Backing Up and Restoring the Monitoring Database" section on page 23 -45. You can also schedule backup jobs that runs periodically. See the "Scheduled Backups" section on page 15 -6 for more information.

Scheduled Backups

Cisco ISE allows you to schedule your system-level backup operations. You can schedule a backup to be run periodically (daily, weekly, monthly), and specify the time of the day when the backup should be run. Backup operations usually take some amount of time and the scheduling option allows you to configure backups at a convenient time. The Scheduled Backup page lists the backups that you have scheduled.

You can schedule a backup from the Cisco ISE CLI or through the Cisco ISE user interface. To schedule a job from the CLI, you must use the **kron** CLI command.

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1* for more information on the **kron** command.

An example is given below:

```
ise/admin(config)# kron policy-list policylistname
ise/admin(config-Policy List)# cli backup backupfilename repository repositoryname
application ise
ise/admin(config-Policy List)# kron occurrence backup_occur_backupfilename
ise/admin(config-Occurrence)# at 10:00 Sunday
ise/admin(config-Occurrence)# recurring
ise/admin(config-Occurrence)# policy-list policylistname
ise/admin(config-Occurrence)# exit
ise/admin(config)# exit
ise/admin#
```

To create a kron job, you must define a policy list. This policy list will also be created when you schedule a backup through the Cisco ISE user interface.

Note If you promote your secondary Administration ISE node to become the primary Administration ISE node, you must reconfigure your scheduled backups on the new primary Administration ISE node because scheduled backup configurations are not replicated from the primary to secondary Administration ISE nodes.

Note After you upgrade from Cisco ISE Release 1.0.3.377 or Cisco ISE Maintenance Release 1.0.4.573 to Cisco ISE, Release 1.1, the scheduled backup jobs need to be recreated, as the older jobs will not work properly.

Scheduling a Backup

Prerequisites:

1. Before you perform this task, you should have a basic understanding of the Backup and Restore, On-Demand Backup, and Scheduled Backups operations in Cisco ISE.
2. Ensure that you have configured repositories. See the "Configuring Repositories" section on page 15 -3 for more information.
3. Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Note For backup and restore operations, you cannot choose the CDROM, HTTP, or HTTPS options because these are read-only repositories.

To schedule a backup from the Cisco ISE user interface, complete the following steps:

Step 1 Choose **Administration > System > Maintenance**.

Step 2 From the Operations navigation pane on the left, choose **Data Management > Administration Node > Scheduled Backup**.

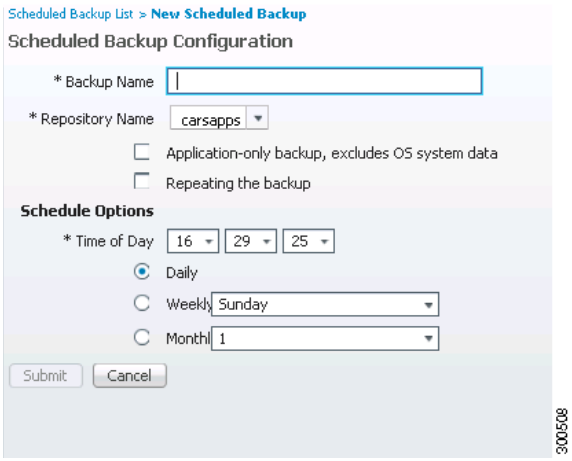
The Scheduled Backup List page appears. This page provides the following information:

- Name—Name of the scheduled backup job.
- Type—The frequency of recurrence, whether it is daily, weekly, or monthly.
- Time:Date—The time at which the backup will be run, the day of the week if the schedule is weekly, and the date if the schedule is monthly.
- Policy—Name of the policy list.
- Recurring—Indicates whether the backup should be repeated at the specified date and time or just performed once.

Step 3 Click **Add** to add a scheduled backup.

The Scheduled Backup Configuration page appears as shown in Figure 15-1.

Figure 15-1 Scheduled Backup: Create Page



Step 4 Enter a name for your backup file.

You can enter a descriptive name of your choice. Cisco ISE appends the timestamp to the backup filename and stores it in the repository. You will have unique backup filenames even if you configure a series of backups.

Note On the Scheduled Backup list page, the backup filename will be prepended with "backup_occur" to indicate that the file is a **kron** occurrence job.

Step 5 Select a repository from the Repository Name drop-down list box.

You cannot enter a repository name. You have to create a repository from the Cisco ISE user interface or through the Cisco ISE CLI. See the "Configuring Repositories" section on page 15 -3 for information on how to create repositories. Ensure that you create a repository before you schedule a backup job.

Step 6 Check the **Application-Only Backup, Excludes OS System Data** check box to back up only the Cisco ISE application data. Uncheck this check box if you want to include the Cisco ADE operating system data in the backup as well.

Step 7 Check the **Repeating the Backup** check box if you want the scheduled backup to recur at the specified date and time. Uncheck this check box if you are scheduling the backup to be run only once.

Step 8 Enter the **Encryption Key**. This key is used to encrypt and decrypt the backup file.

Step 9 In the Schedule Options area:

- Choose the time of the day when you want the backup to run.
- Choose any one of the following:
  - Daily—If you want the backup to be run at a specified time every day.
  - Weekly—Choose the day of the week from the drop-down list box for the backup to be run on the specified day and time every week.
  - Monthly—Choose any date of the month (from 1 to 28) on which the backup will be run at the specified time.

Step 10 Click **Submit** to schedule the backup.

Click the Scheduled Backup List link at the top of this screen to return to the Scheduled Backup Listing page.

For more information:

The scheduled backup will be listed in the Scheduled Backup page. To see the status of your previously scheduled jobs, see the "Viewing Backup History" section on page 15 -10. This procedure schedules a backup job that backs up the Cisco ISE application and the Cisco ADE operating system data. To schedule a Monitoring and Troubleshooting database backup job, see the "Backing Up and Restoring the Monitoring Database" section on page 23 -45.

Deleting a Scheduled Backup

Cisco ISE allows you to delete an existing backup schedule and create a new schedule. There is no option to edit a scheduled backup job in Cisco ISE.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete a scheduled backup job, complete the following steps:

Step 1 Choose **Administration > System > Maintenance**.

Step 2 From the Operations navigation pane on the left, choose **Data Management > Administration Node > Scheduled Backup**.

The Scheduled Backup List page appears with a list of scheduled jobs.

Step 3 Click the radio button next to the scheduled backup job that you want to delete and click **Delete**.

Step 4 The following message appears:

Are you sure you want to delete this scheduled backup?

Step 5 Click **OK** to delete the scheduled backup.

Viewing Backup History

For scheduled backups, you can obtain information about the backup, backup events, and status (when the backup was performed, whether it was successful or not, and so on) from the Backup History page.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Monitoring Admin or Helpdesk Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

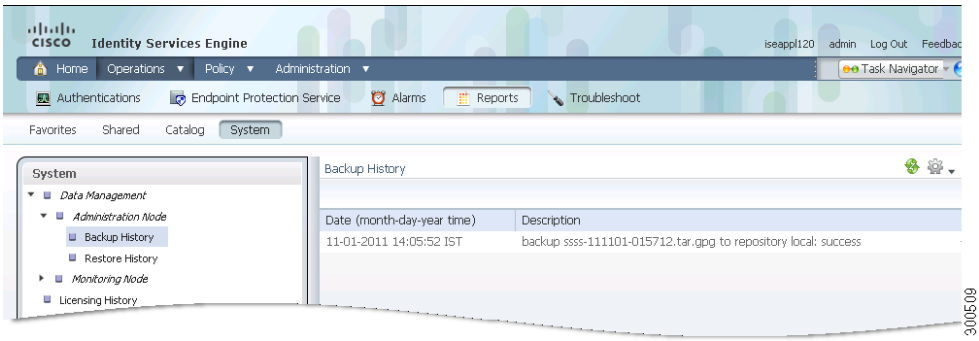
To view the backup history, complete the following steps:

Step 1 Choose **Operations > Reports > System**.

Step 2 From the System navigation pane on the left, choose **Data Management > Administration Node > Backup History**.

The Backup History page appears with information about all backups that were run on the Cisco ISE node as shown in Figure 15-2.

Figure 15-2 Backup History Page



The Backup History page provides basic information about the scheduled backups that were run. For failed backups, you must run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log for more information.

Note The backup history is stored along with the Cisco ADE operating system configuration data. After an application upgrade, backup history is not lost and the Backup History page lists all the backups that were run. The backup history will be removed only when you reimage the primary administration node.

Restoring Data from a Backup

You can restore data only through the Cisco ISE CLI.

- To restore the application data, from the Cisco ISE CLI, enter:

  restore *backupfilename.tar.gpg* **repository** *repositoryname* **application** *application name* **encryption-key hash | plain** *encryption-key name*

- To restore the application and Cisco ADE operating system data, from the Cisco ISE CLI, enter:

  restore *backupfilename.tar.gpg* **repository** *repositoryname* **encryption-key hash | plain** *encryption-key name*

where

- *backupfilename.tar.gpg* is the name of the backup file that you want to restore.
- *repositoryname* is the repository that contains your backup file.
- *encryption-key name* is the key that was used while creating the backup file. Encryption-key is optional while restoring data. To support restoring earlier backups where you have not provided encryption-keys, you can use the restore command without the encryption-key.

After you restore data, you must wait until all the application server processes are up and running. To verify if the Cisco ISE application server processes are running, enter the following command from the Cisco ISE CLI:

show application status ise

For more information, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.*

To check for the status of your restore job, see the "Viewing Restore History" section on page 15 -12.

Note If the sync status and replication status after application restore for any secondary node is *Out of Sync*, you have to reimport the certificate of that secondary node to the primary administration node and perform a manual synchronization. See Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 15-12 for the procedure to perform manual synchronization.

Viewing Restore History

You can obtain information about all restore operations, restore log events, and statuses (when the restore was done, whether it was successful or not, and so on) from the Restore History page.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Monitoring Admin or Helpdesk Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To view the restore history, complete the following steps:

Step 1 Choose **Operations > Reports > System**.

Step 2 From the System navigation pane on the left, choose **Data Management > Administration Node > Restore History**.

The Restore History page appears with information about all the restore operations that were performed on the Cisco ISE node.

Note Similar to the Backup History page, the Restore History page provides basic information on the restore job. For troubleshooting information, you have to run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log file.

Synchronizing Primary and Secondary Nodes in a Distributed Environment

In a distributed environment, after restoring a backup file on your primary administration node, sometimes the Cisco ISE database in the primary and secondary nodes are not synchronized automatically. At such times, you can manually force a full replication from the primary administration node to your secondary ISE nodes. You can force a synchronization only from a primary to secondary nodes. During the sync-up operation, you cannot make any configuration changes. Once a sync-up operation starts, a progress bar appears displaying the progress of the forced replication. Cisco ISE allows you to navigate to other Cisco ISE user interface pages and make any configuration changes only after the synchronization is complete.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To synchronize your secondary Cisco ISE nodes with your primary Cisco ISE node, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

Step 2 From the Deployment navigation pane on the left, click **Deployment**.

The Deployment Nodes page appears.

Step 3 Check the check boxes next to the secondary ISE nodes whose Replication Status is *Out of Sync*.

Step 4 Click **Syncup**.

The nodes are synchronized with the primary administration node. You will have to wait until this process is complete before you can access the Cisco ISE user interface again.

Result

When all the nodes are synchronized, the following message appears:

Sync up is done for all the nodes.

An error message appears if Cisco ISE cannot force a full replication.

Recovering Lost Nodes in Standalone and Distributed Deployments

This section provides troubleshooting information that you can use to recover lost nodes in standalone and multinode deployments. Some of the following use cases use the backup and restore functionality and others use the replication feature to recover lost data:

- Loss of All Nodes in a Distributed Setup, Recovery Using Existing IP Addresses and Hostnames, page 15-13
- Loss of All Nodes in a Distributed Deployment, Recovery Using New IP Addresses and Hostnames, page 15-14
- Standalone Deployment, Recovery Using Existing IP Address and Hostname, page 15-15
- Standalone Deployment, Recovery Using New IP Address and Hostname, page 15-15
- Configuration Rollback, page 15-16
- Primary Node Failure in a Distributed Deployment, page 15-16
- Secondary Node Failure in a Distributed Deployment, page 15-16

Loss of All Nodes in a Distributed Setup, Recovery Using Existing IP Addresses and Hostnames

In a distributed deployment setup, there is a natural disaster leading to the loss of all the nodes. After recovery, you want to use the existing addresses and hostnames.

Scenario

You have two nodes: N1 (primary Administration node) and N2 (secondary Administration node) and a backup of the N1 node is available that was taken at time t1. Later, both N1 and N2 nodes fail because of a natural disaster.

Assumption

All Cisco ISE nodes in the deployment were destroyed. The new hardware was imaged using the same hostnames and IP addresses.

Resolution Steps

1. You have to replace both N1 and N2 nodes. See "Replacing the Cisco ISE Appliance Hardware" section on page 9 -28 for more information. N1 and N2 nodes will now have a standalone configuration.
2. You must then restore the backup on the replaced N1 node. See "Restoring Data from a Backup" section on page 15 -11 for more information. The restore script will try to sync the data on N2, but N2 is now a standalone node and the sync will fail. Data on N1 will be reset to time t1.
3. You must log in to the N1 user interface to delete and reregister the N2 node. See the following for more information:
   - "Removing a Node from Deployment" section on page 9 -26
   - "Registering and Configuring a Secondary Node" section on page 9 -13

   Both the N1 and N2 nodes will now have data reset to time t1.

Loss of All Nodes in a Distributed Deployment, Recovery Using New IP Addresses and Hostnames

In a distributed setup, all the nodes in the deployment are destroyed because of a natural disaster. The new hardware is reimaged at a new location and requires new IP addresses and hostnames.

Scenario

You have two ISE nodes: N1 (primary Administration node) and N2 (secondary Policy Service node) and a backup of N1 node is available that was taken at time t1. Later, both N1 and N2 nodes fail because of a natural disaster. ISE nodes are replaced at a new location and the new hostnames are N1A (primary Administration node) and N2A (secondary Policy Service node). N1A and N2A are standalone nodes at this point in time.

Assumptions

All Cisco ISE nodes in the deployment were destroyed. The new hardware was imaged at a different location using different hostnames and IP addresses.

Resolution Steps

1. Obtain the N1 backup and restore it on N1A. See "Restoring Data from a Backup" section on page 15 -11 for more information. The restore script will identify the hostname change and domain name change, and will update the hostname and domain name in the deployment configuration based on the current hostname.
2. You must generate a new self-signed certificate. See "Generating a Self-Signed Certificate" section on page 13 -7 for more information.

3. You must log in to the Cisco ISE user interface on N1A, go to the deployment page (**Administration > System > Deployment**), and do the following:
   a. Delete the old N2 node. See "Removing a Node from Deployment" section on page 9 -26 for more information.
   b. Register the new N2A node as a secondary node. See "Registering and Configuring a Secondary Node" section on page 9 -13 for more information. Data from the N1A node will be replicated to the N2A node.

Standalone Deployment, Recovery Using Existing IP Address and Hostname

There is a standalone Administration node that goes down.

Scenario

You have a standalone Administration node, N1, and a backup of the N1 database that was taken at time t1 is available. The N1 node goes down because of a physical failure and must be reimaged or a new hardware is required. The N1 node must be brought back up with the same IP address and hostname.

Assumptions

This deployment is a standalone deployment and the new or reimaged hardware has the same IP address and hostname.

Resolution Steps

Once the N1 node is back up after a reimage or you have introduced a new ISE node with the same IP address and hostname, you must restore the backup taken from the old N1 node. You do not have to make any role changes. See "Restoring Data from a Backup" section on page 15 -11 for more information.

Standalone Deployment, Recovery Using New IP Address and Hostname

There is a standalone Administration node that goes down.

Scenario

You have a standalone administration node, N1, and a backup of the N1 database that was taken at time t1 is available. The N1 node goes down because of a physical failure and will be replaced by a new hardware at a different location with a different IP address and hostname.

Assumptions

This deployment is a standalone deployment and the replaced hardware has a different IP address and hostname.

Resolution Steps

1. Replace the N1 node with a new hardware. See "Replacing the Cisco ISE Appliance Hardware" section on page 9 -28 for more information. This node will be in a standalone state and the hostname is N1B.
2. You can restore the backup on the N1B node. See "Restoring Data from a Backup" section on page 15 -11 for more information. No role changes are required.

Configuration Rollback

There may be instances where you inadvertently make configuration changes that you later determine were incorrect. For example, you may delete several NADs or modify some RADIUS attributes incorrectly and realize this issue several hours later. In this case, you can revert back to the original configuration by restoring a backup that was taken before you made the changes.

Scenario

There are two nodes: N1 (primary Administration node) and N2 (secondary Administration node) and a backup of the N1 node is available. You made some incorrect configuration changes on N1 and want to remove the changes.

Resolution Steps

Obtain a backup of the N1 node that was taken before the incorrect configuration changes were made. Restore this backup on the N1 node. See "Restoring Data from a Backup" section on page 15 -11 for more information. Restore script will sync the data from N1 to N2.

Primary Node Failure in a Distributed Deployment

In a multinode deployment, the primary Administration node fails.

Scenario

You have two ISE nodes, N1 (primary Administration node) and N2 (secondary Administration node). N1 fails because of hardware issues.

Assumptions

Only the primary node in a distributed deployment has failed.

Resolution Steps

1. Log into the N2 user interface. Go to the deployment page and configure N2 as your primary node. See "Configuring Administration Cisco ISE Nodes for High Availability" section on page 9 -15 for more information.

   The N1 node is replaced with a new hardware, reimaged, and is in the standalone state.

2. From the N2 user interface, register the new N1 node as a secondary node. See "Registering and Configuring a Secondary Node" section on page 9 -13 for more information.

   Now, the N2 node becomes your primary node and the N1 node becomes your secondary node.

If you wish to make the N1 node the primary node again, log into the N1 user interface and make it the primary node. N2 automatically becomes a secondary server. There is no data loss.

Secondary Node Failure in a Distributed Deployment

In a multinode deployment, a single secondary node has failed. No restore is required.

Scenario

You have multiple nodes: N1 (primary Administration node), N2 (secondary Administration node), N3 (secondary Policy Service node), N4 (secondary Policy Service node). One of the secondary nodes, N3, fails.

Resolution Steps

1. Reimage the new N3A node to the default standalone state.
2. Log into the N1 user interface and delete the N3 node. See "Removing a Node from Deployment" section on page 9 -26 for more information.
3. Reregister the N3A node. See "Registering and Configuring a Secondary Node" section on page 9 -13 for more information.

   Data is replicated from N1 to N3A. No restore is required.



PART 3

Managing Cisco ISE Policy Models



CHAPTER 16

Managing Authentication Policies

This chapter describes how network access is granted to users who request access to your network resources. Using the Cisco Identity Services Engine (ISE) user interface, you can define authentication policies that determine who accesses the resources on your network. This chapter contains the following topics:

- Understanding Authentication Policies, page 16-1
- Protocol Settings, page 16-10
- Network Access Service, page 16-13
- Configuring the Simple Authentication Policy, page 16-26
- Configuring the Rule-Based Authentication Policy, page 16-29
- Authentication Policy Built-In Configurations, page 16-38
- Viewing Authentication Results, page 16-41

Understanding Authentication Policies

Authentication policies define the protocols that Cisco ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. A policy is a set of conditions and a result. A policy condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. Compound conditions are made up of one or more simple conditions that are connected by the AND or OR operator. At runtime, Cisco ISE evaluates the policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

Note During policy condition evaluation, Cisco ISE compares an attribute with a value. It is possible to run into a situation where the attribute specified in the policy condition may not have a value assigned in the request. In such cases, if the operator that is used for comparison is “not equal to,” then the condition will evaluate to true. In all other cases, the condition will evaluate to false.

For example, for a condition Radius.Calling_Station_ID Not Equal to 1.1.1.1, if the Calling Station ID is not present in the RADIUS request, then this condition will evaluate to true. This evaluation is not unique to the RADIUS dictionary and occurs because of the usage of the “Not Equal to” operator.

An authentication policy consists of the following:

- Network Access Service—This service can be one of the following:
  - An allowed protocols service to choose the protocols to handle the initial request and protocol negotiation.
  - A proxy service that will proxy requests to an external RADIUS server for processing.
- Identity Source—An identity source or an identity source sequence to be used for authentication.

After installation, a default identity authentication policy will be available in Cisco ISE that will be used for authentications. Any updates to the authentication policy will override the default settings.

The following is a list of protocols that you can choose while defining your authentication policy:

- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

By default, the identity source that Cisco ISE will look up for user information is the internal users database.

This section contains the following topics:

- Authentication Type, Protocols, and Databases, page 16-2
- Authentication Policy Terminology, page 16-3
- Simple Authentication Policies, page 16-4
- Rule-Based Authentication Policies, page 16-5

Authentication Type, Protocols, and Databases

The authentication type is based on the protocols that are chosen. Table 5-1 on page 5-1 lists the authentication type and the protocols that are supported by the various databases.

The authentication type is password based, where the authentication is performed against a database with the username and password that is presented in the request. The identity method, which is the result of the authentication policy, can be any one of the following:

- Deny access—Access to the user is denied and no authentication is performed.
- Identity database—A single identity database that can be any one of the following:
  - Internal users
  - Internal endpoints
  - Active Directory
  - Lightweight Directory Access Protocol (LDAP) database
  - RADIUS token server (RSA or SafeWord server)
  - Certificate authentication profile
- Identity source sequences—A sequence of identity databases that is used for authentication.

If you choose deny access, a reject message is sent as a response to the request. If you choose an identity database or an identity source sequence and the authentication succeeds, the processing continues to the authorization policy. Some of the authentications fail and these are classified as follows:

- Authentication failed—Received explicit response that authentication has failed such as bad credentials, disabled user, and so on. The default course of action is reject.
- User not found—No such user was found in any of the identity databases. The default course of action is reject.
- Process failed—Unable to access the identity database or databases. The default course of action is drop.

Cisco ISE allows you to configure any one of the following courses of action for authentication failures such as authentication failed, user not found, or process failures:

- Reject—A reject response is sent.
- Drop—No response is sent.
- Continue—Cisco ISE continues with the authorization policy.

Note Even when you choose the Continue option, there might be instances where Cisco ISE cannot continue processing the request due to restrictions on the protocol that is being used. When authentication fails, it is possible to continue to process the authorization policy for PAP/ASCII, EAP-TLS, or MAC authentication bypass (MAB or host lookup).

For all other authentication protocols, when authentication fails, the following happens:

- Authentication failed—A reject response is sent.
- User or host not found—A reject response is sent.
- Process failure—No response is sent and the request is dropped.

Authentication Policy Terminology

Table 16-1 lists some of the commonly used terms in the authentication policy pages.

Table 16-1 Authentication Policy Terminology

Term	Description
Allowed Protocols	Allowed protocols define the set of protocols that Cisco ISE can use to communicate with the device that requests access to the network resources.
Identity Source	Identity source defines which database Cisco ISE should use for user information. The database could be an internal database or an external identity source, such as Active Directory or LDAP. You can add a sequence of databases to an identity source sequence and list this sequence as the identity source in your policy. Cisco ISE will search for the credentials in the order in which the databases are listed in this sequence.
Failover Options	You can define what course of action Cisco ISE should take if the authentication fails, the user is not found, or if the process fails.

Simple Authentication Policies

A simple authentication policy allows you to statically define the allowed protocols and the identity source or identity source sequence that Cisco ISE should use for communication. You cannot define any condition for simple policies. Cisco ISE assumes that all conditions are met and uses the following definitions to determine the result:

- You can create simple policies in situations where you can statically define the allowed protocols and the identity source that must be used always, and no condition needs to be checked.
- You can also create proxy service-based simple policies. Cisco ISE proxies the request to a policy server to determine which identity source should be used for user authentication. If the request is proxied to a different policy server, the protocol negotiation does not happen. The policy server evaluates which identity source should be used for authentication and returns the response to Cisco ISE.

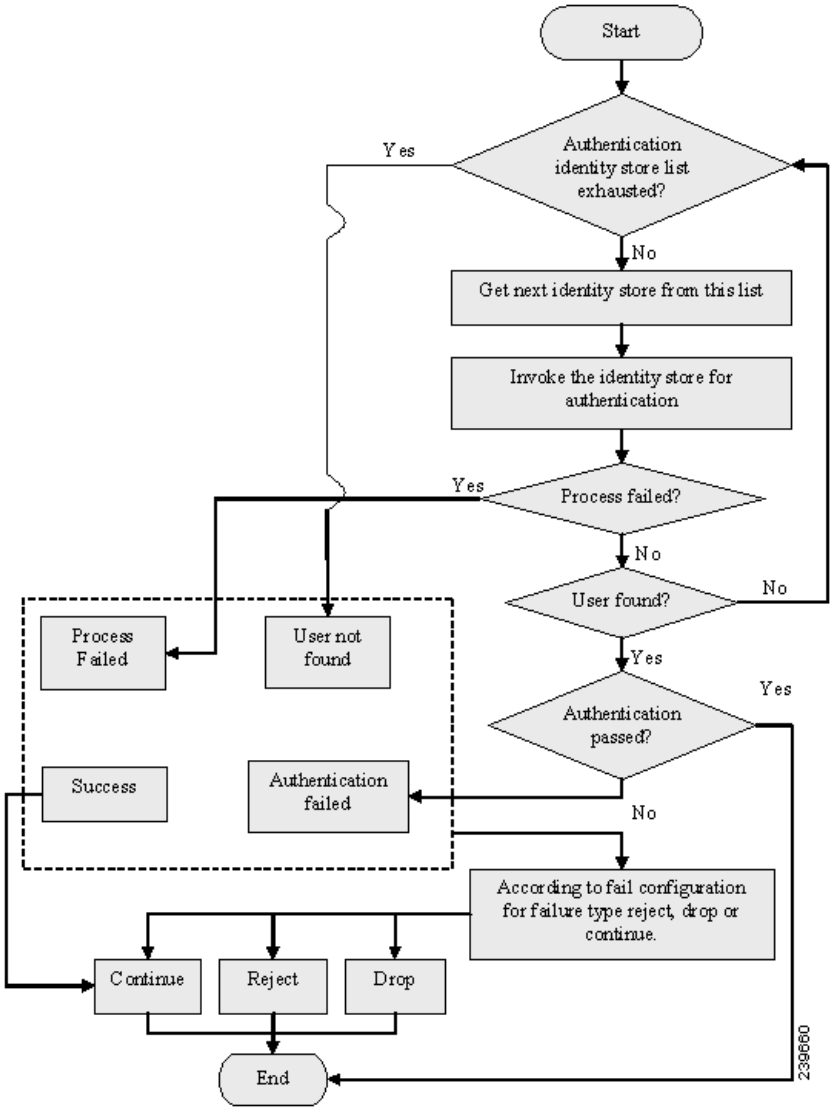
Note Host authentication is performed with the MAC address only (MAB).

The result of a simple policy can be any one of the following:

- Deny access
- Identity database
- Identity sequence

Figure 16-1 shows the simple authentication policy flow.

Figure 16-1 Simple Authentication Policy Flow



Rule-Based Authentication Policies

Rule-based authentication policies consist of attribute-based conditions that determine the allowed protocols and the identity source or identity source sequence to be used for processing the requests. In a simple authentication policy, you can define the allowed protocols and identity source statically. In a rule-based policy, you can define conditions that allows Cisco ISE to dynamically choose the allowed protocols and identity sources. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE supports the following dictionaries:

- *Airespace*
- CERTIFICATE
- *Cisco*
- *Cisco-BBSM*
- *Cisco-VPN3000*
- DEVICE
- *Microsoft*
- *Network access*
- RADIUS

where CERTIFICATE, DEVICE, and RADIUS are system-defined dictionaries and *Airespace, Cisco, Cisco-BBSM, Cisco-VPN3000, Microsoft*, and *Network Access* are RADIUS vendor dictionaries.

See the "Dictionaries and Dictionary Attributes" section on page 7-1 for more information on the dictionaries in Cisco ISE.

Cisco ISE allows you to create conditions as individual, reusable policy elements that can be referred from other rule-based policies. You can also create conditions from within the policy creation page. There are two types of conditions:

- Simple condition—A simple condition takes the form *attribute operand value*. These can be saved and reused in other rule-based policies. The simple condition can take the form: A operand B, where A can be any attribute from the ISE dictionary and B can be one of the values that the attribute A can take.

  This is an example of a simple condition: DEVICE:Device Type Equals All Device Types

  See the "Simple Conditions" section on page 16-31 for more information.

- Compound condition—A compound condition is made up of one or more simple conditions with an AND or OR relationship. These are built on top of simple conditions. These can be saved and reused in other rule-based policies. The compound conditions take any one of the following forms:
  - (X operand Y) AND (A operand B) AND (X operand Z) AND so on
  - (X operand Y) OR (A operand B) OR (X operand Z) OR so on

  where X and A are attributes from the ISE dictionary such as username, device type, and so on.

  This is an example of a compound condition: DEVICE:Model Name Matches Catalyst6K AND Network Access:Use Case Equals Host Lookup.

  See the "Compound Conditions" section on page 16-33 for more information.

Table 16-2 lists the fixed attributes that are supported by these dictionaries, which can be used in policy conditions.

Table 16-2 List of Attributes Supported by the Dictionaries

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Device	Device Type (predefined network device group)	Yes	Yes
	Device Location (predefined network device group)		
	Other Custom Network Device Group		
	Software Version		
	Model Name		
RADIUS	All attributes	Yes	Yes
Network Access[1]	ISE Host Name	Yes	Yes
	AuthenticationMethod	No	Yes
	AuthenticationStatus	No	No
	CTSDeviceID	No	No
	Device IP Address	Yes	Yes
	EapAuthentication (the EAP method that is used during authentication of a user of a machine)	No	Yes
	EapTunnel (the EAP method that is used for tunnel establishment)	No	Yes
	Protocol	Yes	Yes
	UseCase	Yes	Yes
	UserName	No	Yes
	WasMachineAuthenticated	No	No

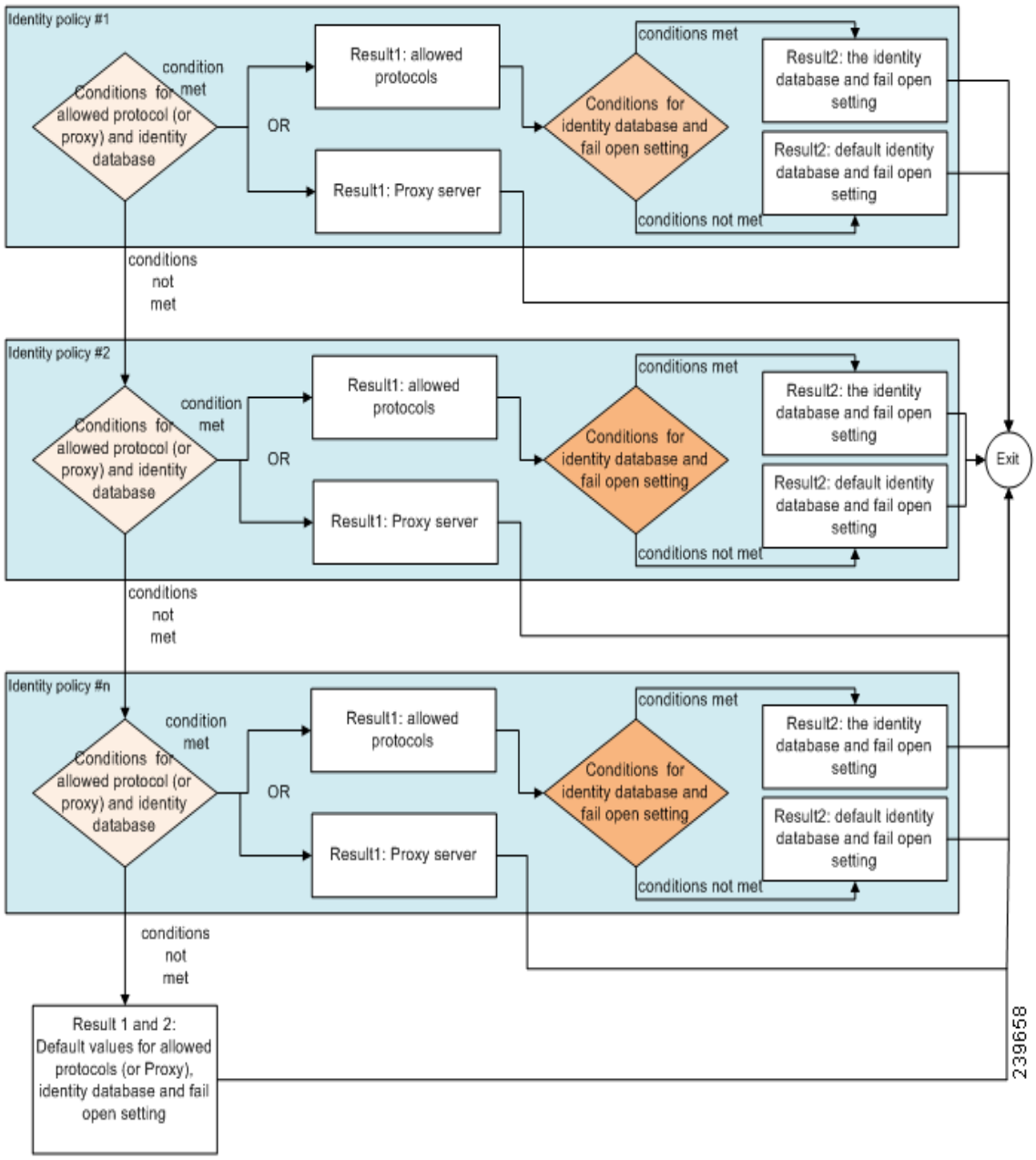
Table 16-2 List of Attributes Supported by the Dictionaries (continued)

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Certificate	Common Name	No	Yes
	Country		
	Email		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - Email		
	Subject Alternative Name - Other Name		
	Subject Serial Number		

1. Not all of these attributes are available for creating all types of conditions. For example, while creating a condition to choose the access service in authentication policies, you would only see the following network access attributes: Device IP Address, ISE Host Name, Network Device Name, Protocol, and Use Case.

Figure 16-2 shows the rule-based authentication policy flow.

Figure 16-2 Rule-Based Authentication Policy Flow



In rule-based policies, you can define multiple rules as illustrated in Figure 16-2. The identity database is selected based on the first rule that matches the criteria.

You can also define an identity source sequence consisting of different databases. You can define the order in which you want Cisco ISE to look up these databases. Cisco ISE will access these databases in sequence until the authentication succeeds. If there are multiple instances of the same user in an external database, the authentication fails. There can only be one user record in an identity source.

Note We recommend that you use only three, or at most four databases in an identity source sequence.

Note If you want to switch between the simple and rule-based policies, you must reconfigure the policies because the policy data will no longer be available.

Protocol Settings

You must define global protocol settings in Cisco ISE before you can use these protocols to process an authentication request. You can use the Protocol Settings page to define global options for the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP) protocols, which communicate with the other devices in your network. This section contains the following topics:

- Configuring EAP-FAST Settings, page 16-10
- Configuring EAP-TLS Settings, page 16-12
- Configuring PEAP Settings, page 16-12
- Generating the PAC for EAP-FAST, page 16-11

Configuring EAP-FAST Settings

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure EAP-FAST settings, complete the following steps:

Step 1 Choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **EAP-FAST > EAP Fast Settings**.

The EAP-FAST Global Settings page appears.

Step 4 Enter the information as described:

- Authority Identity Info Description—(Required) A user-friendly string that describes the Cisco ISE node that sends credentials to a client. The client can discover this string in the Protected Access Credentials (PAC) information for type, length, and value (TLV). The default value is Identity Services Engine.
- Master Key Generation Period—(Required) Specifies the master key generation period in seconds, minutes, hours, days, or weeks. The value must be a positive integer in the range 1 to 2147040000 seconds. The default is 604800 seconds, which is equivalent to one week.

Step 5 Click **Revoke** if you want to revoke all the previously generated master keys and PACs.

Step 6 Click **Save** to save the EAP-FAST settings.

Generating the PAC for EAP-FAST

You can use the Generate PAC option in the Cisco ISE to generate a tunnel or machine PAC for the EAP-FAST protocol.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To generate the PAC for EAP-FAST, complete the following steps:

Step 1 Choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **EAP-FAST > Generate PAC.**

The Generate PAC page appears.

Step 4 Enter information as described:

- Tunnel PAC—(Either tunnel PAC or machine PAC is required) Click this radio button to generate a tunnel PAC. This option is the default.
- Machine PAC—Click this radio button to generate a machine PAC.
- SGA PAC—Click this radio button to generate an SGA PAC.
- Identity—(Required) For the Tunnel and Machine PAC identity field, this specifies the username or machine name that is presented as the "inner username" by the EAP-FAST protocol. If the identity string does not match that username, authentication fails.

  If you are generating the SGA PAC, the Identity field specifies the Device ID of an SGA network device and is provided with an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication fails. See the "OOB SGA PAC" section on page 22-31for more information on SGA PAC.
- PAC Time to Live—(Required) For the Tunnel and Machine PAC, enter a value in seconds that specifies the expiration time for the PAC. The default is 604800 seconds, which is equivalent to one week. This value must be a positive integer between 1 and 157680000 seconds.

  For the SGA PAC, enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is 10 years.
- Encryption Key—(Required) Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.
- Expiration Data—(For SGA PAC only) The expiration date is calculated based on the PAC Time to Live.

Step 5 Click **Generate PAC** to generate the PAC.

Configuring EAP-TLS Settings

You can configure the runtime characteristics of the EAP-TLS protocol from the Global Options page.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure EAP-TLS settings, complete the following steps:

Step 1 Choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **EAP-TLS**.

The EAP-TLS settings page appears.

Step 4 Enter the information as described:

- Enable EAP-TLS Session Resume—Check this check box to support an abbreviated reauthentication of a user who has passed full EAP-TLS authentication. This feature provides reauthentication of the user with only a Secure Sockets Layer (SSL) handshake and without applying the certificates. EAP-TLS session resume works only if the EAP-TLS session has not timed out.
- EAP-TLS Session Timeout—Specifies the time in seconds after which the EAP-TLS session times out. The default value is 7200 seconds.

Step 5 Click **Save** to save the EAP-TLS settings.

Configuring PEAP Settings

You can configure the runtime characteristics of the PEAP protocol from the Global Options page.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure PEAP settings, complete the following steps:

Step 1 Choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **PEAP**.

The PEAP Settings page appears.

Step 4 Enter the information as described:

- Enable PEAP Session Resume—Check this check box for the Cisco ISE to cache the TLS session that is created during phase one of PEAP authentication, provided the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, the Cisco ISE uses the cached TLS session, resulting in faster PEAP performance and a reduced AAA server load.

  You must specify a PEAP session timeout value for the PEAP session resume features to work.
- PEAP Session Timeout—Specifies the time in seconds after which the PEAP session times out. The default value is 7200 seconds.
- Enable Fast Reconnect—Check this check box to allow a PEAP session to resume in the Cisco ISE without checking user credentials when the session resume feature is enabled.

Step 5 Click **Save** to save the PEAP settings.

Network Access Service

A network access service contains the authentication policy conditions for requests. You can create separate network access services for different use cases. For example, Wired 802.1X, Wired MAB, and so on. These are the two types of network access services that you can use in authentication policies:

- Allowed Protocols, page 16-13
- Proxy Service, page 16-21

Allowed Protocols

Allowed protocols define the set of protocols that Cisco ISE can use to communicate with the device that requests access to the network resources. An allowed protocols access service is an independent entity that you should create before you configure authentication policies. Allowed protocols access service is an object that contains your chosen protocols for a particular use case.

The Allowed Protocols Services page lists all the allowed protocols services that you create. There is a default network access service that is predefined in the Cisco ISE.

Related Topics

- Defining Allowed Protocols, page 16-14
- Deleting Allowed Protocols, page 16-21
- Configuring the Simple Authentication Policy, page 16-26
- Configuring the Rule-Based Authentication Policy, page 16-29

Defining Allowed Protocols

Prerequisites:

Before you begin this procedure, you should have a basic understanding of the protocol services that are used for authentication. Review the information and the sections noted in the following:

- The Note in Understanding Authentication Policies to understand authentication type and the protocols that are supported by various databases.
- The Allowed Protocols Service and PAC Options sections, to understand the functions and options for each protocol service, so you can make the selections that are appropriate for your network.
- Ensure that you have defined the global protocol settings. See the "Protocol Settings" section on page 16-10 for more information.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To define an allowed protocols service, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 Click the greater-than sign (>) next to Authentication in the Results navigation pane on the left.

Step 3 Click **Allowed Protocols**. The Allowed Protocols Services page appears.

Note If Cisco ISE is set to operate in FIPS mode, some protocols are disabled be default and cannot be configured.

Step 4 Click **Add**.

Step 5 Enter the following information:

- Name—(Required) Enter the name of the allowed protocols service.
- Description—Enter an optional description for the allowed protocol service.

Step 6 Select the appropriate Authentication Protocols and options for your network, as described in Table 16-3.

Figure 16-3 shows an example of an allowed protocol selection.

Step 7 If you choose to use PACs, make the appropriate selections, as described in Table 16-4.

Note To enable Anonymous PAC Provisioning, you must choose both the inner methods, EAP-MSCHAPv2 and Extensible Authentication Protocol-Generic Token Card (EAP-GTC). Also, be aware that Cisco ISE only supports Active Directory as an external identity source for machine authentication.

Step 8 Click **Submit** to save the allowed protocols service.

The allowed protocols service appears as an independent object in the simple and rule-based authentication policy pages. You can use this object in different rules.

Step 9 You can now create a simple or rule-based authentication policy.

Allowed Protocols Service

Table 16-3 explains the protocol options you specify when Defining Allowed Protocols.

Table 16-3 Allowed Protocols Service

Option	Description
Allowed Protocols	
Process Host Lookup	Check this check box to configure Cisco ISE to process the Host Lookup field (for example, when the RADIUS Service-Type equals 10) and use the System UserName attribute from the RADIUS Calling-Station-ID attribute. Uncheck this check box if you want Cisco ISE to ignore the Host Lookup request and use the original value of the system UserName attribute for authentication. When unchecked, message processing is done according to the protocol (for example, PAP). **Note** When you want to use the Microsoft Active Directory for MAB authentication, you must uncheck the Process Host Lookup check box from the allowed protocol service that is associated to an authentication policy. You can find the allowed protocol services that you have created in the following location: **Policy > Policy Elements > Results > Authentication > Allowed Protocols > Allowed Protocols Services.**
Authentication Protocols	
Allow PAP/ASCII	This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol. When you check the Allow PAP/ASCII check box, you can check the Detect PAP as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of PAP) request.
Allow CHAP	This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
Allow MS-CHAPv1	This option enables MS-CHAPv1.
Allow MS-CHAPv2	This option enables MS-CHAPv2.
Allow EAP-MD5	This option enables EAP-based MD5 hashed authentication. When you check the Allow EAP-MD5 check box, you can check the Detect EAP-MD5 as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of EAP-MD5) request.

Table 16-3 Allowed Protocols Service (continued)

Option	Description
Allow EAP-TLS	This option enables the EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how Cisco ISE will verify the user identity as presented in the EAP identity response from the end-user client. User identity is verified against information in the certificate that the end-user client presents. This comparison occurs after an EAP-TLS tunnel is established between Cisco ISE and the end-user client. **Note** EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates. Refer to Chapter 13, "Managing Certificates" for more information on certificates.
Allow LEAP	This option enables Lightweight Extensible Authentication Protocol (LEAP) authentication.
Allow PEAP	This option enables the PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2. When you check the Allow PEAP check box, you can configure the following PEAP inner methods: • Allow EAP-MS-CHAPv2—Check this check box to use EAP-MS-CHAPv2 as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retries—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-GTC—Check this check box to use EAP-GTC as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retries—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method.

Table 16-3 Allowed Protocols Service (continued)

Option	Description
Allow EAP-FAST	This option enables the EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MS-CHAPv2. When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method: • Allow EAP-MS-CHAPv2 – Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. – Retries—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Allow EAP-GTC • Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. • Retries—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Use PACs—Choose this option to configure Cisco ISE to provision authorization PACs[1] for EAP-FAST clients. Additional PAC options appear. • Don't use PACs—Choose this option to configure Cisco ISE to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and Cisco ISE responds with a Success-TLV without a PAC. When you choose this option, you can configure Cisco ISE to perform machine authentication.
Preferred EAP Protocol	Check this check box to choose your preferred EAP protocols from any of the following options: EAP-FAST, PEAP, LEAP, EAP-TLS, and EAP-MD5. By default, LEAP is the preferred protocol to use if you do not enable this field.

1. PACs = Protected Access Credentials.

PAC Options

The following table describes the PAC options you can choose from when Defining Allowed Protocols.

Table 16-4 PAC Options

Option	Description
Use PAC	• Tunnel PAC Time to Live—The TTL[1] value restricts the lifetime of the PAC. Specify the lifetime value and units. The default is 90 days. The range is between 1 and 1825 days. • Proactive PAC Update will occur after <n%> of PAC Time to Live Has Expired—The Update value ensures that the client has a valid PAC. Cisco ISE initiates an update after the first successful authentication but before the expiration time that is set by the TTL. The update value is a percentage of the remaining time in the TTL. The default is 90%. • Allow Anonymous In-band PAC Provisioning—Check this check box for Cisco ISE to establish a secure anonymous TLS handshake with the client and provision it with a PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. **Note** To enable anonymous PAC provisioning, you must choose both of the inner methods, EAP-MSCHAPv2 and EAP-GTC. • Allow Authenticated In-band PAC Provisioning—Cisco ISE uses SSL server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning but requires that a server certificate and a trusted root CA be installed on Cisco ISE. When you check this option, you can configure Cisco ISE to return an Access-Accept message to the client after successful authenticated PAC provisioning. – Server Returns Access Accept After Authenticated Provisioning—Check this check box if you want Cisco ISE to return an access-accept package after authenticated PAC provisioning. • Allow Machine Authentication—Check this check box for Cisco ISE to provision an end-user client with a machine PAC and perform machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by the administrator (out-of-band). When Cisco ISE receives a valid machine PAC from the end-user client, the machine identity details are extracted from the PAC and verified in the Cisco ISE external identity source. After these details are correctly verified, no further authentication is performed. **Note** Cisco ISE only supports Active Directory as an external identity source for machine authentication. When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When Cisco ISE receives an expired machine PAC, it automatically reprovisions the end-user client with a new machine PAC (without waiting for a new machine PAC request from the end-user client).

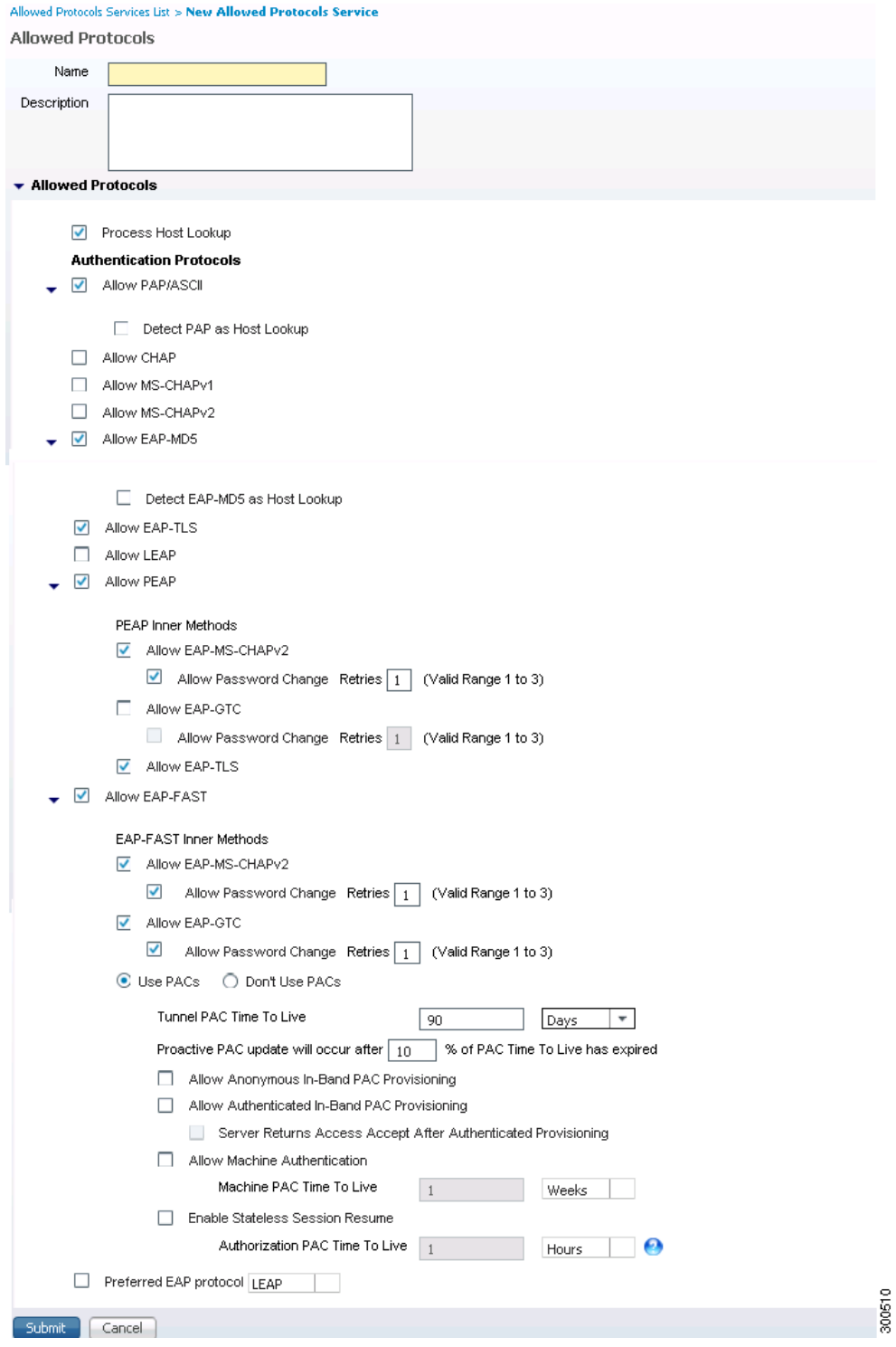
Table 16-4 PAC Options (continued)

Option	Description
	• Enable Stateless Session Resume—Check this check box for Cisco ISE to provision authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled). Uncheck this check box in the following cases: – If you do not want Cisco ISE to provision authorization PACs for EAP-FAST clients – To always perform phase two of EAP-FAST When you check this option, you can enter the authorization period of the user authorization PAC. After this period, the PAC expires. When Cisco ISE receives an expired authorization PAC, it performs phase two EAP-FAST authentication.

1. TTL = Time To Live

Figure 16-3 shows an example of selections made for an allowed protocols service.

Figure 16-3 Allowed Protocols Service



Deleting Allowed Protocols

Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- Ensure that the allowed protocol service that you are about to delete is not referenced in any authentication policies.

To delete an allowed protocol service, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 Click the greater-than sign (>) next to Authentication in the Results navigation pane on the left.

Step 3 Click **Allowed Protocols**.

The Allowed Protocols page appears with the list of allowed protocols that you have defined.

Step 4 Check the check box next to the allowed protocol service or services that you want to delete, then click **Delete**. Alternatively, you can choose the allowed protocol service from the navigation pane on the left and click **Delete service** from the action icon.

Note If you have chosen more than one allowed protocol service to delete, and if one of them is referenced in an authentication policy, then the entire delete operation fails. Ensure that the allowed protocols that you want to delete are not referenced in any authentication policies.

Cisco ISE prompts you with the following message:

Are you sure you want to delete?

Step 5 Click **OK** to delete the allowed protocol service or services that you have selected.

Proxy Service

Cisco ISE acts as a RADIUS proxy server by proxying the requests from a network access device (NAD) to a RADIUS server. The RADIUS server processes the request and returns the result to Cisco ISE. Cisco ISE then sends the response to the NAD. In both simple and rule-based authentication policies, you can use the RADIUS server sequences to proxy the requests to a RADIUS server.

Note The RADIUS server sequence strips the domain name from the RADIUS-Username attribute for RADIUS authentications. This domain stripping is not applicable for EAP authentications, which use the EAP-Identity attribute. The RADIUS proxy server obtains the username from the RADIUS-Username attribute and strips it from the character that you specify when you configure the RADIUS server sequence. For EAP authentications, the RADIUS proxy server obtains the username from the EAP-Identity attribute. EAP authentications that use the RADIUS server sequence will succeed only if the EAP-Identity and RADIUS-Username values are the same.

To use the RADIUS server sequence for authentication, you should successfully complete the following tasks:

- Defining an External RADIUS Server, page 16-22
- Defining a RADIUS Server Sequence, page 16-25

Defining an External RADIUS Server

The Cisco ISE can function both as a RADIUS server and as a RADIUS proxy server. When it acts as a proxy server, the Cisco ISE receives authentication and accounting requests from the network access server (NAS) and forwards them to the external RADIUS server. The Cisco ISE accepts the results of the requests and returns them to the NAS. You must configure the external RADIUS servers in the Cisco ISE to enable it to forward requests to the external RADIUS servers. You can define the timeout period and the number of connection attempts.

The Cisco ISE can simultaneously act as a proxy server to multiple external RADIUS servers. You can use the external RADIUS servers that you configure here in RADIUS server sequences. This External RADIUS Server page lists all the external RADIUS servers that you have defined in Cisco ISE. You can use the filter option to search for specific RADIUS servers based on the name or description or both.

Note Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To search for RADIUS servers, complete the following steps:

Step 1 Choose **Administration > Network Resources > External RADIUS Servers**.

The External RADIUS Servers page appears.

Step 2 Click **Filter > Advanced Filter** to perform your search. The Filter page appears.

Step 3 You must define whether the search should match any or all of the rules that you define on this page.

Step 4 Enter your search criteria based on the name or description of the RADIUS server, choose an operator, and enter the value.

Step 5 You can do the following:

- To add a filter condition, click the plus sign (+).
- To remove a filter condition, click the minus sign (-).
- To clear all filter conditions, click **Clear Filter**.

Step 6 Click **Go** to perform your search.

You can also save the filter criteria so that it can be used again. Click the **Save** icon to save the filter condition.

Results:

A list of external RADIUS servers that match your search criteria are displayed.

Related Topics

- Creating RADIUS Servers, page 16-23
- Editing RADIUS Servers, page 16-24
- Deleting RADIUS Servers, page 16-25

Creating RADIUS Servers

Prerequisites:

- You cannot use the external RADIUS servers that you create in this section by themselves. You must create a RADIUS server sequence and configure it to use the RADIUS server that you create in this section. You can then use the RADIUS server sequence in authentication policies.

  To create the RADIUS server sequence, see the "Defining a RADIUS Server Sequence" section on page 16-25.

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create an external RADIUS server, complete the following steps:

Step 1 Choose **Administration > Network Resources > External RADIUS Servers**.

The RADIUS Servers page appears with a list of external RADIUS servers that are defined in Cisco ISE.

Step 2 Click **Add** to add an external RADIUS server.

Step 3 Enter the values as described:

- Name—(Required) Enter the name of the external RADIUS server.
- Description—Enter a description of the external RADIUS server.
- Host IP—(Required) Enter the IP address of the external RADIUS server.
- Shared Secret—(Required) Enter the shared secret between Cisco ISE and the external RADIUS server that is used for authenticating the external RADIUS server. A shared secret is an expected string of text that a user must provide to enable the network device to authenticate a username and password. The connection is rejected until the user supplies the shared secret. The shared secret can be up to 128 characters in length.
- Enable KeyWrap—This option increases RADIUS protocol security via an AES KeyWrap algorithm, to help enable FIPS 140-2 compliance in Cisco ISE.
- Key Encryption Key—This key is used for session encryption (secrecy).
- Message Authenticator Code Key—This key is used for keyed HMAC calculation over RADIUS messages.
- Key Input Format—Specify the format you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that is available on the WLAN controller. (The value you specify must be the correct [full] length for the key as defined below—shorter values are not permitted.)
  - ASCII—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.

  - Hexadecimal—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.
- Authentication Port—(Required) Enter the RADIUS authentication port number. The valid range is from 1 to 65535. The default is 1812.
- Accounting Port—(Required) Enter the RADIUS accounting port number. The valid range is from 1 to 65535. The default is 1813.
- Server Timeout—(Required) Enter the number of seconds that the Cisco ISE waits for a response from the external RADIUS server. The default is 5 seconds. Valid values are from 5 to 120.
- Connection Attempts—(Required) Enter the number of times that the Cisco ISE attempts to connect to the external RADIUS server. The default is 3 attempts. Valid values are from 1 to 9.

Step 4 Click **Submit** to save the external RADIUS server configuration.

Related Topics

- Defining an External RADIUS Server, page 16-22
- Editing RADIUS Servers, page 16-24
- Deleting RADIUS Servers, page 16-25

Editing RADIUS Servers

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To edit an external RADIUS server, complete the following steps:

Step 1 Choose **Administration > Network Resources > External RADIUS Servers**.

The RADIUS Servers page appears with a list of external RADIUS servers.

Step 2 Check the check box next to the RADIUS server that you want to edit and click **Edit**.

Step 3 Modify the values as described in Step 3 of Creating RADIUS Servers.

Step 4 Click **Submit** to save your changes.

Related Topics

- Defining an External RADIUS Server, page 16-22
- Creating RADIUS Servers, page 16-23
- Deleting RADIUS Servers, page 16-25

Deleting RADIUS Servers

Prerequisites:

- You cannot use a RADIUS server by itself. You have to create a RADIUS server sequence and configure it to use the RADIUS server. Before you delete an external RADIUS server, ensure that no RADIUS server sequence uses it.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete an external RADIUS server, complete the following steps:

Step 1 Choose **Administration > Network Resources > External RADIUS Servers**.

The RADIUS Servers page appears with a list of external RADIUS servers.

Step 2 Check the check box next to the RADIUS server that you want to delete and click **Delete**.

A dialog box appears with the following message:

Are you sure you want to delete?

Step 3 Click **OK** to delete the RADIUS server.

Defining a RADIUS Server Sequence

RADIUS server sequences in Cisco ISE allow you to proxy requests from a NAD to an external RADIUS server that would process the request and return the result to Cisco ISE, which forwards the response to the NAD. This page lists all the RADIUS server sequences that you have defined in Cisco ISE. You can create, edit, or duplicate RADIUS server sequences from this page. See "Creating, Editing, and Duplicating RADIUS Server Sequences" procedure on page 16-25 for more information.

Related Topics

- Proxy Service, page 16-21
- Defining an External RADIUS Server, page 16-22

Creating, Editing, and Duplicating RADIUS Server Sequences

Prerequisites:

- Before you begin this procedure, you should have a basic understanding of the Proxy Service and must have successfully completed the task for Defining an External RADIUS Server.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create, edit, or duplicate a RADIUS server sequence, complete the following steps:

Step 1 Choose **Administration > Network Resources > RADIUS Server Sequences**.

The RADIUS Server Sequences page appears.

Step 2 Click **Add** to add a RADIUS server sequence, or choose an existing RADIUS server sequence and click **Edit** or **Duplicate** to edit or duplicate an existing sequence.

Step 3 Enter the name of the RADIUS server sequence.

Step 4 Enter an optional description.

Step 5 In the User Selected Service Type area, choose the external RADIUS servers that you want to use as policy servers from the Available list box and move them to the Selected list box.

Step 6 Expand **Advanced Settings**.

Step 7 Enter the following information in the Advanced Settings area:

a. Remote Accounting—Check this check box to enable accounting in the remote policy server.

b. Local Accounting—Check this check box to enable accounting in Cisco ISE.

c. Strip Start of Subject Name up to the First Occurrence of the Separator—Check this check box to strip the username from the prefix. For example, if the subject name is acme\smith and the separator is \, the username becomes smith.

d. Strip End of Subject Name from the Last Occurrence of the Separator—Check this check box to strip the username from the suffix. For example, if the subject name is smith@acme.com and the separator is @, the username becomes smith.

Note You must enable the strip options to extract the username from NetBIOS or User Principle Name (UPN) format usernames (user@domain.com or /domain/user) because only usernames are passed to the RADIUS server for authenticating the user.

Step 8 Click **Submit** to save the RADIUS server sequence to be used in policies.

Next Steps:

1. See the "Configuring a Simple Policy Using RADIUS Server Sequence" section on page 16-29 for information on how to configure a simple authentication policy using the RADIUS server sequence that you created.
2. See the "Configuring the Rule-Based Authentication Policy" section on page 16-29 for information on how to configure a rule-based authentication policy using the RADIUS server sequence that you created.

Configuring the Simple Authentication Policy

The procedure for configuring a simple authentication policy includes defining an allowed protocols service and configuring a simple authentication policy. See the "Defining Allowed Protocols" section on page 16-14 for information on how to create an allowed protocols service.

Note

- If you wish to use the RADIUS server sequence, then you must define this access service before you define the policy. See the "Proxy Service" section on page 16-21 for more information.
- If your users are defined in external identity sources, ensure that you have configured these identity sources in Cisco ISE before you define the policy. See the "Managing External Identity Sources" section on page 5-1 for information on how to configure the external identity sources.
- If you want to use an identity source sequence for authenticating users, ensure that you have created the identity source sequence before you define the policy. See the "Creating Identity Source Sequences" section on page 5-52 for more information.
- When you switch between simple and rule-based authentication policies, you will lose the policy that you configured earlier. For example, if you configured a simple authentication policy and you want to move to a rule-based authentication policy, you will lose the simple authentication policy. Also, when you move from a rule-based authentication policy to a simple authentication policy, you will lose the rule-based authentication policy.

Prerequisites:

- Before you begin this procedure, you should have successfully completed the task for Defining Allowed Protocols.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To define a simple authentication policy, complete the following steps:

Step 1 Choose **Policy > Authentication**.

Step 2 Click the **Simple** radio button.

The following message appears:

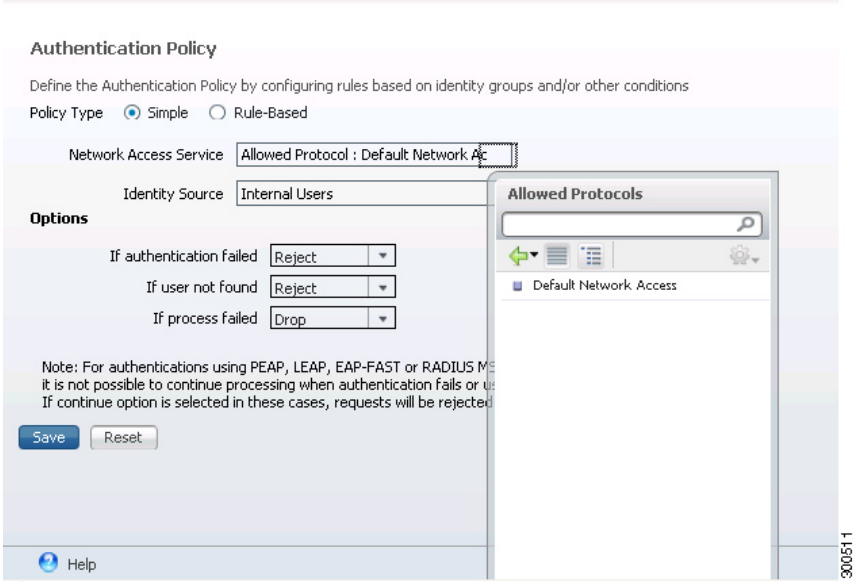
You switched from single to rule-based result selection. Any settings saved in the single mode will be lost when you submit. Click OK to continue.

Step 3 Click **OK** to continue.

Step 4 Choose an allowed protocol that you have already created from the Network Access Service drop-down menu.

To choose your allowed protocols service, expand the Allowed Protocols list by clicking the icon as shown in Figure 16-4.

Figure 16-4 Choosing Network Access Service



Step 5 Choose the identity source that you want to use for authentication from the Identity Source drop-down menu.

Note You can also choose an identity source sequence if you have configured it. See the "Creating Identity Source Sequences" section on page 5-52 for information on how to configure identity source sequences.

Step 6 In the Options area, you can define a further course of action for authentication failure, user not found, or process failure events. You can choose one of the following options:

- Reject—A reject response is sent.
- Drop—No response is sent.
- Continue—Cisco ISE proceeds with the authorization policy.

Step 7 Click **Save** to save your simple authentication policy.

Related Topics

- Understanding Authentication Policies, page 16-1
- Proxy Service, page 16-21
- Configuring a Simple Policy Using RADIUS Server Sequence, page 16-29

Configuring a Simple Policy Using RADIUS Server Sequence

Prerequisites:

- To configure a simple authentication policy using the RADIUS server sequence, you should have a basic understanding of the Proxy Service and have successfully completed the task for Defining a RADIUS Server Sequence.
- The Note in Understanding Authentication Policies to understand authentication type and the protocols that are supported by various databases.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure a simple authentication policy using the RADIUS server sequence, complete the following steps:

Step 1 Choose **Policy > Authentication**.

The Authentication Policy page appears.

Step 2 For the Authentication Method, click the **Simple** radio button.

Step 3 From the Network Access Service drop-down list box, choose the proxy service that you want to use.

Step 4 From the Identity Source drop-down list box, choose the identity database or the identity source sequence that Cisco ISE should use for authentication.

Step 5 In the Options area, you can define a further course of action that Cisco ISE should take if authentication fails, if the user is not found, or if there was a process failure. You can choose any one of the following options:

- Reject—A reject response is sent.
- Drop—No response is sent.
- Continue—Cisco ISE proceeds to evaluate the authorization policy.

Step 6 Click **Save** to save the simple authentication policy.

Result:

You should have a simple authentication policy that is configured using the RADIUS server sequence.

Configuring the Rule-Based Authentication Policy

This section contains:

- Understanding the Authentication Policy User Interface Elements, page 16-30
- Creating a Rule-Based Authentication Policy, page 16-36

Understanding the Authentication Policy User Interface Elements

To reach to the Rule-based Authentication policy user interface, complete the following tasks:

Step 1 Choose **Policy > Authentication**.

The Authentication Policy page appears.

Step 2 For the Authentication Method, click the **Rule-Based** radio button.

Figure 16-5 shows the rule-based authentication policy page, and Table 16-5 describes the rows in this page.

Figure 16-5 Rule-Based Authentication Policy User Interface Elements

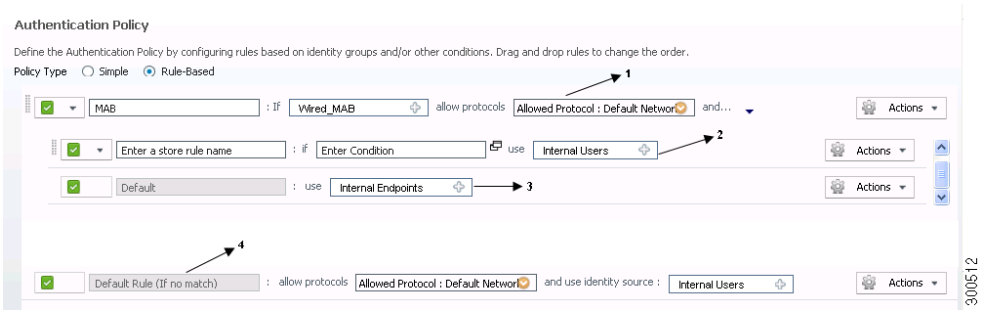


Table 16-5 Rule-Based Authentication Policy User Interface Elements

Callout No.	Description
1	This element is the first rule-based policy. This outer row contains conditions for determining the allowed protocols. You can create more than one outer row, each of which contains conditions for selecting the allowed protocols and identity sources. Each outer row must have one or more inner rows.
2	This element is the inner row, which defines the conditions for identity source selection. This row can contain simple or compound conditions. You can create any number of inner rows, each of which should be based on conditions for selecting identity sources.
3	This element is the default identity source that will be used for this policy when the conditions defined for the allowed protocols match those in the request, but the conditions defined for the identity source selection do not match. This row does not have any condition. It contains only the default identity source that Cisco ISE should use if the allowed protocols conditions match, but the identity source selection conditions do not match.
4	This element is the default allowed protocols and identity sources that will be used if none of the policies match the request. This row does not have any condition. It contains only the default allowed protocols and identity source selection that Cisco ISE should use.

This page contains the following fields:

- Status—The status can be one of the following:
  - Enabled—This policy condition is active.
  - Disabled—This policy condition is inactive and will not be evaluated.
  - Monitor Only—This policy condition will be evaluated, but the result will not be enforced. You can use this option for testing purposes. You can view the results of this policy condition in the monitoring and report viewer. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.
- Name—Name of the condition.
- Conditions—Conditions include the Condition Name or an Expression of type *attribute operand value*. You can create compound conditions using the AND or OR operators at the end of this row. You can create simple and compound conditions under the Policy Elements tab and refer to those conditions in these policies.

For more information:

See Understanding Authentication Policies and Configuring the Rule-Based Authentication Policy for more information.

Simple Conditions

Simple conditions consist of an attribute, an operator, and a value. You can create simple conditions from within the policy pages and also as separate policy elements that can be reused in policies. Cisco ISE allows you to create, edit, and delete simple authentication conditions. This page lists all the simple authentication policy conditions that you have defined in Cisco ISE. See the "Creating Simple Conditions" section on page 16-31 and the "Deleting Simple Conditions" section on page 16-32 for information on how to define simple conditions and delete them, respectively.

Related Topics

- Rule-Based Authentication Policies
- Understanding the Authentication Policy User Interface Elements

Creating Simple Conditions

Prerequisites:

- Before you begin this procedure, you should have a basic understanding of the Rule-Based Authentication Policies, the basic building blocks such as conditions and results, and how they are represented in the GUI. See the "Understanding the Authentication Policy User Interface Elements" section on page 16-30 for more information.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create simple conditions as separate policy elements, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 From the left navigation pane, click the greater-than sign (>) next to **Authentication**.

Step 3 From the left navigation pane, click **Simple Conditions**.

The Conditions page appears.

Step 4 Click **Add** to add a new condition.

Step 5 Enter the following information:

- Name—Enter the name of the reusable condition.
- Description—Enter an optional description for the condition.
- Attribute—Choose the attribute on which you want to build the condition. Click the drop-down arrow to choose the attribute from the dictionary.
- Operator—Choose the operator from the drop-down list box. This list box is populated only after you choose the attribute.
- Value—Choose a value from the drop-down list box. This list box is populated only after you choose the attribute.

Note For some attributes, you can enter the value.

Note If you specify any Identity Groups in simple conditions, ensure you represented them in FQDN form, like the following:

```
(InternalUser:IdentityGroup) : Equal : (UserIdentityGroups: Identity Group Name)
```

Cisco ISE will not accurately resolve Identity Group entries in the form `(InternalUser:IdentityGroup) : Equal : (Identity Group Name).`

Step 6 Click **Submit** to save the condition.

You can now use this condition in rule-based policies.

Next Step:

See the "Creating a Rule-Based Authentication Policy" section on page 16-36 for information on how to define a rule-based authentication policy using the simple conditions that you have created.

Deleting Simple Conditions

Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

- Ensure that the simple condition or conditions that you are about to delete are not referenced in any authentication policies.

To delete a simple authentication condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 From the left navigation pane, click the greater-than sign (>) next to **Authentication**.

Step 3 From the left navigation pane, click **Simple Conditions**.

The Conditions page appears with a list of simple conditions that you have defined.

Step 4 Check the check box next to the simple condition or conditions that you want to delete, then click **Delete**. Alternatively, you can choose the simple condition that you want to delete from the navigation pane on the left and click **Delete Simple Condition** from the action icon.

Note If you are trying to delete multiple simple conditions at the same time and if one of them is used in any authentication policy, then the entire delete operation will fail.

Cisco ISE prompts you with the following message:

Are you sure you want to delete?

Step 5 Click **OK** to delete the simple condition or conditions.

Compound Conditions

Compound conditions are made up of two or more simple conditions. You can create compound conditions as reusable objects from within the policy creation page or from the Conditions page. This page lists all the compound conditions that you have defined in Cisco ISE. See the "Creating Compound Conditions" section on page 16-33 and "Deleting Compound Conditions" section on page 16-35 for information on how to create compound conditions and delete them.

Related Topics

- Rule-Based Authentication Policies, page 16-5
- Understanding the Authentication Policy User Interface Elements, page 16-30

Creating Compound Conditions

Prerequisites:

- Before you begin this procedure, you should have a basic understanding of the Rule-Based Authentication Policies, the basic building blocks such as conditions and results, and how they are represented in the GUI. See the "Understanding the Authentication Policy User Interface Elements" section on page 16-30 for more information. You can create simple conditions that you can use in compound conditions.
- Cisco ISE comes with predefined compound conditions for some of the most common use cases. See the "Authentication Policy Built-In Configurations" section on page 16-38 for more information on these predefined conditions. You can edit these predefined conditions to suit your requirements.

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create a compound condition from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 From the Authentication navigation pane on the left, click **Compound Conditions**.

The Conditions page appears. This page lists any compound conditions that have been defined.

Step 3 Click **Add** to add a new compound condition.

Step 4 Enter a name for the compound condition. You can enter an optional description.

Step 5 Click **Select Existing Condition from Library** to choose an existing simple condition or click **Create New Condition** to choose an attribute, operator, and value from the expression builder.

a. If you have chosen to create a new condition, from the Select Attribute drop-down list box, choose an attribute from the dictionary based on which you want to create a condition.

b. After you have selected an attribute:

- Choose an operator (Equals, Not Equals, Matches, and so on) from the drop-down box.
- Choose the value from the drop-down list box, if available, or enter a value in the text box.
- To save this condition to be reused in other policies, click **Add Condition to Library** from the action icon that appears in the same row.
- Enter a name for this condition in the Condition Name text box and click the ( ) icon.

  The condition is saved as a simple condition and will be available for use in other policies.

Step 6 To add more conditions, click the action icon at the end of this row.

Step 7 Click **Add Attribute/Value** to create a new condition or click **Add Condition from Library** to add an existing simple condition.

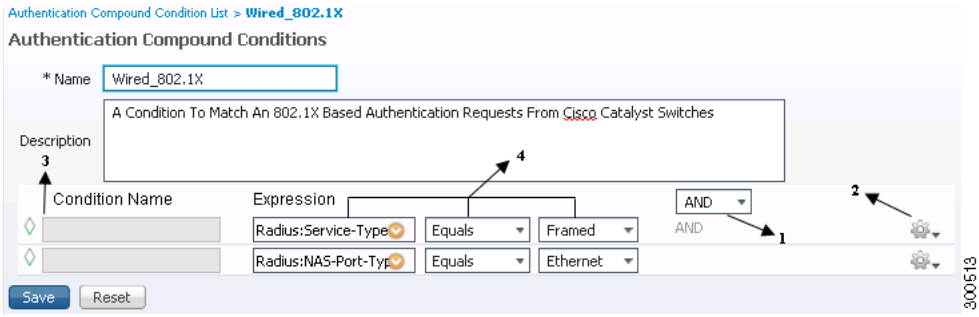
Step 8 Select the operand from the drop-down list box. You can choose either AND or OR and the same operand will be used between all the conditions in this compound condition.

Step 9 Repeat the process from Step 5 to add more conditions.

Step 10 After you have added all the conditions, click **Submit** to create this compound condition.

Figure 16-6 shows a compound conditions page. The table that follows the image provides a description of the user interface elements that appear in this page.

Figure 16-6 Compound Conditions Page



1	This element is the operand to be used between two or more conditions, and can be either AND or OR. For example, compound conditions can be of the following forms: *condition1* AND *condition2* AND *condition3*... or *condition1* OR *condition2* OR *condition3*...
2	You can click the action icon to do the following: • Add new conditions from the library. These are the conditions that you have already created. • Create a condition by adding a new attribute or value. • Duplicate an existing condition. • Add new conditions to the library. • Delete a condition. This option deletes the condition that appears in the same row as the action icon.
3	If you are creating a new condition, you can enter a name here to reuse this condition in other policies. When you provide a name here, this object is created as a separate condition.
4	Choose the attribute based on the reason you want to create the new condition. Choose the operator and the value in the text boxes.

Next Step:

See the "Creating a Rule-Based Authentication Policy" section on page 16-36 for information on how to define a rule-based authentication policy using the compound conditions that you created.

Deleting Compound Conditions

Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

- Ensure that the compound condition or conditions that you are about to delete are not referenced in any authentication policies.

To delete a compound authentication condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 From the left navigation pane, click the greater-than sign (>) next to Authentication.

Step 3 From the left navigation pane, click **Compound Conditions**.

The Conditions page appears with a list of simple conditions that you have defined.

Step 4 Check the check box next to the compound condition or conditions that you want to delete, then click **Delete**. Alternatively, you can choose the compound condition that you want to delete from the navigation pane on the left and click **Delete Compound Condition** from the action icon.

Note If you are trying to delete multiple compound conditions at the same time and if one of them is used in any authentication policy, then the entire delete operation will fail.

Cisco ISE prompts you with the following message:

Are you sure you want to delete?

Step 5 Click **OK** to delete the compound condition or conditions.

Creating a Rule-Based Authentication Policy

Timesaver We recommend that you create the allowed protocol access services, conditions, and identity source sequences before you create the rule-based authentication policy. If you want to use the RADIUS server sequence, you can define the RADIUS server sequence before you create the policy. See the "Proxy Service" section on page 16-21 for more information.

Prerequisites:

- Before you begin this task, you should have a basic understanding of the "Rule-Based Authentication Policies" section on page 16-5, have read the "Understanding the Authentication Policy User Interface Elements" section on page 16-30, and have completed the following tasks successfully:
  - Defining Allowed Protocols
  - Creating Identity Source Sequences if you want to use an identity source sequence
  - Defining a RADIUS Server Sequence if you want to use the RADIUS server sequence in place of the Allowed Protocols access service
- Cisco ISE comes with predefined rule-based authentication policies for the Wired 802.1X, Wireless 802.1X, and Wired MAB use cases. See the "Authentication Policy Built-In Configurations" section on page 16-38 for more information on these predefined policies. You can edit these policies to suit your requirements.

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Note When you switch between a simple and a rule-based authentication policy, you will lose the policy that you configured earlier. For example, if you have a simple authentication policy configured and you want to move to a rule-based authentication policy, you will lose the simple authentication policy. Also, when you move from a rule-based authentication policy to a simple authentication policy, you will lose the rule-based authentication policy.

To create a rule-based authentication policy, complete the following steps:

Note If your users are defined in external identity sources, ensure that you have configured these identity sources in Cisco ISE. See Chapter 5, "Managing External Identity Sources" for information on how to configure the external identity sources.

Step 1 Choose **Policy > Authentication**.

The Authentication Policy page appears.

Step 2 Click the **Rule-Based** radio button.

The following message appears:

You switched from single to rule-based result selection. Any settings saved in the single mode will be lost when you submit. Click OK to continue.

Step 3 Click **OK** to continue.

This page contains default rule-based policies.

Step 4 To create a new rule-based policy, click the action icon ( ) and click **Insert new row above** or **Insert new row below** based on where you want the new policy to appear in this list. The policies will be evaluated sequentially.

Each row in this rule-based policy page is equivalent to the simple authentication policy. Each row contains a set of conditions that determine the allowed protocols and identity sources.

Step 5 Click the **Status** drop-down list box to choose the status of this policy. The Status can be any one of the following:

- Enabled
- Disabled
- Monitor Only

Step 6 Enter a name for this policy. By default, it will be named Standard Policy 1, Standard Policy 2, and so on.

Step 7 In the Condition(s) area, click the Expand ( ) button.

Step 8 Click **Select Existing Condition from Library** or **Create New Condition** as described in Creating Compound Conditions.

Step 9 From the Allow Protocols drop-down list box, choose an allowed protocols service or a proxy service.

If you choose a proxy service, Cisco ISE forwards the request to the external policy server that is defined in the proxy service. The external policy server processes the request and returns the result to Cisco ISE. See the "Defining a RADIUS Server Sequence" section on page 16-25 for information on how to create a RADIUS server sequence.

You have created a condition for selecting the allowed protocols. You must then create a condition for selecting the identity source.

Step 10 Click ( ) next to the word "and" to define conditions for the identity source selection.

The default identity source rule appears next to the current row, but is indented.

Step 11 From the action icon in the default identity source row that is indented, click **Insert new row above**.

Step 12 Enter a name for your identity source rule.

Step 13 Click the button to define the conditions based on which you want to choose the identity source.

Step 14 Click **Select Existing Condition from Library** or **Create New Condition** as described in Creating Compound Conditions.

Step 15 Click the **Expand** button to choose the identity source sequence or the identity source.

a. Choose the identity source from the Identity Source List box.

b. Choose the action that you want Cisco ISE to take if authentication fails, if the user is not found, or if the process fails.

c. Click the **Collapse** button to complete your selection.

Step 16 Click the action icon in this inner row to add more conditions for identity source selection.

Step 17 You can edit the default identity source that you want Cisco ISE to use in case none of the identity sources defined in this rule match the request.

Step 18 Click the action icon in the outer row to add more rule-based policies. Repeat the process from Step 5.

Step 19 The last row in this policy page is the default policy that will be applied if none of the rules match the request. You can edit the allowed protocols and identity source selection for the default policy.

Note It is a good practice to choose Deny Access as the identity source in the default policy if the request does not match any of the other policies that you have defined.

Step 20 Click **Save** to save your rule-based authentication policies.

For more information:

See the "Understanding Authentication Policies" section on page 16-1.

Authentication Policy Built-In Configurations

The Cisco ISE software comes with several built-in configurations that are part of common use cases. These built-in configurations are called defaults. Table 16-6 describes the defaults that relate to authentication policies.

Table 16-6 Authentication Policy Configuration Defaults

Name	Path in the UI	Description	Additional Information
Default Network Access Allowed Protocols Access Service	Policy > Policy Elements > Configuration > Allowed Protocols	This default is the built-in network access allowed protocols service to be used in authentication policies.	You can use this access service for wired and wireless 802.1X, and wired MAB authentication policies.
Wired 802.1X Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Framed • RADIUS:NAS-Port-Type equals Ethernet	This compound condition is used in the wired 802.1X authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wired 802.1X authentication policy.
Wireless 802.1X Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Framed • RADIUS:NAS-Port-Type equals Wireless-IEEE802.11	This compound condition is used in the wireless 802.1X authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wireless 802.1X authentication policy.
Wired MAB Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Call-Check • RADIUS:NAS-Port-Type equals Ethernet	This compound condition is used in the wired MAB authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wired MAB authentication policy.

Table 16-6 Authentication Policy Configuration Defaults (continued)

Name	Path in the UI	Description	Additional Information
Catalyst Switch Local Web Authentication Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Outbound • RADIUS:NAS-Port-Type equals Ethernet	To use this compound condition, you must create an authentication policy that would check for this condition. See Configuring the Rule-Based Authentication Policy for more information. You can also define an access service based on your requirements or use the default network access allowed protocols service for this policy. SeeNetwork Access Service for more information.
Wireless Lan Controller (WLC) Local Web Authentication Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Outbound • RADIUS:NAS-Port-Type equals Wireless-IEEE802.11	To use this compound condition, you must create an authentication policy that would check for this condition. See Configuring the Rule-Based Authentication Policy for more information. You can also define an access service based on your requirements or use the default network access allowed protocols service for this policy. SeeNetwork Access Service for more information.
Wired 802.1X Authentication Policy	Policy > Authentication > Rule-Based	This policy uses the wired 802.1X compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wired 802.1X compound condition.	This default policy uses the internal endpoints database as its identity source. You can edit this policy to configure any identity source sequence or identity source based on your needs.

Table 16-6 Authentication Policy Configuration Defaults (continued)

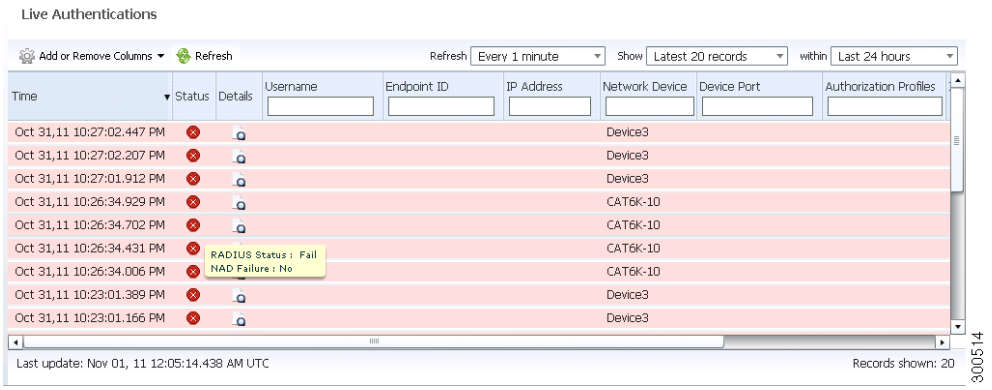
Name	Path in the UI	Description	Additional Information
Wireless 802.1X Authentication Policy	Policy > Authentication > Rule-Based	This policy uses the wireless 802.1X compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wireless 802.1X compound condition.	This default policy uses the internal endpoints database as its identity source. You can edit this policy to configure any identity source sequence or identity source based on your needs.
Wired MAB Authentication Policy	Policy > Authentication > Rule-Based	This policy uses the wired MAB compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wired MAB compound condition.	This default policy uses the internal endpoints database as its identity source.

Viewing Authentication Results

The Cisco ISE dashboard provides a summary of all authentications that take place in your network. To view real-time authentication summary, choose **Operations > Authentications**. A screen similar to the one shown in Figure 16-7 appears.

Note Every Cisco ISE administrator account is assigned one or more administrative roles. To view the reports in Cisco ISE, you must have one of the following roles assigned: Super Admin or Helpdesk Admin or Monitoring Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

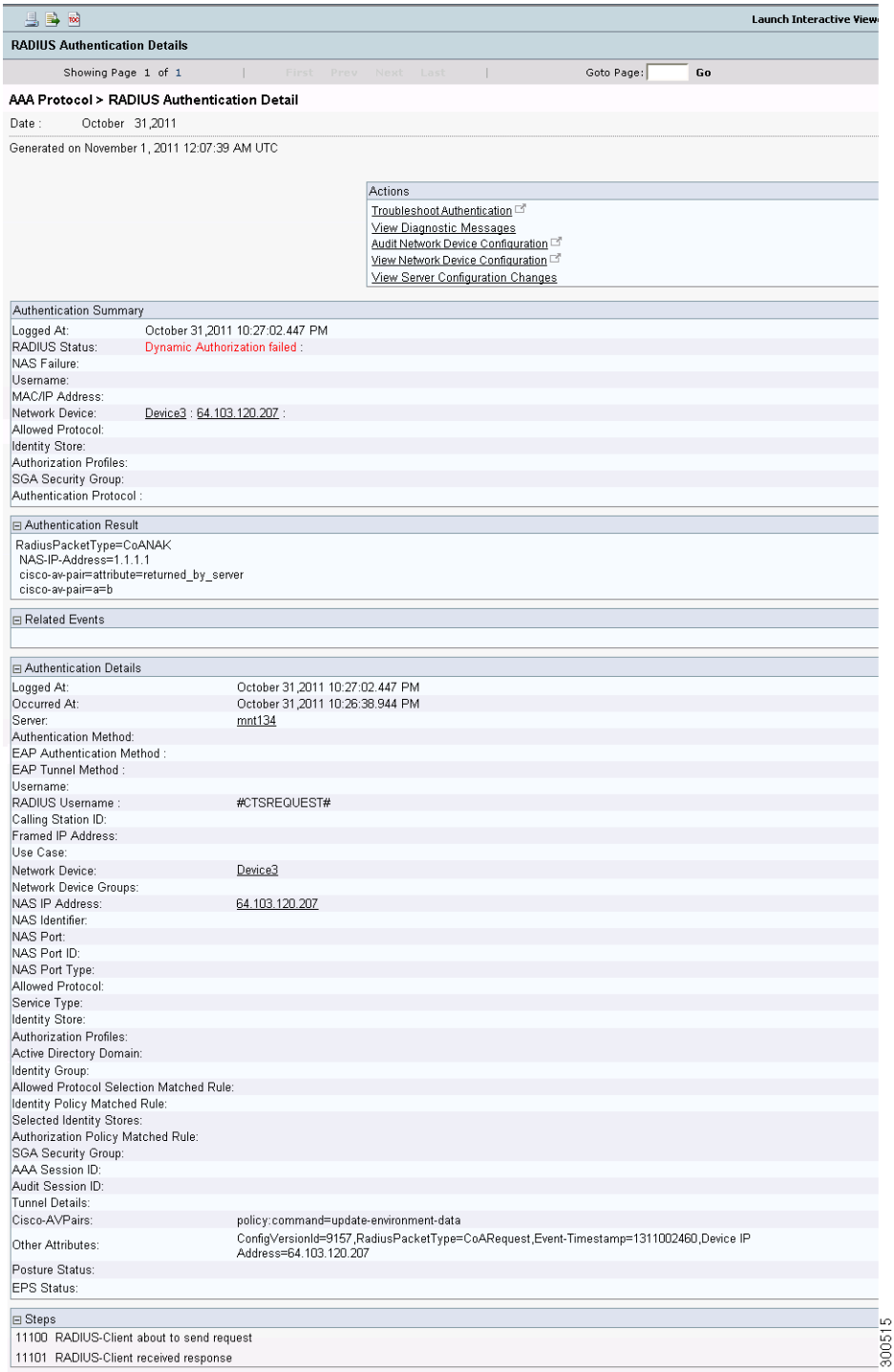
Figure 16-7 Authentications Screen



You can move your mouse over the Status icon to view the results of the authentication and a brief summary. A pop-up that is similar to the one shown in Figure 16-7 appears.

To filter your results, enter your search criteria in any one or more of the text boxes that appear at the top of the list, and press **Enter**. You can click the magnifier icon under the Details column to view a detailed report, as shown in Figure 16-8.

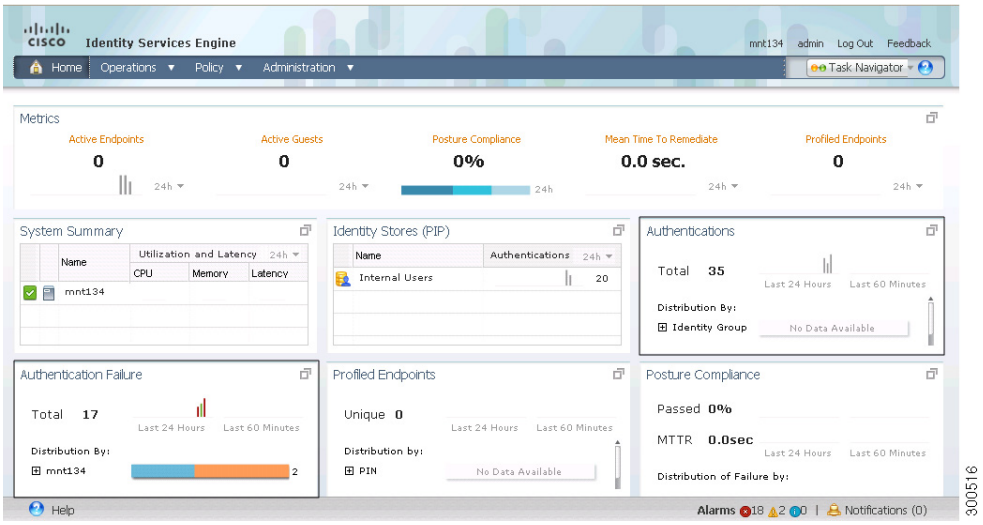
Figure 16-8 Detailed Authentication Summary Report



Cisco ISE also provides at-a-glance information about authentications and authentication failures in the form of dashlets that appear on the Cisco ISE dashboard.

Figure 16-9 shows the Cisco ISE dashboard.

Figure 16-9 Cisco ISE Dashboard



The Authentications and Authentication Failure dashlets provide the following statistical information about the RADIUS authentications that Cisco ISE has handled:

- The total number that appears in the Authentications dashlet is the total number of RADIUS authentication requests that Cisco ISE has handled including passed authentications, failed authentications, and simultaneous logins by the same user.
- The total number that appears in the Authentication Failure dashlet is the total number of failed RADIUS authentications requests that Cisco ISE has processed.

For information on dashboard and dashlets and how to drill down to look for more information, see Chapter 2, "Introducing the Dashboard" and Chapter 23, "Cisco ISE Dashboard Monitoring."

Apart from the authentication details, Cisco ISE provides various reports and troubleshooting tools that you can use to efficiently manage your network.

Table 16-7 provides a list of reports that you can run to understand the authentication trend and traffic in your network. You can generate reports for historical as well as current data.

Table 16-7 List of Reports

Report
AAA Protocol Reports
AAA Diagnostics
Authentication Trend
RADIUS Accounting
RADIUS Authentication
Allowed Protocol Reports
Allowed Protocol Authentication Summary

Table 16-7 List of Reports (continued)

Report
Top *N* Authentications By Allowed Protocol
Server Instance Reports
Server Authentication Summary
Top *N* Authentications By Server
Endpoint Reports
Endpoint MAC Authentication Summary
Top *N* Authentications By Endpoint MAC Address
Top *N* Authentications By Machine
Failure Reason Reports
Authentication Failure Code Lookup
Failure Reason Authentication Summary
Top *N* Authentications By Failure Reason
Network Device Reports
Network Device Authentication Summary
Top *N* Authentications By Network Device
User Reports
Top *N* Authentications By User
User Authentication Summary
Session Directory Reports
RADIUS Active Sessions
RADIUS Session History
RADIUS Terminated Sessions

For more information on how to generate reports and work with the interactive viewer, see Chapter 24, "Reporting."



CHAPTER 17

Managing Authorization Policies and Profiles

This chapter introduces the authorization policies that are used when creating the authorization profiles in the Cisco Identity Services Engine (ISE). Using the ISE user interface menus, tabs, and options, you can create an authorization policy, which form the basis of authorization profiles.

An authorization policy is where an overall authorization policy is generated, which is composed of authorization rules. Authorization rules have three elements: name, attributes, and permissions. It is the permissions function that maps to an authorization profile.

This chapter provides a description of authorization policies and provides example procedures for the following authorization policy-related tasks:

- Understanding Authorization Policies, page 17-1
- Cisco ISE Authorization Policies and Profiles, page 17-5
- Configuring Authorization Policies, page 17-14
- Configuring Policy Elements Conditions, page 17-17
- Configuring Permissions for Authorization Profiles, page 17-27

Understanding Authorization Policies

Authorization policies are a component of the Cisco ISE network authorization service that allows you to define authorization policies and configure authorization profiles for specific users and groups of users that access your network resources.

Network authorization policies associate rules with specific user and group identities to create the corresponding profiles. Whenever these rules match the configured attributes, the corresponding authorization profile that grants permission is returned by the policy, network access is authorized accordingly.

Authorization policies can contain conditional requirements that combine one or more identity groups using a compound condition that includes authorization checks that can return one or more authorization profiles. In addition, conditional requirements can exist apart from the use of a specific identity group (such as in using the default “Any”). Cisco ISE is an attribute-based policy system, with identity groups being one of the many important attributes.

For example, authorization profiles can include a range of permissions that are contained in the following types:

- Standard profiles
- Exception profiles
- Device-based profiles

Profiles consist of attributes chosen from a set of resources, which are stored in a dictionary and these are returned when the compound condition for the specific authorization policy matches. Because authorization policies can include compound conditions mapping to a single network service rule, these can also include a list of authorization checks.

For simple scenarios, all authorization checks are made using the AND Boolean operator within the rule. For advanced scenarios, any type of authorization verification expression can be used, but all these authorization verifications must comply with the authorization profiles to be returned. Authorization verifications typically comprise one or more conditions, including a user-defined name that can be added to a library, which can then be reused by other authorization policies.

For more information:

- For information about policy terminology, see Understanding Authorization Policy Terminology, page 17-2.
- For policy and profile information, see Cisco ISE Authorization Policies and Profiles, page 17-5.
- For information about configuring policies, see Configuring Authorization Policies, page 17-14.
- For information about configuring policy elements conditions, see Configuring Policy Elements Conditions, page 17-17.
- For information about configuring permissions for profiles, see Configuring Permissions for Authorization Profiles, page 17-27.
- For information about configuring permissions for DACLs, see Configuring Permissions for Downloadable ACLs, page 17-33.

Understanding Authorization Policy Terminology

Table 17-1 defines and describes basic terminology for Cisco ISE authorization policies and profiles.

Table 17-1 Cisco ISE Basic Authorization Policy and Profile Terminology

Term	Description
Network Authorization	Authorization is an important requirement to ensure which users can access the Cisco ISE network and its resources. Network authorization controls user access to the network and its resources and what each user can do on the system with those resources. The Cisco ISE network defines sets of permissions that authorize read, write, and execute privileges. Cisco ISE lets you create a number of different authorization policies to suit your network needs. This release supports only Remote Authentication Dial-In User Service (RADIUS) access to the Cisco ISE network and its resources.
Policy Elements	Policy elements are components that define the authorization policy. The policy elements are as follows: • Rule name • Identity groups • Condition(s) • Permissions These policy elements are referenced when you create policy rules and your choice of conditions and attributes can create specific types of authorization profiles.
Authorization Profile	An authorization profile acts as a container where a number of specific permissions allow access to a set of network services. The authorization profile is where you define a set of permissions to be granted for a network access request and can include: • A profile name • A profile description • An associated DACL • An associated VLAN • An associated SGACL • Any number of other dictionary-based attributes

Table 17-1 Cisco ISE Basic Authorization Policy and Profile Terminology (continued)

Term	Description
Authorization Policy	An authorization policy can consist of a single rule or a set of rules that are user-defined. These rules act to create a specific policy. For example, a standard policy can include the rule name using an If-Then convention that links a value entered for identity groups with specific condition(s) or attributes to produce a specific set of permissions that create a unique authorization profile. There are two authorization policy options you can set: • First Matched Rules Apply • Multiple Matched Rule Applies These two options direct Cisco ISE to use either the first matched or the multiple matched rule type listed in the standard policy table when it matches the user's set of permissions. These are the two types of authorization policies that you can configure: • Standard • Exception Standard policies are policies created to remain in effect for long periods of time, to apply to a larger group of users or devices or groups, and allow access to specific or all network endpoints. Standard policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges. Standard policies can be used as templates in which you modify the original values to serve the needs of a specific identity group, using specific conditions or permissions to create another type of standard policy to meet the needs of new divisions, or groups of users, devices, or groups in your network. By contrast, exception policies are appropriately named because this type of policy acts as an exception to the standard policies. Exception polices are intended for authorizing limited access that is based on a variety of factors (short-term policy duration, specific types of network devices, network endpoints or groups, or the need to meet special conditions or permissions or an immediate requirement). Exception policies are created to meet an immediate or short-term need such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users. This allows you to create different or customized policies to meet your corporate, group, or network needs.
Access Control Lists	An ACL on the Cisco ISE system is a list of permissions attached to a specific object or network resource. An ACL specifies which users or groups are granted access to an object, as well as what operations are allowed on a given object or network resource. Each entry in a typical ACL specifies a subject and an operation or provides the state (for example, Permit or Deny). A DACL represents a downloadable ACL.

Cisco ISE Authorization Policies and Profiles

This section describes the authorization policies and authorization profiles used in Cisco ISE. Using the Cisco ISE user interface (Authorization Policy and Authorization Profile windows), you can manage all of your authorization policies and profiles by performing the following policy management operations:

- Displaying existing policies
- Creating new policies
- Duplicating existing policies (for use as templates that you can modify to create new policies)
- Modifying existing policies (create customized policies by changing desired rules or permissions)
- Deleting existing policies

For more information:

Descriptions of the components and elements in the Authorization Policy and Authorization Profile windows that you use to create policies and profiles are in the following topics:

- For information about the user interface elements you can use to create authorization policies, see Authorization Policy Window, page 17-5 and Authorization Policy and Profile User Interface, page 17-10.
- For information about the user interface elements you can use to create authorization profiles, see Authorization Profile Window, page 17-8 and Authorization Policy and Profile User Interface, page 17-10.
- For guidelines about creating authorization policies and profiles, see Authorization Policy and Profile Guidelines, page 17-9.

Next Steps:

To configure authorization policies and profiles, see the following topics:

- Configuring Authorization Policies, page 17-14
- Configuring Policy Elements Conditions, page 17-17
- Configuring Permissions for Authorization Profiles, page 17-27
- Configuring Permissions for Downloadable ACLs, page 17-33

Authorization Policy Window

To display the Authorization Policy window, you start from the Authorization tab (choose **Policy > Authorization**). The Authorization Policy window is your starting point for creating the following types of Cisco ISE authorization policies:

- Exception: Exception policies are, like the name implies, exceptions to a standard policy, which is designed for use by large numbers of users or groups, or to remain in effect for an extended period. Exception policies are instead designed for a custom purpose, for a short period of time, or for use by one or more users or a group for a specific purpose.
- Standard: Standard policies are those that you create for use for an extended period of time, by large numbers of users or groups, and that provide a standard set of permissions and rules tailored for standard network needs.

Note The Cisco ISE user interface provides a Status indicator for each authorization policy that can be set to display one of the three following states: Enabled, Disabled, or Monitor Only.

When managing authorization polices, you can display existing exception or standard policies, or create, modify, or delete these policies to meet specific user or group requirements in your network. To create a new Exception or Standard authorization policy, you need to complete the following sequence of tasks to configure these following four policy element values:

- Rule Name—This where you define a unique name for the authorization policy.
- Identity Groups—This is where you select an existing identity group from a list of available choices.
- Other Conditions—This is where you select a simple condition (or a compound condition) from existing Condition Name dictionary choices (or you can select an attribute from existing Attribute dictionary choices).
- Permissions—This is where you select a profile from an existing Profiles dictionary choices.

You can create a new authorization policy by choosing and combining values for these four policy elements using the Cisco ISE user interface menus and options in the Authorization Policy window. Once you have selected your policy choices, click **Done**.

The policies that you create appear in the Authorization Policy page in a read-only mode.

You can click the **Edit** link in the authorization policy to edit the policy rules. After you have modified your policy choices, click **Done**.

When you add a new policy or edit an existing policy, a pencil icon appears next to the rule name. The pencil icon indicates that there are unsaved changes to the authorization policy. You must click **Save** to save your changes in the Cisco ISE system database.

Authorization policy rules are grouped by rank in the list, and you can change the position of rules in this ranked list by using the following options:

- Insert a new policy above or below a highlighted or selected policy.
- Insert a duplicate of a selected policy above or below a highlighted or selected policy.
- Delete a selected policy.

You can also drag and drop rules to change their rank in the list.

When you create a new authorization policy, it is populated with default values for all of the required policy fields. You will be prompted to do the following:

- To modify an existing authorization policy, choose any policy element you want to change, modify its value, and click **Save** to create the modified policy in the Cisco ISE system database.
- To delete an existing authorization policy, select it in the displayed list, and click **Delete** to remove this policy from the Cisco ISE system database. Normally, you would delete only those authorization policies that you no longer intend to support or use as templates for future policies.

Note When you delete an existing authorization policy, Cisco ISE prompts you to confirm the deletion before the selected policy is deleted from the Cisco ISE system database. Any changes that you make to a policy without clicking **Save** are not sent to or registered on the Cisco ISE system database.

- To duplicate an existing policy, select its intended position (above or below) in the ranked list. Cisco ISE copies all of the policy values from the existing policy, and creates an identical policy except that it now has a different policy ID (Cisco ISE requires each policy ID to be unique). By starting with a duplicate of an existing policy, you can use it as a template, modify selected fields or attributes, and create a new authorization policy.

Note You can set each exception or standard authorization policy that you create as **Enabled**, **Disabled**, or **Monitor Only**. To do this, choose the corresponding pull-down option in the green check box adjacent to the Rule Name column for each entry.

- To reuse a valid attribute when creating authorization policy conditions, select it from a dictionary that contains the supported attributes. For example, Cisco ISE provides an attribute named AuthenticationIdentityStore, which is located in the NetworkAccess dictionary. This attribute identifies the last identity source that was accessed during the authentication of a user:
  - When a single identity source is used during authentication, this attribute includes the name of the identity store to which the authentication succeeded.
  - When an identity source sequence is during authentication, this attribute includes the name of the last identity source accessed.

  You can use the AuthenticationStatus attribute in combination with the AuthenticationIdentityStore attribute to define a condition that identifies the identity source to which a user has successfully been authenticated. For example, to check for the a Condition where a user authenticated using an LDAP directory (LDAP13) in the authorization policy, you can define the following reusable condition:

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

Note The AuthenticationIdentityStore represents a text field that allows you to enter data for the condition. Ensure that you enter or copy the name correctly into this field. If the name of the identity source changes, you must ensure to modify this condition to match the change to the identity source.

- To define authorization conditions that are based on an endpoint identity group that has been previously authenticated, Cisco ISE supports authorization that was defined during endpoint identity group 802.1X authentication status. When Cisco ISE performs 802.1X authentication, it extracts the MAC address from the “Calling-Station-ID” field in the RADIUS request and uses this value to look up and populate the session cache for the device's endpoint identity group (defined as an endpointIDgroup attribute).

  This process makes the endpointIDgroup attribute available for use in creating authorization policy conditions, and allows you to define an authorization policy based on endpoint identity group information using this attribute, in addition to user information.

  The condition for the endpoint identity group can be defined in the ID Groups column of the authorization policy configuration page. Conditions that are based on user-related information need to be defined in the “Other Conditions” section of the authorization policy. If user information is based on internal user attributes, then use the ID Group attribute in the internal user dictionary. For example, you can enter the full value path in the identity group using a value like “User Identity Group:Employee:US”.

For more information:

- For more information on endpoint identity groups, see Endpoint Identity Groups, page 4-70.

Authorization Policies and Supported Dictionaries

For simple condition-based policy scenarios, authorization checks are made using the AND Boolean operator within the rule. For compound condition-based policies, any type of authorization verification expression can be used. However, for both authorization policy types the verification must comply with the authorization profiles to be returned.

Verifications typically include one (or more) condition(s) that include a user-defined name that can then be added to a library and reused by other policies. You define conditions using the attributes from the Cisco ISE dictionary, which supports the following dictionaries:

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft
- RADIUS

where RADIUS is a system-defined dictionary and Airespace, Cisco, Cisco-BBSM, Cisco-VPN3000, and Microsoft are RADIUS-vendor dictionaries. See the "Dictionaries and Dictionary Attributes" section on page 7-1 for more information on Cisco ISE dictionaries.

Authorization Profile Window

To display the Authorization Profile window, you start from the Policy tab (choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**). The Authorization Profile window is your starting point for managing the Cisco ISE standard authorization profiles. This is where you can display any existing profiles, create new profiles, or modify or delete existing authorization profiles to meet your specific user or group network needs.

To create a new authorization profile, you must define the profile name and access type. All other profile elements are optional. To configure values for these other profile elements, use the text fields, drop-down lists, and check boxes in the following Authorization Profile page panels:

- **Authorization Profile**
  - Name
  - Description
  - Access Type

Note The only profile elements required to create a new authorization profile are the profile Name and Access Type, which are marked with an asterisk (*). All other profile elements are optional elements.

- **Common Task**s

  This is where you can configure settings that support commonly-used attributes.
  - DACL Name
  - VLAN
  - Voice Domain Permission

  - Posture Discovery
  - Centralized Web Authentication
  - Auto SmartPort
  - Filter-ID
  - Reauthentication
  - MACSec Policy
  - NEAT
  - Web Authentication (Local Web Auth)
  - Wireless LAN Controller (WLC)
  - ASA VPN

Note For details about Common Task settings, see Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28.

- **Advanced Attributes Settings**

  This is where you can configure advanced attributes settings using attributes contained in dictionaries you can access from the drop-down list.

- **Attributes Details**

  This is where the attributes you configure in the Common Settings and Advanced Attribute panes are displayed.

After you have selected or entered your authorization profile choices, click **Submit** to create a new authorization profile.

To modify an existing authorization profile, select the check box corresponding to the profile you want to change, modify the profile settings as desired, and click **Save** to create a new modified authorization profile. Any changes that you make to a profile without clicking **Save** are not sent to or registered on the Cisco ISE system database.

To delete an existing authorization profile, select the check box corresponding to the profile you want to delete, and click **Delete**. For the procedures explaining how to create, modify, or delete authorization profiles, see Configuring Permissions for Authorization Profiles, page 17-27.

Authorization Policy and Profile Guidelines

Observe the following guidelines when managing or administering authorization polices and profiles:

- Rule Names you create must use only the following supported character set:
  - Symbols: plus (+), hyphen (-), underscore (_), period (.), and a space ( ).
  - Alphabetic characters: A-Z and a-z.
  - Numeric characters: 0-9.
- Identity Groups default to “Any” (you can use this global default to apply to all users).
- Conditions allow you to set one or more policy values. However, conditions are optional and are not required to create an authorization policy. These are the two methods for creating conditions:
  - Choose an existing condition or attribute from a corresponding dictionary of choices.

  - Create a custom condition that allows you to select a suggested value or use a text box to enter a custom value.
- Condition names you create must use only the following supported character set:
  - Symbols: hyphen (-), underscore (_), and period (.).
  - Alphabetic characters: A-Z and a-z.
  - Numeric characters: 0-9.
- Permissions are important when choosing an authorization profile to use for a policy. A permission can grant access to specific resources or allow you to perform specific tasks. For example, if a user belongs to a specific identity group (such as Device Admins), and the user meets the defined conditions (such as a site in Boston), then this user is granted the permissions associated with that group (such as access to a specific set of network resources or permission to perform a specific operation on a device).

Note Make sure that you click **Save** to save the new or modified policy or profile in the Cisco ISE database.

Authorization Policy and Profile User Interface

To manage your authorization policies and authorization profiles, use the controls within each of the corresponding user interface windows. The following list identifies the Cisco ISE user interface controls and elements needed to perform the following tasks:

- To configure an authorization policy—choose **Policy > Authorization > Standard** (or **Exception**)
- To configure an authorization profile—choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**

Authorization Policy, Rule, and Profile Configuration Defaults

The Cisco ISE software comes installed with a number of pre-installed default conditions, rules, and profiles that provide common settings that make it easier for you to create the rules and policies required in Cisco ISE authorization policies and profiles. These built-in configuration defaults contain specified values that are described in Table 17-2.

Table 17-2 Authorization Policy, Profile, and Rule Configuration Defaults

Name	Path in the UI	Description	Additional Information
Authorization Policy Configuration Defaults			
Default Compound Conditions for Authorization Policies	**Policy > Policy Elements > Conditions > Authorization**	These are pre-installed configuration defaults for conditions, rules, and profiles to be used in authorization policies.	You can use the related attributes for creating authorization policies: • Wired 802.1x • Wired MAB • Wireless 802.1x • Catalyst Switch Local Web authentication • WLC Web authentication

Table 17-2 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the UI	Description	Additional Information
Authorization Policy Configuration Defaults			
Wired 802.1X Compound Condition	**Policy > Policy Elements > Conditions > Authorization > Compound Conditions**	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Ethernet	This compound condition is used in the Wired 802.1X authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wired 802.1X authorization policy.
Wired MAB Compound Condition	**Policy > Policy Elements > Conditions > Authorization > Compound Conditions**	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Call-Check • RADIUS:NAS-Port-Type = Ethernet	This compound condition is used in the Wired MAB authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wired MAB authorization policy.
Wireless 802.1X Compound Condition	**Policy > Policy Elements > Conditions > Authorization > Compound Conditions**	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Framed • RADIUS:NAS-Port-Type = Wireless-IEEE802.11	This compound condition is used in the Wireless 802.1X authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wireless 802.1X authorization policy.
Catalyst Switch Local Web Authentication Compound Condition	**Policy > Policy Elements > Conditions > Authorization > Compound Conditions**	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Ethernet	To use this compound condition, you need to create an authorization policy that would check for this condition.
Wireless Lan Controller (WLC) Local Web Authentication Compound Condition	**Policy > Policy Elements > Conditions > Authorization > Compound Conditions**	This compound condition checks for the following attributes and values: • RADIUS:Service-Type = Outbound • RADIUS:NAS-Port-Type = Wireless-IEEE802.11	To use this compound condition, you must create an authorization policy that would check for this condition.

Table 17-2 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the UI	Description	Additional Information
Authorization Rule Configuration Defaults			
Profiled Cisco IP Phone Authorization Rule	**Policy > Authorization Policy**	This authorization policy uses a configuration default rule with the following values: • Rule Name: Profiled Cisco IP Phones • Endpoint Identity Group: Cisco IP Phones • Conditions: Any • Authorization Profile: Cisco IP Phones This authorization policy will evaluate requests that match the criteria specified in this policy.	This default rule uses Cisco IP Phones as its default endpoint identity group and the values listed in this table.
Default Authorization Rule	**Policy > Authorization Policy**	This authorization policy uses a configuration default rule with the following values: • Rule Name: Default • Endpoint Identity Group: Any • Conditions: Any • Authorization Profile: PermitAccess This authorization policy will evaluate requests that match the criteria specified in this policy.	This default rule uses "any" as its default endpoint identity group and the values listed in this table.
Authorization Profile Configuration Defaults			
Default Authorization Profile	**Policy > Policy Elements > Permissions > Authorization Profiles > Standard**	This authorization profiles uses a configuration default profile with the following values: • Name: Cisco IP Phones • DACL: PERMIT_ALL_TRAFFIC • VSA: cisco:av-pair:device-traffic-class=voice This profile will evaluate requests that match the criteria specified in this profile.	This default authorization profile uses the DACL and vendor-specific attribute (VSA) to authorize all "voice" traffic (PERMIT_ALL_TRAFFIC).

Configuring Authorization Policies

The Authorization Policy window lets you display, create, duplicate/modify, or delete authorization policies. The following topics provide procedures for performing these tasks:

- Displaying Existing Authorization Policies, page 17-14
- Creating a New Authorization Policy, page 17-14
- Duplicating and Modifying an Existing Authorization Policy, page 17-16
- Deleting an Existing Authorization Policy, page 17-17

Note The following authorization policy profile sections reference example actions directed at a standard authorization policy. You can follow the same process for managing an exception authorization policy.

Displaying Existing Authorization Policies

Use this procedure to display all existing Exception or Standard authorization policies, choose the matched rule policy, or view the policy-based choices that can be made.

To display existing authorization policies, complete the following steps:

Step 1 Choose **Policy > Authorization.**

The Authorization Policy window appears listing all existing configured authorization policies.

Note When performing this action initially, there will be only be a Default rule displayed and you are limited to one policy-based option (using Insert New Rule Above).

Step 2 Click **action** (icon), which displays a drop-down list with the following policy-based choices:

- Insert New Rule Above
- Insert New Rule Below
- Duplicate Above
- Duplicate Below
- Delete

Note To set the matched rule policy for authorization policies, under Authorization Profiles click the drop-down arrow, and choose **First Matched Rule Applies** or **Multiple Matched Rule Applies**.

Creating a New Authorization Policy

Use this procedure to create a new authorization policy.

To create a new authorization policy, complete the following steps:

Step 1 Choose **Policy > Authorization > Standard**.

Step 2 Click to select either **Insert New Rule Above** or **Insert New Rule Below**.

A new policy entry appears in the position you designated in the Standard panel of the Authorization Policy window.

Step 3 Enter values for the following authorization policy fields:

- Rule Name—You need to define a rule name for the new policy.
- Identity Groups—Choose a name for the identity group that you want associated with the policy.
  - Click **+** ("plus" sign) next to the word "Any" to display a drop-down list of group choices, or choose **Any** for the policy for this identity group to include all users.
- Condition(s)—Choose the types of conditions or attributes for the identity group associated with the policy. Click **+** next to Condition(s) to display the following list of condition and attribute choices that you can configure:
  - Select a Condition Name option from the drop-down list (**Simple Conditions**, **Compound Conditions**, or **Time and Date Conditions**) as needed.
  - Select one of the Attribute options as needed. This displays a list of dictionaries that contain specific attributes related to the dictionary type.

    When you select an attribute, you can define it as Equals, Not Equals, or Matches using a pull-down list of operator options, and select an AND or OR directive using a pull-down directive option.

Note Not all attributes you select will include the Equals, Not Equals, and Matches operator options.

Note The "Matches" operator supports and uses regular expressions (REGEX) not wildcards.

Example 1a: Equals—You select the RADIUS dictionary, and you select the Error-Cause value, which displays RADIUS:Error-Cause in the Expression field. You select the Equals operator in the second field (pull-down list). In the third field (pull-down list), you select the value that you want the RADIUS:Error-Cause to equal (for example, Unsupported Service). This condition is configured as follows: RADIUS:Error-Cause EQUALS Unsupported Service.

Example 1b: Equals—You select the CERTIFICATE dictionary, and you select the Subject value, which displays CERTIFICATE:Subject in the Expression field. You select the Equals operator in the second field (pull-down list). In the third field (text field), you must configure the value properly that you want the CERTIFICATE:Subject to equal (for example, a username such as User123). To achieve a match, this condition must be configured using the prefix of "cn=" as follows: CERTIFICATE:Subject EQUALS cn=User123.

Example 1c: Equals—You select the CERTIFICATE dictionary, and you select the Subject Alternative Name value, which displays CERTIFICATE:Subject Alternative Name in the Expression field. You select the Equals operator in the second field (pull-down list). In the third field (text field), you must configure the value properly that you want the CERTIFICATE:Subject Alternative Name to equal (for example, a username such as User123@acme.com). To achieve a match, this condition must be configured as follows: CERTIFICATE:Subject Alternative Name EQUALS User123@acme.com.

Example 2: Not Equals—You select the RADIUS dictionary, and you select the User-Name value, which displays RADIUS:User-Name in the Expression field.You select the Not Equals operator in the second field (pull-down list). In the third field (text box), you enter the value that you want the RADIUS:User-Name to not equal (for example, guest113). This condition is configured as: RADIUS:User-Name NOT_EQUALS guest113.

Example 3: Matches—You select the CERTIFICATE dictionary, and you select the Organization value, which displays CERTIFICATE:Organization in the Expression field. You select the Matches operator in the second field (pull-down list). In the third field (text box), you enter a REGEX value to match Organization value. The following are some common options for "Matches:

- 'Starts with'—for example, using the REGEX value of ^(Acme).*—this condition is configured as CERTIFICATE:Organization MATCHES 'Acme' (any match with a condition that starts with "Acme").
- 'Ends with'—for example, using the REGEX value of .*(mktg)$—this condition is configured as CERTIFICATE:Organization MATCHES 'mktg' (any match with a condition that ends with "mktg").
- 'Contains'—for example, using the REGEX value of .*(1234).*—this condition is configured as CERTIFICATE:Organization MATCHES '1234' (any match with a condition that contains "1234", such as Eng1234, 1234Dev, and Corp1234Mktg).
- 'Does not start with'—for example, using the REGEX value of ^(?!LDAP).*—this condition is configured as CERTIFICATE:Organization MATCHES 'LDAP' (any match with a condition that does not start with "LDAP", such as usLDAP or CorpLDAPmktg).

- Permissions—Choose the authorization profile to associate with this authorization policy.
  - Click **+** next to Permissions to display a drop-down list of profile choices. Select a profile option (for example, the Standard profile offers two default choices: DenyAccess or PermitAccess).

d. Click **Done**.

Step 4 Click **Save** to save your changes to the Cisco ISE system database and create this new authorization policy.

Duplicating and Modifying an Existing Authorization Policy

Use this procedure to duplicate an existing authorization policy and modify it to create a new policy based upon its initial set of existing values.

To duplicate and modify an existing authorization policy, complete the following steps:

Step 1 Choose **Policy > Authorization > Standard**.

Step 2 To choose the authorization policy you want to duplicate and modify, click **action** (icon) for that policy row and select **Duplicate above** or **Duplicate below**.

A duplicate policy entry appears in the Standard panel of the Authorization Policy window (either above or below the existing policy that you selected).

Step 3 Enter a new name for this policy in the Rule Name field.

Step 4 Modify the desired values to create the new authorization policy in the corresponding fields by selecting the desired set of option choices.

Step 5 Click **Save** to save your changes to the Cisco ISE database, which creates this new authorization policy.

Deleting an Existing Authorization Policy

Use this procedure to delete an existing authorization policy and remove it from the Cisco ISE database.

To delete an existing authorization policy, complete the following steps:

Step 1 Choose **Policy > Authorization > Standard**.

Step 2 To select the authorization policy you want to delete, click **action** (icon) for that policy row and choose **Delete**.

A confirmation dialog appears in the Standard panel of the Authorization Policy window.

Step 3 Click **Delete** to confirm that you want to delete the authorization policy.

Step 4 Click **Save** to save your changes to the Cisco ISE system database and delete this authorization policy.

Note If you do not click **Save**, you will only delete the authorization policy locally.

Configuring Policy Elements Conditions

Cisco ISE provides a way to create conditions that are individual, reusable policy elements that can be referred from other rule-based policies. You can create conditions from within the policy pages and as separate policy elements to be reused by other types of Cisco ISE policies such as Sponsor group or Client Provisioning policies. Whenever a policy is being evaluated, the conditions that comprise it are evaluated first.

Note Under Policy > Policy Elements > Conditions, the initial Conditions pane displays the following policy element condition options: Authentication, Authorization, Profiling, Posture, Guest, and Common.

Typically, policies consist of rules, where each rule consists of conditions that when met allow actions to be performed (such as access to network resources). Rule-based conditions form the basis of policies, the sets of rules used when evaluating requests.

Simple conditions consist of an attribute, an operator, and a value. You can create simple conditions from within the policy pages and also as separate policy elements that can be reused in policies. ISE allows you to create, edit, and delete simple authorization conditions. When authorized, Cisco ISE returns a permission.

Compound conditions are typically made up of two or more simple conditions. You can create compound conditions as reusable objects from within the policy creation page or from the Conditions page. This page lists all the compound conditions that you have defined in ISE.

Simple Conditions

Prerequisites:

- Before you begin any procedures, you should have a basic understanding of the rule-based authorization policies, the basic building blocks of identity groups, conditions, and permissions, and how these are used in the Cisco ISE user interface. See Understanding Authorization Policy Terminology, page 17-2, Authorization Policy Window, page 17-5, and Configuring Policy Elements Conditions, page 17-17 for more information.
- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Policy Admin. See Table 4-11 for more information on the various administrative roles and the privileges associated with each of them.

Simple Condition Format

This type uses the form *attribute operand value*. Rule-based conditions are essentially a comparison of values (the attribute with its value), and these can be saved and reused in other rule-based policies.

Simple conditions take the format of A operand B, where A can be any attribute from a Cisco ISE dictionary and B can be one of the values that attribute A can take. For example, simple conditions can take the following form:

- Network Access:Protocol Equals RADIUS.

Compound Conditions

Prerequisites:

- Before you begin any procedures, you should have a basic understanding of rule-based authorization policies, the basic building blocks of identity groups, conditions, and permissions, and how they are represented in the Cisco ISE user interface. See Understanding Authorization Policy Terminology, page 17-2, Authorization Policy Window, page 17-5, and Configuring Policy Elements Conditions, page 17-17 for more information.
- Cisco ISE comes with predefined compound conditions for some of the most common use cases. See Authorization Policy, Rule, and Profile Configuration Defaults, page 17-10 for more information on these predefined conditions. You can edit these predefined conditions to suit your requirements.
- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Policy Admin. See Table 4-11 for more information on the various administrative roles and the privileges associated with each of them.

Compound Condition Format

This condition type comprises one or more simple conditions that use an AND or OR relationship. These are built on top of simple conditions and can be saved and reused in other rule-based policies. Compound conditions can take any of the following forms:

- (X operand Y) AND (A operand B) AND (X operand Z) AND ... (so on)
- (X operand Y) OR (A operand B) OR (X operand Z) OR ... (so on)

where X and A are attributes from the Cisco ISE dictionary and can include username and device type. For example, compound conditions can take the following form:

– DEVICE:Model Name Matches Catalyst6K AND Network Access:Use Case Equals Host Lookup.

Configuring Authorization Policy Conditions

Use the Policy Elements Conditions window to display, create, modify, delete, duplicate, and search authorization policy element conditions. The following topics provide procedures for performing these tasks:

- Displaying Existing Authorization Policy Element Conditions, page 17-19
- Creating New Authorization Policy Element Conditions, page 17-19
- Modifying Existing Authorization Policy Element Conditions, page 17-20
- Duplicating Existing Authorization Policy Element Conditions, page 17-21
- Deleting Existing Authorization Policy Element Conditions, page 17-22
- Searching Existing Authorization Policy Element Conditions, page 17-22

Note For more information about simple and compound conditions, see Configuring Policy Elements Conditions, page 17-17.

Displaying Existing Authorization Policy Element Conditions

Use this procedure to display all existing authorization policy element conditions (both simple or compound).

To display existing authorization policy element conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements> Conditions > Authorization > Simple Conditions** (or **Compound Conditions**).

The Conditions window appears listing all of the existing configured authorization policies (which correspond to the condition type you selected, simple or compound).

Creating New Authorization Policy Element Conditions

Use this procedure to create new authorization policy element conditions (simple or compound).

To create new authorization policy element conditions, complete the following steps:

Step 1 Click **Policy > Policy Elements> Conditions > Authorization> Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To create a new simple condition, click **Create**.

The Simple Conditions page displays.

Step 3 Enter values in the following fields to define a new simple condition:

- Name—Enter the name of the simple condition.
- Description—Enter the description of the simple condition.
- Attribute—Click to choose a dictionary from the drop-down list of dictionary options, and choose an attribute from the corresponding attribute choices.
- Operator—Enter **Equals** or **Not Equals**.
- Value—Enter a value that matches the selected attribute.

Step 4 Click **Submit** to save your changes to the Cisco ISE database and create this authorization condition.

Note The Name, Attribute, Operator, and Value fields in simple conditions are required and are marked with an asterisk (*).

Note Compound conditions consist of one or more simple conditions that include different **Equals**, **Not Equals**, and **Matches** operators, and **AND** and **OR** directives that are built upon existing simple conditions. The procedure for creating a new compound condition follows the same steps and processes that are used to create a simple condition. For more details about compound conditions, see Compound Conditions, page 17-18.

Note The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

Modifying Existing Authorization Policy Element Conditions

Use this procedure to modify existing authorization policy element conditions (simple or compound).

To modify existing authorization policy element conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements> Conditions > Authorization> Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To edit an existing condition, select the check box corresponding to the condition you want to modify, and click **Edit**.

The Simple Conditions (or Compound Conditions) page appears. Modify the values as needed in the following fields:

- Name—Enter the name of the simple condition.
- Description—Enter the description of the simple condition.
- Attribute—Click to choose a dictionary from the drop-down list of dictionary options, and choose an attribute from the corresponding attribute choices.
- Operator—Enter **Equals** or **Not Equals**.
- Value—Enter a value that matches the selected attribute.

Step 3 Click **Save** to save your changes to the Cisco ISE system database and create this modified authorization condition.

Note The Name, Attribute, Operator and Value fields in simple conditions are required and marked with an asterisk (*).

Note Compound Conditions consist of one or more simple conditions that include different **Equals**, **Not Equals,** and **Matches** operators, and **AND** and **OR** directives that are built upon existing simple conditions. The procedure for creating a new compound condition follows the same sequence of steps used to create a simple condition. For more details about compound conditions, see Compound Conditions, page 17-18.

Note The "Matches" operator supports and uses regular expressions (REGEX) not wildcards.

Duplicating Existing Authorization Policy Element Conditions

Use this procedure to duplicate existing authorization policy element conditions (simple or compound). This option provides a means for using an existing authorization policy as a template whereby you can:

- Change the name to create a duplicate policy with the same policy element conditions
- Change the name and modify one or more policy elements as desired

Note You must click **Submit** to save your changes to the Cisco ISE database in either case when you duplicate existing policy element conditions.

To duplicate existing authorization policy element conditions, complete the following steps:

Step 1 Click **Policy > Policy Elements> Conditions > Authorization> Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To duplicate an existing simple condition authorization policy, select the check box corresponding to the condition you want to duplicate, and click **Duplicate**.

The Simple Conditions (or Compound Conditions) page appears. You can change the name for this policy:

- Name—Enter a new name for this simple condition, or you can modify one or more values as needed in the following fields to define a new simple condition policy:
- Description—Enter the description of the simple condition.
- Attribute—Click to choose a dictionary from the drop-down list of dictionary options, and choose an attribute from the corresponding attribute choices.
- Operator—Enter **Equals** or **Not Equals**.
- Value—Enter a value that matches the selected attribute.

Step 3 Click **Submit** to save your changes to the Cisco ISE database and create this authorization condition.

Note The Name, Attribute, Operator, and Value fields in simple conditions are required and are marked with an asterisk (*).

Note Compound conditions consist of one or more simple conditions that include different **Equals**, **Not Equals**, and **Matches** operators and **AND** and **OR** directives that are built upon existing simple conditions. The procedure for creating a new compound condition follows the same steps and processes that are used to create a simple condition. For more details about compound conditions, see Compound Conditions, page 17-18.

Note The "Matches" operator supports and uses regular expressions (REGEX) not wildcards.

Deleting Existing Authorization Policy Element Conditions

Use this procedure to delete existing authorization policy element conditions.

To delete existing authorization policy element conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements> Conditions > Authorization> Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To delete an existing condition, select the check box corresponding to the condition you want to delete, and click **Delete**.

- A confirmation window appears prompting if you want to delete the selected item(s).
- Click **Delete** to confirm that you want to delete the authorization condition (or click **Cancel** to end operation).

Searching Existing Authorization Policy Element Conditions

Use this procedure to search for existing authorization policy element conditions that match your desired search criteria.

To search existing authorization policy element conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Authorization> Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To search for a specific value in the existing authorization policy conditions, click **Filter** and choose either **Quick Filter** or **Advanced Filter**.

- If you choose **Quick Filter**, you can search for authorization policy conditions that match the condition name or description attribute value you specify:
  - Enter a value to search for in either the **Name** or **Description** field.
  - Any attribute matching the specified condition name or description displays in the Conditions table beneath these two search fields.
- If you choose **Advanced Filter**, you can search using a variety of authorization policy conditions that match the attribute, operator, and value fields that you configure in the following search rule:
  - Click the Filter drop-down list and choose either **Name** or **Description**.
  - Click the operator drop-down list and choose from among the following options: Contains, Does not contain, Does not equal, Ends with, Is empty, Is exactly (or equals), Is not empty, or Starts with.
  - Enter an attribute that matches the search values with which you want to filter. You can add additional rules.
- Click **Go** to display any matches in the Conditions table beneath the search fields.

Configuring Time and Date Conditions

Use the Policy Elements Conditions window to display, create, modify, delete, duplicate, and search time and date policy element conditions. Policy elements are shared objects that define a condition that is based on specific time and date attribute settings that you configure.

Time and date conditions let you set or limit permission to access Cisco ISE system resources to specific times and days as desired by the attribute settings you make. The following topics provide procedures for performing time and date attribute-related tasks:

- Displaying Existing Time and Date Conditions, page 17-23
- Creating New Time and Date Conditions, page 17-24
- Modifying Existing Time and Date Conditions, page 17-25
- Deleting Existing Time and Date Conditions, page 17-25
- Duplicating Existing Time and Date Conditions, page 17-26
- Searching Existing Time and Date Conditions, page 17-26

Displaying Existing Time and Date Conditions

Use this procedure to display all existing time and date policy element conditions.

To display all existing time and date conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.

The Time and Date Conditions window appears listing all the existing configured time and date conditions.

Creating New Time and Date Conditions

Use this procedure to create new time and date policy element conditions.

To create new time and date conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.

The Time and Date Conditions window appears listing all the existing configured time and date conditions.

Step 2 To create a new time and date condition, click **Add**.

The Time and Date Condition page displays.

Step 3 Enter values in the following fields to define a new time and date condition:

- Condition Name—Enter the name of the time and date condition.
- Description—Enter a description of the time and date condition.

Note You can choose to create a time and date condition using the options in the Standard Settings or the Exceptions panes.

- If you choose to use the Standard Settings pane options—Choose the options corresponding to the time and date conditions you want to set:
  - All Day (the default option) or Specific Hours (this option provides drop-down lists you can use to configure hours, minutes, and AM/PM to set a to-and-from time range).
  - Every Day (the default option) or Specific Days (this option provides check boxes you can use to configure one or more specific days of the week).
  - No Start and End Dates (the default option), or Specific Date Range (this option provides drop-down lists you can use to configure the month, day, and year to set a to-and-from date range), or Specific Date (this option provides drop-down lists you can use to configure a specific month, day, and year).
- If you choose to use the Exceptions pane options—Choose the options corresponding to the time and date conditions you want to set:
  - Time Range (this option provides drop-down lists you can use to configure the hours, minutes, and AM/PM to set a to-and-from time range).
  - Week Days (this option provides check boxes you can use to configure one or more specific days of the week).
  - Date Range (this provides two options):

    Specific Date Range—Provides drop-down lists you can use to configure a specific to-and-from date range by month, day, and year.

    Specific Date—Provides drop-down lists you can use to configure a specific month, day, and year.

Step 4 Click **Submit** to save your changes to the Cisco ISE database and create this time and date condition.

Note The Condition Name field for time and date conditions is required and is marked with an asterisk (*).

Modifying Existing Time and Date Conditions

Use this procedure to modify existing time and date policy element conditions.

To modify existing time and date conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.

The Time and Date Conditions window appears listing all the existing configured time and date conditions.

Step 2 To edit an existing time and date condition, select the check box corresponding to the condition you want to modify, and click **Edit**.

The Time and Date Condition page appears. Modify the options and settings in the following fields as needed (see field and option descriptions in Creating New Time and Date Conditions, page 17-24):

- Condition Name
- Description
- Standard Settings or Exceptions (using the set of options in the panel you choose)

Step 3 Click **Save** to save your changes to the Cisco ISE system database and create this modified time and date condition.

Note The Condition Name field for time and date conditions is required and is marked with an asterisk (*).

Deleting Existing Time and Date Conditions

Use this procedure to delete existing time and date policy element conditions.

To delete existing time and date conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.

The Time and Date Conditions window appears listing all the existing configured time and date conditions.

Step 2 To delete an existing condition, select the check box that corresponds to the time and date condition you want to delete, and click **Delete**.

- A confirmation window appears.
- Click **OK** to confirm that you want to delete the selected time and date condition (or click **Cancel** to end operation).
- A Condition(s) deleted successfully window appears.

Duplicating Existing Time and Date Conditions

Use this procedure to duplicate existing time and date policy element conditions, from which you can create a new time and date condition.

To duplicate existing time and date conditions, complete the following steps:

Step 1 Click **Policy > Policy Elements> Conditions > Common > Time and Date**.

The Time and Date Conditions page appears listing all existing configured time and date conditions.

Step 2 To duplicate an existing time and date condition, select the check box corresponding to the condition you want to duplicate, and click **Duplicate**.

The Time and Date Conditions page appears. You can modify the following conditions in the upper panel as necessary:

- Name—Enter a new name for this condition, or you can modify one or more values as needed in the following fields to define a new time and date condition.
- Description—Enter the description of the time and date condition.

Step 3 In the Standard Settings panel, modify the following values as needed:

- All Day
- Specific Hours (by setting the specific time range in HH:MM:AM/PM using the pull-down options)
- Every Day
- Specific Days (by selecting the check box(es) that match your desired days)
- No Start and End Date
- Specific Date Range (by setting the specific Month:Date:Year from/to date range using the pull-down options)
- Specific Date (by setting the specific Month:Date:Year date using the pull-down options)

Step 4 Click **Save** to save your changes to the Cisco ISE database and create this authorization condition.

Note The Condition Name field in time and date conditions is required and are marked with an asterisk (*).

Searching Existing Time and Date Conditions

Use this procedure to search existing date and time policy element conditions that match a desired search criteria.

To search existing time and date conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.

The Time and Date Conditions window appears listing all the existing configured time and date conditions.

Step 2 To search for a specific value in the existing date and time conditions, click **Filter** and choose either **Quick Filter** or **Advanced Filter**.

- If you choose **Quick Filter**, you can search for time and date conditions that match the condition name or description attribute value you specify:
  - Type the desired search attribute value in the Condition Name or Description fields.
  - Any attribute matching the specified condition name or description displays in the Time and Date Conditions table beneath these two search fields.
- If you choose **Advanced Filter**, you can search using a variety of time and date conditions that match the attribute values you specify:
  - Type the desired search attributes values in the appropriate fields.
  - Any attributes that matches the search values you specified displays in the Time and Date Conditions table beneath these search fields.

Configuring Permissions for Authorization Profiles

Before you start configuring permissions for authorization profiles, make sure you understand the relationship between authorization policies and profiles, are familiar with the Authorization Profile window, know the basic guidelines to follow when configuring policies and profiles, understand what comprises permissions in an authorization profile, and are aware of configuration default values that are described in the following topics:

- Cisco ISE Authorization Policies and Profiles, page 17-5
- Authorization Profile Window, page 17-8
- Authorization Policy and Profile Guidelines, page 17-9
- Authorization Policy, Rule, and Profile Configuration Defaults, page 17-10

Use the Results navigation pane as your starting point in the process for displaying, creating, modifying, deleting, duplicating, or searching policy element permissions for the different types of authorization profiles on your network. The following topics provide procedures for performing these tasks:

- Displaying an Existing Authorization Profile and Permissions, page 17-28
- Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28
- Modifying an Existing Authorization Profile, page 17-31
- Deleting an Existing Authorization Profile, page 17-31
- Duplicating an Existing Authorization Profile, page 17-31
- Searching an Existing Authorization Profile, page 17-32

Note The Results pane initially displays Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access options.

Authorization profiles let you choose the attributes to be returned when a RADIUS request is accepted. Cisco ISE provides a mechanism where you can configure Common Tasks settings to support commonly-used attributes. You need to enter the value for the Common Tasks attributes, which Cisco ISE translates to the underlying RADIUS values.

Displaying an Existing Authorization Profile and Permissions

Use this procedure to display the permissions for an existing authorization profile.

Note The Results navigation pane displays Authorization Profiles, Downloadable ACL, and Inline Posture node options under Authorization.

To display existing permissions for an authorization profile, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

The Authorization Profiles window appears listing all existing configured authorization profiles.

Creating and Configuring Permissions for a New Standard Authorization Profile

Use this procedure to create a new standard authorization profile and configure its permissions.

To create a new standard authorization profile and permissions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

The Authorization Profiles window appears listing all existing configured authorization profiles.

Step 2 To create a new profile, choose one of the two following methods:

- In the Authorization pane, click **action** (icon) and click **Create Standard Authorization Profile**

  or

- In the Standard Authorization Profiles page, click **Add**

The Authorization Profiles > New Authorization profile page appears.

Step 3 Enter values in the following panels and fields as needed to create a new authorization profile:

- **Authorization Profile**
  - Name—Enter a name that identifies the new authorization profile.
  - Description—Enter a description of the authorization profile.
  - Access Type—Choose from the two drop-down list access type options (**ACCESS_ACCEPT** or **ACCESS_REJECT**).

Note The Name and Access Type fields are required and are marked with an asterisk (*).

- **Common Tasks**
  - DACL Name—To choose, select the check box and choose existing downloadable ACL options from the drop-down list (for example, Cisco ISE provides two default values in the drop-down list: **PERMIT_ALL_TRAFFIC** or **DENY_ALL_TRAFFIC**). The drop-down list will include all current DACLs in the local database.
  - VLAN—To choose, select the check box and enter an attribute value that identifies a virtual LAN (VLAN) ID that you want associated with the new authorization profile you are creating (both integer and string values are supported for the VLAN ID). The format for this entry would be *Tunnel-Private-Group-ID:VLANnumber*.



Note If you do not select a a VLAN ID, Cisco ISE uses a default value of VLAN ID = 1. For example, if you only entered 123 as your VLAN number, the Attributes Details pane would reflect the following value: Tunnel-Private-Group-ID = 1:123.

  - Voice Domain Permission—To choose, select the check box to enable the vendor-specific attribute (VSA) of "cisco-av-pair" to be associated with a value of "device-traffic-class=voice". In a multi-domain authorization mode, if the network switch receives this VSA, the endpoint is placed on to a voice domain after authorization.
  - Posture Discovery—To choose, select the check box to enable a redirection process used for Posture discovery in Cisco ISE, and enter an ACL on the device that you want to associate with this authorization profile. For example, if the value you entered is acl119, this is reflected in the Attributes Details pane as: cisco-av-pair = url-redirect-acl = acl119. The Attributes Details pane also displays: cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&action=cpp.
  - Centralized Web Authentication—To choose, select the check box to enable a redirection process that is similar to Posture discovery, but it redirects guest user access requests to the Guest server in Cisco ISE. Enter an ACL on the device that you want to associate with this authorization profile, and select the Default or Manual option from the Redirect drop-down list. For example, if the value you entered is acl-999, this is reflected in the Attributes Details pane as: cisco-av-pair = url-redirect-acl = acl-99. The Attributes Details pane also displays: cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&action=cwa.
  - Auto SmartPort—To choose, select the check box to enable Auto SmartPort functionality and enter a corresponding event name value in the text box. This enables the VSA cisco-av-pair with a value for this option as "auto-smart-port=event_name". Your choice is reflected in the Attributes Details pane.
  - Filter-ID—To choose, select the check box to enable a RADIUS filter attribute that sends the ACL name that you define in the text box (which is automatically appended with ".in"). Your choice is reflected in the Attributes Details pane.
  - Reauthentication—To choose, select the check box and enter a value in seconds for maintaining connectivity during reauthentication. You can also choose attribute values from the Timer drop-down list. You choose to maintain connectivity during reauthentication by selecting to use either the default (a value of 0) or RADIUS-Request (a value of 1) from the drop-down list. Setting this to the RADIUS-Request value maintains connectivity during the reauthentication process.
  - MACSec Policy—To choose, select the check box to enable the MACSec encryption policy whenever a MACSec-enabled client connects to Cisco ISE, and choose one of the following three options in the corresponding drop-down list: must-secure, should-secure, or must-not-secure. For example, your choice is reflected in the Attributes Details pane as: cisco-av-pair = linksec-policy=must-secure.

- NEAT—To choose, select the check box to enable Network Edge Access Topology (NEAT), a feature that extends identity recognition between networks. Selecting this check box displays the following value in the Attributes Details pane: cisco-av-pair = device-traffic-class=switch.
- Web Authentication (Local Web Auth)—To choose, select the check box to enable local web authentication for this authorization profile. This value lets the switch recognize authorization for web authentication by Cisco ISE sending a VSA along with a DACL. The VSA is cisco-av-pair = priv-lvl=15 and this is reflected in the Attributes Details pane.
- Wireless LAN Controller (WLC)—To choose, select the check box and enter an ACL name in the text field. This value is used in a required Airespace VSA to authorize the addition of a locally defined ACL to a connection on the WLC. For example, if you entered rsa-1188, this would be reflected in the Attributes Details pane as: Airespace-ACL-Name = rsa-1188.
- ASA VPN—To choose, select the check box to enable an Adaptive Security Appliances (ASA) VPN group policy. From a drop-down Attributes list, click a value to configure this setting. For example, if you selected Cisco-BBSM, and then selected CBBSM-Bandwidth, this would be reflected in the Attributes Details pane as: Class = Cisco-BBSM:CBBSM-Bandwidth.

Note The Name and Access Type fields are required and are marked with an asterisk (*).

- **Advanced Attributes Settings**
  - Click the down-arrow icon to display the available options in the Dictionaries window. Click to select the desired dictionary and attribute to configure in the first field.
  - Click the down-arrow icon to display the available options in the Attribute Values window. Click to select the desired attribute group and attribute value for the second field. This value matches the one selected in the first field. Any Advanced Attributes setting(s) that you configure will be displayed in the Attribute Details panel.

Note To modify or delete any of the read-only values that are displayed in the Attributes Details pane, you must modify or delete these values in the corresponding Common Tasks field or in the attribute that you selected in the Attribute Values text box in the Advanced Attributes Settings pane.

- **Attributes Details**
  - This pane displays any of the configured attribute values that you set for the Common Tasks and Advanced Attributes.

Note The values displayed in the Attributes Details pane are read-only and cannot be edited or deleted in this pane.

Step 4 Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.

Modifying an Existing Authorization Profile

Use this procedure to modify the permissions in an existing authorization profile.

To modify permissions in an existing authorization profile, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

The Authorization Profiles window appears listing all existing configured authorization profiles.

Step 2 To edit permissions in an existing authorization profile, select the check box corresponding to the existing authorization profile you want to modify, and click **Edit.**

Step 3 Modify the values in the Authorization Profile, Common Tasks, Advanced Attributes Settings, and Attributes Details panels as needed.

Step 4 Click **Save** to save your changes to the Cisco ISE database to create an authorization profile.

For more information:

- For details about the values in the Authorization Profile, Common Tasks, Advanced Attributes Settings, and Attributes Details panels, see the descriptions in Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28.

Deleting an Existing Authorization Profile

Use this procedure to delete an existing authorization profile, which also deletes its corresponding policy element permissions.

To delete an existing authorization profile, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

The Authorization Profiles window appears listing all existing configured authorization profiles.

Step 2 To delete an existing authorization profile, select the check box corresponding to the existing authorization profile you want to delete, and click **Delete**.

A confirmation deletion window appears alerting you that the authorization profile was deleted.

Step 3 Click **OK** to confirm you want to delete this authorization profile from the Cisco ISE system database.

Duplicating an Existing Authorization Profile

Use this procedure to duplicate an existing authorization profile, from which you can create a new authorization profile.

To duplicate an existing authorization profile, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

The Authorization Profiles window appears listing all existing configured authorization profiles.

Step 2 To duplicate an existing authorization, select the check box corresponding to the authorization profile you want to duplicate, and click **Duplicate**.

The Authorization Profiles page appears.

Step 3 Modify the values in the Authorization Profile, Common Tasks, Advanced Attributes Settings, and Attributes Details panels as needed.

Step 4 Click **Submit** to save your changes to the Cisco ISE database and create this new authorization profile.

Note Values in the Name and Access Type fields are required and are marked with an asterisk (*).

For more information:

- For details about the values in the Authorization Profile, Common Tasks, Advanced Attributes Settings, and Attributes Details panels, see the descriptions in Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28.

Searching an Existing Authorization Profile

Use this procedure to search for existing authorization profile conditions that match a desired search criteria.

To search an existing authorization profile, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles.**

The Authorization Profiles window appears listing all existing configured authorization profiles.

Step 2 To search for a specific value in the existing authorization policy conditions, click **Filter** and choose between the **Quick Filter** or **Advanced Filter** options.

If you choose **Quick Filter**, you can search for authorization profile that matches the name or description value you specify:

- Enter a value to search for in the **Name** or **Description** fields.

Any attribute that matches the specified authorization profile name or description displays in the Conditions table beneath these two search fields.

- If you choose **Advanced Filter**, you can search for an authorization profile that matches the attribute, operator, and value fields that you configure in the following search rule:
  - In the Filter drop-down list, select either **Name** or **Description**.
  - In the operator drop-down list, select from the following options: Contains, Does not contain, Does not equal, Ends with, Is empty, Is exactly (or equals), Is greater than, Is greater than or equal to, Is less than, Is less than or equal to, Is not empty, or Starts with.
  - Enter an attribute that matches the search values with which you want to filter. You can add additional rules.
- Click **Go** to display any matches in the Conditions table beneath the search fields.

Configuring Permissions for Downloadable ACLs

To start the process where you can display, create, modify, or delete policy element permissions for downloadable ACLs (DACLs), you need to locate its navigation pane in the Cisco ISE user interface. To do this, choose **Policy > Policy Elements > Results > Authorization** to display the Authorization navigation pane.

The Authorization navigation pane initially displays:

- Authorization Profiles
- Downloadable ACLs
- Inline Posture Node Profiles

For more information:

- For more information about configuring permissions for and managing DACLs, see Configuring DACLs, page 17-33.

Configuring DACLs

The following topics provide procedures for configuring permissions for DACLs:

- Displaying Existing Permissions for DACLs, page 17-33
- Creating and Configuring Permissions for a New DACL, page 17-33
- Modifying Permissions for an Existing DACL, page 17-34
- Deleting an Existing DACL, page 17-34
- Duplicating an Existing DACL, page 17-35
- Searching an Existing DACL, page 17-35

Displaying Existing Permissions for DACLs

Use this procedure to display the permissions for any existing DACLs.

To display existing DACL permissions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

The DACL Management window appears listing all existing configured DACLs.

Creating and Configuring Permissions for a New DACL

Use this procedure to create a new DACL and configure its permissions.

To configure permissions for a new DACL, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

The DACL Management window appears listing all existing configured DACLs.

Step 2 To create a new DACL, click **action** (icon) and select **Create DACL** or click **Add** (+) in the DACL Management window.

Step 3 Enter values for the DACL in the following fields:

- Name—Enter a name that identifies the DACL.
- Description—Enter a description of the DACL.
- DACL Content—Enter the type of desired content in the ACL (IPPermit or IPDeny).

Note The Name and DACL Content fields require that values be entered and are marked with an asterisk (*).

Step 4 Click **Submit** to save your configured values to the Cisco ISE database and create this DACL.

Modifying Permissions for an Existing DACL

Use this procedure to modify the permissions for any existing DACL.

To modify permissions for an existing DACL, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

The DACL Management window appears listing all existing configured DACLs.

Step 2 To edit an existing DACL, select the check box corresponding to the DACL that you want to modify, and click **Edit**.

The DACL Management page appears.

Step 3 Modify the values for the DACL as needed in the following fields:

- Name—Enter a name that identifies the DACL.
- Description—Enter a description of the DACL.
- DACL Content—Choose the type of desired content in the ACL (IPPermit or IPDeny).

Note The Name and DACL Content fields require that values be entered and are marked with an asterisk (*).

Step 4 Click **Submit** to save your configured values to the Cisco ISE database and create this modified DACL.

Deleting an Existing DACL

Use this procedure to delete an existing DACL.

To delete an existing ACL, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

The DACL Management window appears listing all existing configured DACLs.

Step 2 To delete an existing DACL, select the check box corresponding to the DACL that you want to delete, and click **Delete**.

A deletion confirmation window appears.

Step 3 Click **OK** to confirm that you want to delete the DACL, or click **Cancel** to end the operation.

Duplicating an Existing DACL

Use this procedure to duplicate an existing DACL, from which you can create a new DACL.

To duplicate an existing DACL, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

The DACL Management window appears listing all existing configured DACLs.

Step 2 To duplicate an existing DACL, select the check box corresponding to the DACL you want to duplicate, and click **Duplicate**.

The Downloadable ACL window appears.

Step 3 Modify the values in the Name, Description, DACL Content fields as needed.

Step 4 Click **Submit** to save your changes to the Cisco ISE database and create this new authorization profile.

Note The Name and DACL Content fields require that values be entered and are marked with an asterisk (*).

Searching an Existing DACL

Use this procedure to search an existing DACL using criteria that searches for existing DACL values that match your settings.

To search an existing DACL, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

The DACL Management window appears listing all existing configured DACLs.

Step 2 To search for a specific value in the existing DACLs, click **Filter** and choose between the **Quick Filter** or **Advanced Filter** options.

If you choose **Quick Filter**, you can search for DACL values that match the name or description value you specify:

- Enter a value to search for in the **Name** or **Description** fields.

Any attribute that matches the specified DACL name or description appears in the Conditions table beneath these two search fields:

- If you choose **Advanced Filter**, you can search for a DACL that matches the attribute, operator, and value fields that you configure in the following search rule:
  - In the Filter drop-down list, select either **Name** or **Description**.

  - In the operator drop-down list, select from the following options: Contains, Does not contain, Does not equal, Ends with, Is empty, Is exactly (or equals), Is not empty, or Starts with.
  - Enter an attribute that matches the search values with which you want to filter. You can add additional rules.
- Click **Go** to display any matches in the Conditions table beneath the search fields.

Configuring Policies for SGACLs

To learn how to configure policies for security group access control lists (SGACLs), which allow you to display, create, modify, or delete policy element permissions for SGACLs, see Configuring Cisco Security Group Access Policies, page 22-1.

Machine Access Restriction and Active Directory Users

Cisco ISE Release 1.1 contains a Machine Access Restriction (MAR) component that provides an additional means of controlling authorization for Microsoft Active Directory-authentication users. This form of authorization is based on the machine authentication of the computer used to access the Cisco ISE network. For every successful machine authentication, Cisco ISE caches the value that was received in the RADIUS Calling-Station-ID attribute (attribute 31) as evidence of a successful machine authentication.

Cisco ISE retains each Calling-Station-ID attribute value in cache until the number of hours that was configured in the “Time to Live” parameter in the Active Directory Settings page expires. Once the parameter has expired, Cisco ISE deletes it from its cache.

When a user authenticates from an end-user client, Cisco ISE searches the cache for a Calling-Station-ID value from successful machine authentications for the Calling-Station-ID value that was received in the user authentication request. If Cisco ISE finds a matching user-authentication Calling-Station-ID value in the cache, this affects how Cisco ISE assigns permissions for the user that requests authentication in the following ways:

- If the Calling-Station-ID value matches one found in the Cisco ISE cache, then the authorization profile for a successful authorization should be assigned.
- If the Calling-Station-ID value is not found to match one in the Cisco ISE cache, then the authorization profile for a successful user authentication without machine authentication should be assigned.

For more information

- For more details, see Machine Authentication, page 5-5.



CHAPTER 18

Configuring Endpoint Profiling Policies

This chapter describes the profiling service in the Cisco Identity Services Engine (Cisco ISE) appliance, which allows you to efficiently manage an enterprise network of varying scale and complexity.

This chapter guides you through the features of the Cisco ISE profiling service in detail.

- Profiling Service in Cisco ISE, page 18-2
- Understanding the Profiling Service, page 18-2
  - Profiled Endpoints Dashlet, page 18-6
  - Viewing Profiler Reports, page 18-7
- Change of Authorization, page 18-8
- Configuring the Probes, page 18-12
  - Filtering Endpoint Attributes, page 18-14
- Endpoint Profiling Policies, page 18-35
  - A Quick Reference to Creating a New Endpoint Profiling Policy in Cisco ISE, page 18-44
- Endpoint Profiling, page 18-52
- Profiling Results, page 18-57
  - Profiling Exception Actions, page 18-58
  - Profiling Network Scan Actions, page 18-62
- Endpoint Profiling by Integrating Network Mapper in Cisco ISE, page 18-67
- Endpoint Profiling by Using an IOS Sensor on a Network Access Device, page 18-69
- Excluding Static Endpoints in Advanced Licenses, page 18-74
- IP Address and MAC Address Binding in Cisco ISE, page 18-75
- Integrating Cisco ISE with Cisco Network Admission Control Appliance, page 18-75
  - Configuring Cisco Clean Access Managers in Cisco ISE, page 18-76
  - Filtering, Adding, Editing, and Deleting Clean Access Managers in Cisco ISE, page 18-77

Profiling Service in Cisco ISE

The Cisco ISE profiling service provides a unique functionality in discovering, locating, and determining the capabilities of all the attached endpoints on your network (known as identities in Cisco ISE), regardless of their device types, in order to ensure and maintain appropriate access to your enterprise network. It primarily collects an attribute or a set of attributes of all the endpoints on your network and classifies them according to their profiles.

For details on the profiling service, see the "Understanding the Profiling Service" section on page 18-2.

The Profiler in Cisco ISE

The Cisco ISE profiler is comprised of the following components:

- The sensor contains a number of probes. The probes capture network packets by querying network access devices and forward attributes and attribute values that are collected from endpoints to the analyzer.

  The probe manager within the sensor provides support to the profiling service, initializing and controlling various probes that run on the sensor. The probe manager allows you to configure probes to start and stop collecting attributes and their values from endpoints. An event manager within the sensor allows communication of the events between the probes in the probe manager.

  A forwarder stores endpoints into the Cisco ISE database along with their attributes data, and then notifies the analyzer of new endpoints detected on your network. The analyzer classifies endpoints into endpoint identity groups and stores endpoints with the matched profiles in the Cisco ISE database.

- An analyzer evaluates endpoints, by using configured policies and identity groups to match attributes and their attribute values that are collected, which classifies endpoints into the specified group and stores endpoints with the matched profile in the Cisco ISE database.

Understanding the Profiling Service

The profiling service collects attributes of endpoints from the network devices and the network, classifies endpoints into a specific group according to their profiles, and stores endpoints with their matched profiles in the Cisco ISE database. You can use a list of possible attributes that includes any or all of the attributes defined in the system dictionaries. You can leverage the existing dictionaries as well as define an ad-hoc dictionary for any attribute during run-time. All the attributes that are handled by the profiling service need to be defined in the profiler dictionaries.

An endpoint is a network-capable device that connects to your enterprise network. The MAC address is always the unique representation of an endpoint, but you can also identify an endpoint with a varying set of attributes and the values associated to them, called an attribute-value pair. You can collect a varying set of attributes for endpoints based on the endpoint capability, the capability and configuration of the network access devices (NADs), and the methods (probes) that you use to collect these attributes.

You can associate each endpoint on your network to an existing endpoint identity group in the system, or to a new group that you can create and associate to the parent group. By grouping endpoints, and applying endpoint profiling policies to the group, you can determine the mapping of endpoints to the endpoint profiles by checking the corresponding endpoint profiling policies.

For details on endpoint profiling on Cisco ISE, see "Endpoint Profiling" section on page 18-3.

For details on licenses that you need to install for the profiling service, see "Licenses for the Profiling Service" section on page 18-4.

For details on how to deploy the profiling service, see "Deploying the Profiling Service" section on page 18-4.

For details on Profiled Endpoints dashlet, see "Profiled Endpoints Dashlet" section on page 18-6.

For details on endpoint profiling reports, see the "Viewing Profiler Reports" section on page 18-7.

Endpoint Profiling

Endpoint profiling in Cisco ISE identifies each endpoint on your network, and groups those endpoints according to their profiles.

The Cisco ISE profiler provides you with an efficient and effective means of addressing the challenge in the deployment and management of the following next-generation security mechanisms:

- Facilitates an efficient and effective deployment and ongoing management of authentication by using IEEE standard 802.1X port-based authentication access control, MAC Authentication Bypass (MAB) authentication, and Network Admission Control (NAC) for any enterprise network of varying scale and complexity.
- Identifies, locates, and determines the capabilities of all of the attached network endpoints regardless of endpoint types.
- Protects against inadvertently denying access to some endpoints.

The profiler provides a contextual inventory of all the endpoints that are using your network resources to identify what is connected to your network, and where it exists on your network. The profiler allows both static and dynamic endpoint profiling, where dynamic endpoint profiling allows you to discover endpoints on your Cisco ISE enabled network, and notify attribute changes resulting from the network to your Cisco ISE deployment.

In order to effectively profile endpoints on your network, you require a thorough understanding of the types of endpoints (devices) that are connecting to your network, their location, and their abilities relative to the state of the port on which they currently reside. You can define endpoint profiling policies in Cisco ISE, which allow you to group endpoints according to their profiles. Cisco ISE deployment creates the following three endpoint identity groups: Blacklist, Profiled, and Unknown.

An endpoint profiling policy can contain a single condition, or a set of conditions (compound condition) that are logically combined using an AND or OR operator, against which you check and categorize endpoints. All the conditions can either be used with an AND operator or an OR operator together for a given rule in a policy. However, the rules in a given policy are evaluated separately, and only by using an OR operator.

A condition is used to check the collected endpoint attribute value against the value specified in the condition for an endpoint. If you map more than one attribute, you can logically group the conditions, which helps you to classify and categorize endpoints on your network. You can check endpoints against one or more such conditions with a corresponding certainty metric (an integer value that you define) associated with it in a rule. The certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. The certainty metric for all the valid rules are added together to form the matching certainty. The certainty metric measures how each condition contributes which improves the overall classification of endpoints on your network. Each policy has a minimum certainty metric (an integer value) associated to it.

An exception action is a configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the exception conditions that are associated with the action are met.

An endpoint scan action is a configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the conditions that are associated with the network scan action are met.

Licenses for the Profiling Service

Prerequisites:

To enable the profiling service in Cisco ISE, you must install an advanced license package on top of the base license. You can utilize all of the session services, including the Network Access, Guest, Posture, Client Provisioning, Profiling Service, and Security Group Access (SGA) depending on your configuration on the nodes.

Cisco ISE allows you to configure the profiling service to run on multiple nodes that assume the Policy Service persona in a distributed Cisco ISE deployment. You can also configure the profiling service on a single node in a standalone Cisco ISE deployment.

With a Base license installed, you cannot profile endpoints on your network. You can only manage endpoints including import and the static assignment of endpoints by using the Endpoints page, and view endpoints on the Endpoint Identity Groups page. For more details, see the Endpoints, page 4-15, and Endpoint Identity Groups, page 4-70 sections in Chapter 4, "Managing Identities and Admin Access."

Cisco ISE consumes Advanced licenses when endpoints are matched to an authorization policy. For more information, see "Excluding Static Endpoints in Advanced Licenses" section on page 18-74.

For more information on Cisco ISE license packages, refer to the Performing Post Installation Tasks chapter in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

Deploying the Profiling Service

Prerequisites:

Before you begin, you should have an understanding of the centralized configuration and management of Cisco ISE nodes in the distributed deployment.

For information on Cisco ISE distributed deployment, Chapter 9, "Setting Up Cisco ISE in a Distributed Environment"

You can deploy the Cisco ISE profiling service either in a standalone environment (on a single node), or in a distributed environment (on multiple nodes). Depending on your deployment type and the license you have installed, the profiling service of Cisco ISE can run on a single node or on multiple nodes. You need to install either the base license to take advantage of the basic services or the advanced license to take advantage of all the services of Cisco ISE.

Cisco ISE distributed deployment includes support for the following:

- The Deployment Nodes page supports the infrastructure for distributed nodes in the distributed deployment.
- A node specific configuration of probes—The Profiling Configuration page allows you to configure the probe per node from the Administration ISE node.
- Global Implementation of the profiler Change of Authorization (CoA).
- Configuration to allow syslogs to be sent to the appropriate profiler node.

Configuring the Profiling Service in Cisco ISE

From the Administration menu, you can choose Deployment to manage the Cisco ISE deployment on a single node or multiple nodes. You can use the Deployment Nodes page to configure the profiling service for your Cisco ISE deployment.

To manage the Cisco ISE deployment, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

The Deployment menu window appears on the left pane of the user interface. You can use the Table view button or the List view button to display the nodes in your Cisco ISE deployment.

Step 2 Click the **Table** view button.

Step 3 Click the **Quick Picker** (right arrow) icon to view the nodes that are registered in your deployment.

The Table view displays all the nodes that are registered in a row format on the right pane of the user interface.

Note To view the nodes in your deployment in a tree, click the **List** view button. An arrow appears in front of the Deployment menu. Click the arrow in front of the Deployment menu to view the nodes that are registered in your deployment in a tree view.

From the Deployment menu, you can configure the profiling service on any Cisco ISE node that assumes the Policy Service persona in a distributed deployment.

To deploy the profiling service, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

The Deployment menu window appears. You can use the Table view or the List view button to display the nodes in your deployment.

Step 2 Click the **Table** view button.

Step 3 Click the **Quick Picker** (right arrow) icon to view the nodes that are registered in your deployment.

The Table view displays all the nodes that are registered in a row format on the Deployment Nodes page of the user interface. The Deployment Nodes page displays the nodes that you have registered along with their names, personas, roles, and the replication status for the secondary nodes in your deployment.

Step 4 Choose a Cisco ISE node from the Deployment Nodes page.

Note If you have more than one node registered in a distributed deployment, all the nodes that you have registered appear in the Deployment Nodes page, along with the primary node. You have the option to configure each node as a Cisco ISE node (Administration, Policy Service, and Monitoring personas), or an Inline Posture node. If you have the Policy Service persona enabled, but the **Enable Profiling Services** check box unchecked, Cisco ISE does not display the Profiling Configuration tab. If you have the Policy Service persona disabled on any node, Cisco ISE displays only the General Settings tab and does not display the Profiling Configuration tab that prevents you from configuring the probes on the node.

Step 5 Click the **Edit** button.

The Edit Node page appears. This page contains the General Settings tab to configure the deployment and the Profiling Configuration tab to configure the probes on each node. The Profiling Configuration tab will not be made available on the secondary Administration ISE node.

Note If you have the Policy Service persona disabled, or if enabled but the **Enable Profiling Services** option is not selected, then the Cisco ISE administrator user interface does not display the Profiling Configuration tab. If you have the Policy Service persona disabled on any Cisco ISE node, Cisco ISE displays only the General Settings tab. It does not display the Profiling Configuration tab that prevents you from configuring the probes on the node.

Step 6 From the General Settings tab, check the **Policy Service** check box, if it is not already active.

If you have the Policy Service check box unchecked, both the session services and the profiling service check boxes are disabled.

Step 7 For the Policy Service persona to run the Network Access, Posture, Guest, and Client Provisioning session services, check the **Enable Session Services** check box, if it is not already active. To stop the session services, uncheck the **Enable Session Services** check box.

Step 8 For the Policy Service persona to run the profiling service, check the **Enable Profiling Services** check box. To stop the profiling service, uncheck the **Enable Profiling Services** check box.

Note The profiling service only runs on Cisco ISE nodes that assume the Policy Service persona and does not run on Cisco ISE nodes that assume the Administration and Monitoring personas in a distributed deployment.

Step 9 Click **Save** to save the node configuration.

Next Steps:

See the "Configuring the Probes" section on page 18-12 for more information on how to configure the profiler probes after installing the Cisco ISE application for your network.

Profiled Endpoints Dashlet

The Profiled Endpoints dashlet summarizes the number of dynamically profiled endpoints for the last 24-hour period, as well as 60 minutes from the current system time. It refreshes data every minute and displays it on the dashlet. You can invoke the Endpoint Profiler Summary report from the tool tips that are displayed on the 24-hour and 60-minutes spark lines for a specific period. The stack bars display endpoints distribution details by Place in Network (PIN), matching endpoint profiles, and identity groups.

The Profiled Endpoints dashlet does not reflect endpoints for the following type of endpoints:

- Endpoints that are classified as Unknown
- Endpoints that are statically assigned to endpoint profiles. (Static assignment can be done from the Endpoints list page by editing endpoints and setting the Static Assignment flag to true.)
- Endpoints that are imported with specified profiles.

For endpoints imported from a .csv file, the Profiled Endpoints dashlet will reflect endpoints for which an endpoint profile is not specified.

Table 18-1 describes the fields on the Profiled Endpoints dashlet on Cisco ISE. The dashlet provides profiler distribution details for the last 24-hour period, as well as 60-minutes from the current system time.

Table 18-1 Profiled Endpoints Dashlet

Name	Description
Unique	A summary of unique endpoints profiled in Cisco ISE for the last 24-hour from the current system time.
PIN (Place in Network)	The location of all the profiled endpoints with subnet mask information.
Profile	The endpoint profiling policies that are used to profile endpoints.
Identity Group	
Endpoint Identity Group	Displays endpoint identity groups of endpoints that they belong, which do not fall under 802.1X authentication. In addition, it also displays endpoint identity groups of endpoints and user identity groups of users for 802.1X authentication.
User Identity Group	Displays the user identity groups of users when endpoints are 802.1X authenticated.

Viewing Profiler Reports

Cisco ISE provides you with various reports on endpoint profiling, and troubleshooting tools that you can use to efficiently manage your network. You can generate reports for historical as well as current data. You may be able to drill down on a part of the report to look into more details. For large reports, you can also schedule reports and download them in various formats.

For more information on how to generate reports and work with the interactive viewer, see Chapter 24, "Reporting."

For more information on endpoint profiling reports, see "Standard Reports" section on page 18-7.

Standard Reports

For your convenience, the standard reports present a common set of predefined report definitions. You can click on the Report Name link to run the report for today. You can query the output by using various system predefined parameters. You can enter specific values for these parameters.

You can use the Run button to run the report for a specific period, as well as use the Query and Run option. The Query and Run option allows you to query the output by using various parameters. The Add to Favorite button allows you to add reports that you use frequently to the Operations > Reports > Favorites location. The Reset Reports button allows you to reset your reports in this catalog to factory defaults.

You can run the reports on endpoint profiling from the following location:

Operations > Reports > Catalog > Endpoint.

The following are the standard reports for endpoint profiling:

- Endpoint_MAC_Authentication_Summary—A report that lets you view the RADIUS authentication summary information for a particular MAC/MAB along with a graphical representation for a selected time period.
- Endpoint_Profiler_Summary—A report that lets you view the profiler summary information for a particular MAC address for a selected time period.
- Endpoint_Time_To_Profile—A report that lets you view the time to profile information for a particular MAC address for a selected time period.
- Top_N_Authentications_By_Endpoint_Calling_Station_ID—A report that lets you view the top N passed/failed/total authentications count for RADIUS protocol with respect to an endpoint calling station ID for a selected time period.
- Top_N_Authentications_By_Machine—A report that lets you view the top N passed/failed/total authentications count for RADIUS protocol with respect to machine information for a selected time period.

In addition, you can view a fewer accounting records for intervals of less than an hour with an enhanced option for profiling endpoints that uses an embedded IOS sensor.

For more information, see RADIUS Accounting Reports, page 18-74.

Change of Authorization

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) for endpoints that are already authenticated to enter your network. The global configuration of CoA in Cisco ISE enables the profiling service with more control over endpoints.

You can use the global configuration option to disable CoA by using the default No CoA option or enable CoA by using port bounce and reauthentication options. If you have configured Port Bounce CoA in Cisco ISE, the profiling service may still result in issuing other CoAs as described in the CoA Exemptions section. For information on CoA exemptions, see the "CoA Exemptions" section on page 18-10.

You can primarily make use of the RADIUS probe or the Monitoring persona REST API to address the authentication of endpoints. For performance reasons, you can enable the RADIUS probe, which allows faster performance. If you have enabled CoA, then Cisco recommends you to enable the RADIUS probe in conjunction with your CoA configuration in the Cisco ISE application. The profiling service can then issue an appropriate CoA for endpoints by using the RADIUS attributes that are collected. If you have disabled the RADIUS probe in the Cisco ISE application, you can rely on the Monitoring persona REST API to issue CoAs over HTTPS to provide complementary information, as required, before triggering CoA. This allows the profiling service to support a wider range of endpoints without requiring the support of the RADIUS probe.

Note Since both primary and secondary Monitoring nodes have identical session directory information, Cisco ISE arbitrarily designates one of those nodes as the default destination for REST queries.

No CoA

You can use this default option to disable the global configuration of CoA.

Port Bounce

You can use this option only if there is only one session on a switch port. If the port exists with multiple sessions, then the CoA option that is used is the Reauth option.

Reauth

You can use this option to enforce reauthentication of an already authenticated endpoint when profiled.

If you have multiple active sessions on a single port, the profiling service issues a CoA with the Reauth option even though you have configured CoA with the Port Bounce option. This function potentially avoids disconnecting other sessions as might occur with the Port Bounce option.

The profiling service initiates the CoA in the following cases:

- Static assignment of an endpoint
- An exception action is configured
- An endpoint is profiled for the first time
- Endpoint deleted

Static Assignment of an Endpoint

The profiling service issues a CoA, if you have an existing endpoint successfully authenticated already on your network that is now statically assigned to a different profile or a different endpoint identity group and the endpoint profiling policy has changed.

An Exception Action is Configured

The profiling service issues a CoA for an endpoint, if you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint so that the profiling service moves the endpoint to the corresponding static profile by issuing a CoA.

For more information on exception action, see the "Profiling Exception Actions" section on page 18-58.

An Endpoint is Profiled for the First Time

The profiling service issues a CoA for an endpoint that is not statically assigned and profiled for the first time, that is, the profile changes from an unknown to a known profile.

An Endpoint is Deleted

The profiling service issues a CoA when an endpoint is deleted from the Endpoints page and the endpoint is most likely disconnected or removed from the network.

For more information on CoA exemptions, see the "CoA Exemptions" section on page 18-10.

For more information on CoA configuration details, see Table 18-2.

CoA Exemptions

The implementation of CoA in Cisco ISE is described in "Change of Authorization" section on page 18-8.

This section describes a few environments in Cisco ISE where the profiler does not issue a CoA even though it matches as described in the Change of Authorization section.

An Endpoint Disconnected from the Network

The profiling service does not issue a CoA when a disconnected endpoint from your network is discovered.

Authenticated Wired EAP-Capable Endpoint

The profiling service does not issue a CoA when an authenticated wired EAP-capable endpoint is discovered.

Multiple Active Sessions per Port

The profiling service issues a CoA with the Reauth option even though you have configured CoA with the Port Bounce option when you have multiple active sessions on a single port. This function potentially avoids disconnecting other sessions as might occur with the Port Bounce option.

Packet-of-Disconnect CoA (Terminate Session) when a Wireless Endpoint is Detected

If an endpoint is discovered as wireless by using the Wireless - 802.11 or Wireless - Other values according to the NAS-Port-Type attribute (the values for RADIUS Attribute 61) of that endpoint, then a Packet-of-Disconnect CoA (Terminate-Session) is issued instead of the Port Bounce CoA. The benefit of this change is to match the Wireless LAN Controller (WLC) CoA.

Note Here, the No CoA and Reauth CoA configurations are not affected and it applies the same for wired and wireless endpoints. Refer to Table 18-2.

Table 18-2 summarizes CoA for different environments for each CoA configuration in Cisco ISE.

Table 18-2 Change of Authorization for Each CoA Configuration

Scenarios	CoA Configuration - No CoA	CoA Configuration - Port Bounce	CoA Configuration - Reauth	Additional information
Global CoA configuration in Cisco ISE (typical)	No CoA	Port Bounce	Reauthentication	
An endpoint is disconnected on your network	No CoA	No CoA	No CoA	It is determined by RADIUS attribute Acct -Status -Type value Stop.
An authenticated wired EAP-capable endpoint	No CoA	No CoA	No CoA	If authentication fails, then it is the same as the typical configuration.

Table 18-2 Change of Authorization for Each CoA Configuration (continued)

Scenarios	CoA Configuration - No CoA	CoA Configuration - Port Bounce	CoA Configuration - Reauth	Additional information
Wired with Multiple Active Sessions on the same switch port	No CoA	Reauthentication	Reauthentication	It avoids disconnecting other sessions.
Wireless endpoint	No CoA	Terminate Session (PoD)	Reauthentication	Support to WLC.
Incomplete CoA data	No CoA	No CoA	No CoA	Due to missing RADIUS attributes.

CoA Global Configuration

You can use the Settings menu window to configure the CoA globally on your Cisco ISE distributed deployment.

To configure CoA, complete the following steps:

Step 1 Choose **Administration > System > Settings**.

The Settings menu window appears.

Step 2 From the Settings menu window, choose **Profiling**.

Step 3 Configure the CoA.

The profiling configuration for CoA has the following options:

- No CoA (default)
- Port Bounce
- Reauth

Step 4 Click **Save**.

Configuring the Probes

Prerequisite:

Before you begin, you should have a basic understanding of the Cisco ISE distributed deployment. Review the following:

Deploying the Profiling Service to understand how the profiling service is enabled in the Cisco ISE distributed deployment.

A probe is a method used to collect an attribute or a set of attributes from an endpoint on your network. The probe allows you to create or update endpoints with their matched profile in the database. The Profiling Configuration tab from the Edit Node page contains the configuration options that allow you to enable or disable the probes on each node, where a node specific configuration of probes can be done on your Cisco ISE appliances.

For more information on filtering endpoints attributes, see the Filtering Endpoint Attributes, page 18-14.

You can reach the Deployment menu from the Administration mega menu. The Deployment menu window displays the registered nodes in your deployment. You can use the Table view or the List view button to display the nodes in your deployment. You can also select a node from the Deployment menu window.

To configure a probe on a node, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

Step 2 From the Deployment menu window, choose the node.

The Deployment Nodes page displays the nodes that you have registered with their names, personas, roles, and the replication status in your deployment.

Note If you have a single node registered, only the node that you have registered appears in the Deployment Nodes page. You need to enable the Administration, Policy Service, and Monitoring personas on it. If you have more than one node registered, all the nodes that you have registered appear in the Deployment Nodes page. You have the option to configure each node as an ISE node (Administration, Policy Service, and Monitoring personas) or an Inline Posture node. If you have the Policy Service persona disabled on any node, Cisco ISE displays only the General Settings tab and does not display the Profiling Configuration tab, which prevents you from configuring the probes on the node.

Step 3 From the Deployment Nodes page, choose **Edit**.

The Edit Node page appears. This page contains the General Settings tab for configuring Cisco ISE deployment and the Profiling Configuration tab for configuring probes on each node.

Note If you have the Policy Service persona enabled, but the **Enable Profiling Services** check box is unchecked, Cisco ISE does not display the Profiling Configuration tab. If you have the Policy Service persona disabled on any node, Cisco ISE displays only the General Settings tab and does not display the Profiling Configuration tab that allows you to configure the probe on the node.

Step 4 Choose the **Profiling Configuration** tab.

The Probe Configuration page displays all the probes that Cisco ISE supports and their configuration options in a single page.

Step 5 Configure the values in the Edit Node page for each probe.

The procedures for configuring each probe on a node in the profiling service includes the following tasks:

- Configuring the NetFlow Probe
- Configuring the DHCP Probe
- Configuring the DHCP SPAN Probe
- Configuring the HTTP Probe
- Configuring the RADIUS Probe
- Configuring the Network Scan (NMAP) Probe
- Configuring the DNS Probe
- Simple Network Management Protocol
  - Configuring the SNMP Query Probe
  - Configuring the SNMP Trap Probe

Step 6 Click **Save** to save the probe configuration.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Filtering Endpoint Attributes

Cisco ISE, when enabled with multiple probes per node, experiences a considerable performance degradation due to numerous attributes per endpoint that are collected and stored in the administration node database. Some of the attributes that are collected are temporal in nature as well as not required for endpoint profiling. The huge collection of attributes per probe for each endpoint that cannot be used for endpoint profiling results in Cisco ISE administration node database persistence and performance degradation.

To address performance degradation of Cisco ISE, filters for RADIUS, DHCP (both DHCP Helper and DHCP SPAN), HTTP, and SNMP probes have been implemented in the profiler probes, except for the NetFlow probe). Each probe filter contains the list of attributes that are temporal and irrelevant for endpoint profiling and removes those attributes from the attributes collected by the probes.

The forwarder component of the profiler invokes the filter event to remove attributes that are specified in each of the filter. They remove attributes from the collection before merging them with existing attributes and their values in the endpoint cache. In addition to removing attributes from the attributes that are collected from all the probes, the profiler dictionaries also have been updated with a list of attributes that are required for endpoint profiling.

A DHCP filter for both the DHCP Helper and DHCP SPAN contains all the attributes that are not necessary and they are removed after parsing DHCP packets. The attributes after filtering are merged with existing attributes in the endpoint cache for an endpoint.

An HTTP filter is used for filtering attributes from HTTP packets, where there is no significant change in the set of attributes after filtering.

A RADIUS filter is used once the syslog parsing is complete and endpoint attributes are merged into the endpoint cache for profiling.

A SNMP filter removes all the attributes that are not relevant after the SNMP Query probe collects a large number of attributes.

The Cisco ISE Bootstrap log contains messages that deal with the creation of dictionaries as well as filtering of attributes from the dictionaries. You can also log a debug message when endpoints go through the filtering phase to indicate that filtering has occurred.

Configuring the NetFlow Probe

Table 18-3 describes the fields that allow you to configure the NetFlow probe on the Edit Nodes page.

To enable the NetFlow probe, configure the following fields:

Table 18-3 NetFlow Configuration

Field	Description
The Enable check box	To enable the NetFlow probe on a node, check the **Enable** check box. To disable the NetFlow probe on a node, uncheck the **Enable** check box.
Interface	Click the drop-down arrow to choose the interface.
Port	Enter the port number.
Description	The description of the NetFlow probe.

Cisco ISE profiler implements Cisco IOS NetFlow Version 9, and supports earlier versions that are beginning with version 5. The MAC address is not a part of IP flows in earlier versions of NetFlow. This requires you to profile endpoints with their IP addresses by correlating the attributes information collected from the network access devices in the endpoints cache.

Cisco IOS NetFlow version 9 is a proprietary Cisco product that allows you to access to IP flows on your network and export IP flows from the NetFlow-enabled network access devices. The Cisco IOS software allows NetFlow to export IP flows by using the UDP, a non congestion-aware protocol.

The basic output of NetFlow is a flow record and the most recent evolution of the flow record format is NetFlow version 9. The distinguishing feature of NetFlow version 9 is that the flow record format is based on a template. The template describes the flow record format, and the attributes of the fields (such as type and length) within the flow record. The template provides flexibility, and it is extensible to the flow record format, a format that allows future enhancements to the NetFlow services without requiring concurrent changes to the basic output. It provides the versatility needed to support new fields, and also record types. The templates cannot be stored in network access devices, and are refreshed every time from IP flows.

You can collect NetFlow version 9 attributes from the NetFlow-enabled network access devices to create an endpoint, or update an existing endpoint in the Cisco ISE database. You can configure NetFlow version 9 to attach the source and destination MAC addresses of endpoints and update them. You can also create a dictionary of NetFlow attributes to support NetFlow-based profiling.

If you have Cisco IOS NetFlow version 9, the values of the ICMP_TYPE field are based on the PROTOCOL field in the NetFlow attributes collected by the NetFlow probe.

- If the value of the PROTOCOL field in the NetFlow attributes that are collected by the NetFlow probe is 6 (TCP) or 17 (UDP), then the value of the ICMP_TYPE field will always be equal to the value of the L4_DST_PORT field.
- If the value of the PROTOCOL field in the NetFlow attributes that are collected by the NetFlow probe is 1 (ICMP), then the value of the ICMP_TYPE field will be a combination of ICMP Type and ICMP code.

For more detailed information, see Table 6, NetFlow Version 9 Field Type Definitions of The NetFlow Version 9 Flow Record Format in the following link:

http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html

The following are the known attributes that are collected by the NetFlow probe:

IN_BYTES	IN_PKTS	FLOWS
PROTOCOL	SRC_TOS	TCP_FLAGS
L4_SRC_PORT	IPV4_SRC_ADDR	SRC_MASK
L4_DST_PORT	IPV4_DST_ADDR	DST_MASK
IPV4_NEXT_HOP	LAST_SWITCHED	FIRST_SWITCHED
OUT_BYTES	OUT_PKTS	IPV6_SRC_ADDR
IPV6_DST_ADDR	IPV6_SRC_MASK	IPV6_DST_MASK
IPV6_FLOW_LABEL	ICMP_TYPE	DST_TOS
IN_SRC_MAC	OUT_DST_MAC	SRC_VLAN
DST_VLAN	IP_PROTOCOL_VERSION	DIRECTION

Cisco IOS NetFlow Version 5

Cisco IOS NetFlow version 5 packets do not contain MAC addresses of endpoints. The attributes that are collected from NetFlow version 5 cannot be directly added to the Cisco ISE database. You can discover endpoints by using their IP addresses, and append the NetFlow version 5 attributes to endpoints. However, these endpoints must have been previously discovered with the RADIUS or SNMP probe. It can be done by combining IP addresses of the network access devices, and IP addresses obtained from the NetFlow version 5 attributes.

For more detailed information on the NetFlow version 5 Record Format, see the following link:

http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html#wp1030618

To support the Cisco ISE profiling service, Cisco recommends using the latest version of NetFlow (version 9), which has additional functionality needed to operate the profiler. If you use NetFlow version 5 in your network, then you can use version 5 only on the primary NAD at the access layer, as it will not work anywhere else.

The following are the known attributes that are collected by the NetFlow version 5:

srcaddr	dstaddr	nexthop
input	output	first
last	srcport	dstport
tcp_flags	prot	flow_sequence
sys_uptime		

Configuring the DHCP Probe

Table 18-4 describes the fields that allow you to configure the DHCP probe on the Edit Nodes page.

To enable the DHCP probe, configure the following fields:

Table 18-4 DHCP Configuration

Field	Description
The Enable check box	To enable the DHCP probe on a node, check the **Enable** check box. To disable the DHCP probe on a node, uncheck the **Enable** check box.
Interface	Click the drop-down arrow to choose the interface.
Port	Enter the port number.
Description	The description of the DHCP probe.

Dynamic Host Configuration Protocol (DHCP) is an auto configuration protocol, which is used on IP networks for allocating IP addresses dynamically, or statically. It provides reliability in several ways such as periodic renewal, rebinding, and failover in client-server communications. There are two versions of DHCP, one for IPv4, and one for IPv6. While both the versions bear the same name DHCP, and perform much the same purpose, the details of the DHCP protocol for IPv4 and IPv6 are sufficiently different that they can be considered as separate protocols.

A DHCP server manages a pool of IP addresses and information about client configuration parameters. In addition to allocating IP addresses, DHCP also provides other configuration information such as the subnet mask, default gateway, domain name, and name servers to DHCP clients on an IP network. DHCP clients that do not use DHCP for IP address configuration may still use it to obtain other configuration parameters.

DHCP uses the same UDP ports as defined for the BOOTP protocol by Internet Assigned Numbers Authority (IANA). DHCP messages are sent to the DHCP server UDP port 67 from a client to a server, and from a server to a client are sent to the DHCP client UDP port 68. As DHCP communications are connectionless, DHCP clients and servers on the same subnet communicate by using UDP broadcasts. If they are on different subnets, then the clients send DHCP discovery, and request messages by using UDP broadcasts, but receive DHCP lease offer, and acknowledgement messages by unicast.

A DHCP server processes the following incoming DHCP messages from a DHCP client based on the current state of the binding for that client: DHCPDISCOVER, DHCPREQUEST, and also such as DHCPDECLINE, DHCPRELEASE, and DHCPINFORM. A DHCP server responds to the client with the following DHCP messages: DHCPOFFER, DHCPACK, and also such as DHCPNAK.

DHCPDISCOVER—A message that a DHCP client broadcasts to locate available DHCP servers

DHCPOFFER—A message that a DHCP server sends to DHCP clients in response to discovery messages with an offer for client configuration parameters

DHCPREQUEST—A message that a DHCP client sends to DHCP servers either requesting the offered parameters from one server, and implicitly declining offers from all others, or confirming correctness of previously allocated address after a system reboot, or extending the lease on a particular network address.

DHCPACK—A message that a DHCP server sends to DHCP clients with configuration parameters, including committed network addresses.

The DHCP probe in your Cisco ISE deployment, when enabled, allows the Cisco ISE profiling service to re-profile endpoints based only on new requests of INIT-REBOOT, and SELECTING message types. Though other DHCP message types are processed such as RENEWING, and REBINDING, they are not used for profiling endpoints. Any attribute parsed out of DHCP packets is mapped to endpoint attributes.

DHCPREQUEST Generated During INIT-REBOOT State:

If the DHCP client checks to verify a previously allocated and cached configuration, then the client must not fill in the Server identifier (server-ip) option, but fill in the Requested IP address (requested-ip) option with its notion of the previously assigned IP address, and fill in the ‘ciaddr’ (client’s network address) field with zero in its DHCPREQUEST message. The DHCP server sends a DHCPNAK message to the client, if the requested IP address is incorrect, or the client is located on the wrong network.

DHCPREQUEST Generated During SELECTING State:

The DHCP client inserts the IP address of the selected DHCP server in the Server identifier option, fill in the Requested IP address (requested-ip) option with the ‘yiaddr’ field value from the chosen DHCPOFFER by the client, and fill in the ‘ciaddr’ field with zero in its DHCPREQUEST message.

Table 18-5 describes the different states of DHCP client messages. For more information on DHCP, refer to www.faqs.org/rafts/rfc2131.html.

Table 18-5 DHCP Client Messages from Different States

	INIT-REBOOT	SELECTING	RENEWING	REBINDING
broadcast/unicast	broadcast	broadcast	unicast	broadcast

Table 18-5 DHCP Client Messages from Different States (continued)

	INIT-REBOOT	SELECTING	RENEWING	REBINDING
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP address	IP address

DHCP IP Helper

DHCP clients send out discovery messages (broadcast) to locate a DHCP server on a network, and in the process, these messages are relayed to the remote DHCP servers as unicast. When DHCP clients and servers are not located on the same subnet, you can configure the network access devices on your network by using the "ip helper-address x.x.x.x" command along with the IP addresses of DHCP servers. This helps the Cisco ISE profiler to receive DHCP packets from one or more interfaces, and parse them to capture endpoint attributes, which can be used for profiling.

For example,

```
Router(config-if)#ip helper-address x.x.x.x
```

You can create a profiling condition of DHCP type, where you can use the dhcp-requested-address attribute for profiling an endpoint. For a fully qualified domain name (FQDN) lookup, the Domain Service Name (DNS) probe extracts the source IP address from the dhcp-requested-address attribute, which is collected by the DHCP

Wireless LAN Controller Configuration

It is recommended that you configure WLCs in DHCP bridging mode, where you can forward all the DHCP packets from the wireless clients to Cisco ISE. You must also ensure that the DHCP IP helper command points to the Cisco ISE Policy Service node.

You must clear the Enable DHCP Proxy check box in the WLCs by using the WLC web interface: **Controller > Advanced > DHCP Master Controller Mode > DHCP Parameters > Enable DHCP proxy**.

Configuring the DHCP SPAN Probe

Table 18-6 describes the fields that allow you to configure the DHCP SPAN probe on the Edit Nodes page.

To enable the DHCP SPAN probe, configure the following fields:

Table 18-6 DHCP SPAN Configuration

Field	Description
The Enable check box	To enable the DHCP SPAN probe on a node, check the **Enable** check box. To disable the DHCP SPAN probe on a node, uncheck the **Enable** check box.
Interface	Click the drop-down arrow to choose the interface.
Description	The description of the DHCP SPAN probe.

DHCP Switched Port Analyzer (SPAN) probe, when initialized on a Cisco ISE node, listens to network traffic, which are coming from network access devices on a specific interface. You need to configure network access devices to forward DHCP SPAN packets to the Cisco ISE profiler from the DHCP servers. The profiler receives these DHCP SPAN packets and parses them to capture the attributes of an endpoint, which can be used for profiling endpoints.

You can create a profiling condition of DHCP type, where you can use the dhcp-requested-address attribute for profiling an endpoint. For a FQDN lookup, the Domain Service Name (DNS) probe extracts the source IP address from the dhcp-requested-address attribute, which is collected by the DHCP SPAN probe.

Configuring the HTTP Probe

Table 18-7 describes the fields that allow you to configure the HTTP probe on the Edit Nodes page.

To enable the HTTP probe, configure the following fields:

Table 18-7 HTTP Configuration

Field	Description
The Enable check box	To enable the HTTP probe on a node, check the **Enable** check box. To disable the HTTP probe on a node, uncheck the **Enable** check box.
Interface	Click the drop-down arrow to choose an interface.
Description	The description of the HTTP probe.

Hypertext Transfer Protocol (HTTP) is an application layer protocol, which is designed within the framework of the Internet Protocol Suite. It is a generic, stateless, protocol which can be used in distributed object management systems beyond its use for hypertext. It functions as a request-response protocol, which is widely used for communications within distributed client-server architectures. A web browser is a client application (often referred as user agent), which implements HTTP originating an HTTP request message. When the web browser operates, it typically identifies itself, its application type, operating system, software vendor, and software revision by submitting a characteristic identification string to its operating peer. In HTTP, this is transmitted in an HTTP request-header field User-Agent.

The User-Agent is an attribute, which can be used to create a profiling condition of IP type, and check the web browser information. The profiler captures the web browser information from the User-Agent attribute, as well as other HTTP attributes from the request messages, and add them to the list of endpoint attributes. Cisco ISE provides many default profiles, which are built into the system to identify endpoints based on the User-Agent attribute.

HTTP SPAN Probe

An HTTP session is a sequence of network request-response transactions. The web browser initiates an HTTP request message, which establishes a Transmission Control Protocol (TCP) connection to a particular port on the web server (typically port 80). A web server listening on that port waits for the HTTP request message from the web browsers. The HTTP probe in your Cisco ISE deployment, when enabled with the SPAN probe, allows the profiler to capture HTTP packets from the specified interfaces. You can use the SPAN capability on port 80, where the Cisco ISE server listens to communication from the web browsers.

HTTP Switched Port Analyzer (SPAN) collects HTTP attributes of an HTTP request-header message along with the IP addresses in the IP header (L3 header), which can be associated to an endpoint based on the MAC address of an endpoint in the L2 header. This information is useful for identifying different mobile and portable IP enabled devices such as Apple devices, as well as computers with different operating systems. Identifying different mobile and portable IP enabled devices is now made more reliable by having the Cisco ISE server redirect capture during a guest login or client provisioning download. This allows the profiler to collect the User-Agent attribute, as well as other HTTP attributes, from the request messages and then identify devices such as Apple devices. The Cisco ISE server listens to communication from the web browsers on both port 80, as well as port 8080.

You can create a profiling condition of IP type, where you can use the IP attribute to capture the source IP address of the web browser. For an FQDN lookup, the Domain Service Name (DNS) probe extracts the source IP address from the IP attribute, which is collected by the HTTP SPAN probe.

Cisco ISE Profiler Does Not Collect HTTP Traffic When the Profiler Is Running On VMware

If you deploy Cisco ISE on an ESX server (VMware), the Cisco ISE profiler collects the DHCP traffic but does not collect the HTTP traffic due to configuration issues on the vSphere client.

In order to collect HTTP traffic on a VMware setup, you have to configure the security settings by changing the Promiscuous Mode to Accept from Reject (by default) of the virtual switch that you create for the Cisco ISE profiler. When the SPAN probe for DHCP and HTTP are enabled, Cisco ISE profiler collects both the DHCP and HTTP traffic.

Configuring the RADIUS Probe

Table 18-8 describes the fields that allow you to configure the RADIUS probe on the Edit Nodes page.

To enable the RADIUS probe, configure the following fields:

Table 18-8 RADIUS Configuration

Field	Description
The Enable check box	To enable the RADIUS probe on a node, check the **Enable** check box. To disable the RADIUS probe on a node, uncheck the **Enable** check box.
Description	The description of the RADIUS probe.

RADIUS is an application layer protocol, which is used in client-server communication. It provides centralized Authentication, Authorization and Accounting (AAA) management for authentication and authorization of users, or devices before granting them access to network services, and also accounting for usage of network services. It supports a variety of methods for user authentication by using user name and password. RADIUS is an extensible protocol, where all the client-server transactions comprise of variable length attribute-value pairs (AVPs), and also new attribute-value pairs can be added without disturbing existing implementations of the protocol. The attribute-value pairs carry data in both the RADIUS request and response messages for authentication, authorization, and accounting transactions.

A Network Access Server (NAS) functions as a client of RADIUS, which provides user credentials to a RADIUS server. The RADIUS server returns configuration information necessary for NAS to deliver requested services to the user. Cisco ISE can function as a RADIUS server, as well as a RADIUS proxy client to other RADIUS servers. When it acts as a proxy client, it uses external RADIUS servers to

process RADIUS requests and response messages. You can configure Cisco ISE for authentication with RADIUS, where you can define a shared secret that you can use in client-server transactions. For more information on Cisco ISE network device configuration, see Chapter 6, "Managing Network Devices."

With the RADIUS request and response messages received from the RADIUS servers, the profiler can collect RADIUS attributes, which can be used for profiling endpoints.

You can create a profiling condition of RADIUS type, where you can use the Framed-IP-Address attribute for profiling an endpoint. For an FQDN lookup, the Domain Service Name (DNS) probe extracts the source IP address from the Framed-IP-Address attribute, which is collected by the RADIUS probe.

For a list of attributes and RADIUS RFCs, refer to http://en.wikipedia.org/wiki/RADIUS.

The following are the known attributes that are collected by the RADIUS probe:

User-Name	NAS-IP-Address	NAS-Port	Framed-IP-Address
Calling-Station-Id	Acct-Session-Id	Acct-Session-Time	Acct-Terminate-Cause

Configuring the Network Scan (NMAP) Probe

Table 18-9 describes the fields that allow you to configure the Network Scan (NMAP) probe on the Edit Nodes page.

To enable the Network Scan probe, configure the following fields:

Table 18-9 Network Scan Configuration

Field	Description
The Enable check box	To enable the Network Scan probe on the Policy Service ISE node, check the **Enable** check box. To disable the Network Scan probe on the Policy Service ISE node, uncheck the **Enable** check box.
Description	The description of the Network Scan probe.
Manual Scan Subnet	Enter a valid subnet to initiate a subnet scan manually. If you enter an invalid subnet, Cisco ISE displays the following error message: "Invalid Subnet." For example, enter a valid subnet format, such as10.10.10.0/8, 10.10.0.0/16, 10.0.0.0/24, and 10.10.10.10/32 in the Manual Scan Subnet field. It is active and available for you to enter the subnet only when you enable the Network Scan probe on the Edit Nodes page to run the manual scan.
Run Scan	Click the **Run Scan** button to start a manual subnet scan. It is only active before you initiate to run the subnet scan manually.
Cancel Scan	Click the **Cancel Scan** button to stop a manual subnet scan. It is only active while the manual subnet scan is running.
Click to see latest scan results link	Click the **Click to see latest scan results** link, which redirects you to **Administration > Identities > Identities** (menu window). Choose **Latest Network Scan Results.** to view the most recently detected endpoints.

A Network Scan

A network scan is a very specific way to scan a subnet on your network, by using the Network Scan probe to run from the Policy Service ISE nodes. The network scan allows you to detect endpoints on a specified subnet, their operating systems, and SNMP ports (UDP 161 and 162) in any distributed deployment.

Cisco ISE displays a message that running a network scan on a specified subnet is a lengthy procedure, as it depends on the size and density of the subnet. Also scanning a subnet is highly resource intensive. You can also cancel a subnet scan at any time while the subnet scan is in progress. The number of active scans is always restricted to one scan, and so you can scan only a single subnet at a time.

Each subnet scan has a unique numeric ID that is used to update an endpoint source information with that scan ID. Upon detection, the endpoint source information can also be updated to indicate that it is discovered by the Network Scan probe.

The network scan is augmented with an SNMP Query whenever the scan discovers that UDP port 161 is open on an endpoint. This SNMP Query can result in more attributes being collected for greater classification accuracy. The SNMP Query uses the default community string settings (public), which allows you to collect additional attributes such as the system description, and others.

Depending on the location of the subnet that you are scanning, the Network Scan may or may not return the MAC addresses of endpoints. The Network Scan may not be able to resolve MAC addresses for those endpoints, as an ARP resolution is entirely dependent on the network topology and the subnet being scanned which is away from the Policy Services ISE node. Having implemented an IP-MAC binding, Cisco ISE must be able to resolve their MAC addresses for those endpoints from the IP addresses received. If they are not resolved to MAC addresses, then there is no way to map those IP addresses to actual endpoints, and they are dropped.

The NMAP manual subnet scan requires the MAC address of an endpoint in order to add the endpoint to the database, as the MAC address is the unique identifier for all the endpoints.

The following limitations do not apply to dynamic endpoints that join the Cisco ISE network, as they are authenticated, and assigned to an IP address dynamically, and those endpoints are detected by the profiling service through the RADIUS and DHCP probes.

Cisco ISE enables you to detect devices, by using the NMAP manual subnet scan. The manual subnet is useful to detect devices that are constantly connected to the ISE network with a static IP address assigned to them, such as printers, and therefore those devices cannot be discovered by other probes.

Scanned devices are added to the endpoints list, only if the IP address to the MAC address binding exists. During the manual subnet scan, the NMAP probe detects whether the SNMP port 161 is open on the device. If the port is open, an SNMP Query is triggered with a default community string (public). If the device supports SNMP and the default community string is set to public, you can obtain the MAC address of the device from the MIB value “ifPhysAddress”.

When scanning a subnet that is not adjacent to the Policy Service node, but contains devices in the subnet that do not support SNMP, then you have to define the NAD that resides in the subnet in the Cisco ISE administrator user interface. You must also enable the SNMP probe on the Policy Service node in order to retrieve the ARP table from the NAD that provides the IP address to MAC address binding for those endpoints that are scanned in the subnet.

If there is a L2 adjacency to the Policy Service node that performs the manual subnet scan, the NMAP scan can detect the MAC address, and add the endpoints to Cisco ISE.

For an iDevice, and other devices that do not support SNMP, the MAC address can be discovered by the ARP table, which can be queried from the network access device (NAD) by an SNMP Query probe. iDevices can also be profiled using DHCP.

Latest Network Scan Results

The most recent network scan results are stored in **Administration > Identities > Identities (menu window) > Latest Network Scan Results**.

For more information on the latest network scan results, see the section on Latest Network Scan Results, page 4-26.

For more information on the manual network scan, see Chapter 18, "Configuring the Network Scan (NMAP) Probe."

Configuring the DNS Probe

Table 18-10 describes the fields that allow you to configure the DNS probe on the Edit Nodes page.

To enable the DNS probe, configure the following fields:

Table 18-10 DNS Configuration

Field	Description
The Enable check box	To enable the DNS probe on a node, check the **Enable** check box. To disable the DNS probe on a node, uncheck the **Enable** check box.
Timeout	Enter the timeout in seconds.
Description	The description of the DNS probe.

Note For the DNS probe to work on a particular ISE node in a distributed deployment, you must enable any one of the following probes: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. For a DNS lookup, one of the probes mentioned above must be started along with the DNS probe.

When you deploy Cisco ISE in a standalone, or in a distributed environment for the first time, you are prompted to run the setup utility to configure the Cisco ISE appliance. Here, you will configure the Domain Name System (DNS) domain and the primary nameserver (primary DNS server), where you can configure one primary nameserver, and one or more nameservers during setup. You can also change, or add DNS nameservers later after deploying Cisco ISE using the CLI commands.

For more information on the CLI commands, refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

The DNS probe in your Cisco ISE deployment, when enabled, allows the profiler to lookup an endpoint, and get the fully qualified domain name (FQDN) of that endpoint. A DNS lookup tries to determine the endpoint fully qualified domain name. Upon an endpoint detection on your Cisco ISE enabled network, a list of endpoint attributes is collected from the NetFlow, DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP probes. For a DNS lookup, one of the following probes must be started along with the DNS probe: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP.

The following list shows the specific endpoint attribute, and the probe that collects the attribute:

- The dhcp-requested-address attribute—an attribute collected by the DHCP, and DHCP SPAN probes
- The SourceIP attribute—an attribute collected by the HTTP probe
- The Framed-IP-Address attribute—an attribute collected by the RADIUS probe

- The cdpCacheAddress attribute—an attribute collected by the SNMP probe

This allows the DNS probe in the profiler to do a reverse DNS lookup (FQDN lookup) against specified name servers that you define in your Cisco ISE deployment. A new attribute is added to the attribute list for an endpoint, which can be used for an endpoint profiling policy evaluation. The FQDN is the new attribute, which exists in the system IP dictionary. You can create an endpoint profiling condition to validate the FQDN attribute, and its value for profiling.

Inline Posture Deployment in Bridged Mode and DNS Probe

For more information on Inline Posture deployment, see Chapter 10, "Setting Up Inline Posture."

For DNS probe to work with Inline Posture deployment in the Bridged mode, you must ensure that you configure the callStationIdType information sent in RADIUS messages for the Wireless LAN Controllers (WLC). The WLCs need to be configured to send the calling station ID in the MAC address format instead of the current IP address format in RADIUS messages. Once configured in the WLCs, this configuration uses the selected calling station ID for communications with RADIUS servers and other applications. It results in endpoints authentication, and then the DNS probe to do a reverse DNS lookup (FQDN lookup) against the specified name servers, and update the FQDN of endpoints.

Wireless LAN Controller GUI Configuration

You can use the WLC web interface to configure the Call Station ID Type information. You can go to the Security tab of the WLC web interface, and choose RADIUS > Authentication from AAA. Here, you can configure the System MAC Address from the drop-down list to the Call Station ID Type on the RADIUS Authentication Servers page. The MAC Delimiter field is set to Colon by default.

For more information on various WLC GUI configuration, refer to the Using the GUI to Configure RADIUS section (Chapter 6, Configuring Security Solutions) in the *Cisco Wireless LAN Controller Configuration Guide, Release 7.0*.

Wireless LAN Controller CLI Configuration

You can use the config radius callStationIdType command with the macAddr option in the command-line interface (CLI) for the Wireless LAN Controllers.

For more information on WLC CLI configuration, refer to the config radius callStationIdType command (Chapter 2, CLI Commands) in the *Cisco Wireless LAN Controller Command Reference, Release 7.0.*

For example, you can go to the configuration mode for the WLCs, and enter the following command:

config radius callStationIdType {ipAddr | macAddr | ap-macAddr-only | ap-macAddr-ssid}

Syntax Description

config	Configure parameters.
radius callStationIdType	Configure callStationIdType information.

{ipAddr | macAddr | ap-macAddr-only | ap-macaddr-ssid}	• Enter ipAddr to configure Call Station ID type to IP address (only layer 3) • Enter macAddr to configure Call Station ID type to the system's MAC address (layers 2 and 3) • Enter ap-macAddr-only to configure Call Station ID type to use the access point's MAC address (layers 2 and 3) • Enter as-macAddr-ssid to config Call Station ID type to use the access point's MAC address with SSID

Command Modes Configuration.

Usage Guidelines The Framed-IP-Address attribute in RADIUS messages does not contain the Call Station ID type in the MAC address format. Therefore, RADIUS messages cannot be associated with the MAC address of endpoints, and the DNS probe is unable to perform the reverse DNS lookup. In order to profile endpoints, you must enable the RADIUS, and DNS probes in Cisco ISE, and then configure the WLCs to send the calling station ID in the MAC address format instead of the current IP address format in RADIUS messages.

Examples

```
config radius callStationIdType macAddr
```

Configuring the SNMP Query Probe

Table 18-11 describes the fields that allow you to configure the SNMP Query probe on the Edit Nodes page.

To enable the SNMP Query probe, configure the following fields:

Table 18-11 SNMP Query Configuration

Field	Description
The Enable check box	To enable the SNMP Query probe on a node, check the **Enable** check box. To disable the SNMP Query probe on a node, uncheck the **Enable** check box.
Retries	Enter the number of retry attempts allowed**.**
Timeout	Enter the timeout in seconds.
EventTimeout	Enter the SNMP event timeout in seconds.
Description	The description of the SNMP Query probe.

For more information on SNMP, see the "Simple Network Management Protocol" section on page 18-30.

From the Network Devices list page, you can configure new network devices where SNMP settings can also be configured. The polling interval that you specify here query network access devices at regular intervals. In addition to configuring the SNMP Query probe, you must also configure other SNMP settings in the following location:

Administration > Network Resources > Network Devices.

You can turn on and turn off SNMP querying for specific NADs based on the following configurations:

- SNMP Query on Link up and New MAC notification turned on or turned off
- CDP SNMP Query on Link up and New MAC notification turned on or turned off
- SNMP Query timer for once an hour for each switch by default

Note When you configure SNMP settings on the network devices, you must ensure that the Cisco Device Protocol (CDP) is enabled (by default) on all the ports of the network devices. If you disable CDP on any of the ports on the network devices, then you may not be able to profile properly as you will miss the CDP information of all the connected endpoints. You must also ensure that the Link Layer Discovery Protocol (LLDP) is running on all the ports of the network devices.

CDP Attributes Collection

Cisco Discovery Protocol (CDP) is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches). CDP allows network management applications to automatically discover and learn about other Cisco devices that are connected to the network.

You must enable CDP globally by using the **cdp run** command on a network device, and enable CDP by using the **cdp enable** command on any interface of the network access device. To disable CDP on the network device and on the interface, use the **no** keyword at the beginning of the command.

LLDP Attributes Collection

IEEE 802.1AB Link Layer Discovery Protocol (LLDP) is a neighbor discovery protocol that runs over Layer 2 (the data link layer), which allows two systems running different network layer protocols to learn about each other. LLDP is used for network devices to advertise information about themselves to other devices on the network. A switch that supports the IEEE 802.1AB LLDP provides support to devices that are not cisco devices, and it allows for inter operability between other devices.

The Cisco ISE profiler has enhanced data collection capabilities, because it uses an SNMP Query to collect LLDP attributes. You can also collect LLDP attributes from an IOS sensor, which is embedded in the network device by using the RADIUS probe.

You must enable LLDP globally to allow a device to send LLDP packets, by using the **lldp run** command on a network device, but no changes are required at the interface level. You can also configure any interface to send and receive LLDP packets, by using the **lldp transmit** and **lldp receive** commands. To disable LLDP on the network device and on the interface, use the **no** keyword at the beginning of the command.

To change the default LLDP settings, use the LLDP global configuration and LLDP interface configuration commands on the network access devices.

Table 18-12 shows the default LLDP configuration.

Table 18-12 Default LLDP Configuration

Feature	Feature
LLDP global state	Disabled
LLDP holdtime (before discarding)	120 seconds
LLDP timer (packet update frequency)	30 seconds
LLDP reinitialization delay	2 seconds
LLDP tlv-select	Enabled to send and receive all TLVs.
LLDP interface state	Enabled
LLDP receive	Enabled
LLDP transmit	Enabled
LLDP med-tlv-select	Enabled to send all LLDP-MED TLVs

The **Attribute List** of an endpoint displays a single character value for lldpCacheCapabilities and lldpCapabilitiesMapSupported attributes. The values are the Capability Codes that are displayed for the network access device that runs cdp and lldp.

Example1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

Example2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

Example 3

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

LLDP-MIB (v1)

For more information, see LLDP-MIB (v1). LLDP-MIB (v1) is MIB that was recently added to the existing list of supported MIBs for an SNMP Query.

The local attributes are collected once during an SNMP Query as a result of polling LLDP capable local network devices. The remote attributes are tabular, and they correspond to each LLDP capable remote device that is attached to the local network device. These attributes are collected during an SNMP Query

as a result of polling the MIB, as well as when a notification is received through traps or a RADIUS Accounting Start message (a RADIUS Accounting Request packet containing an Acct-Status-Type attribute with the value “start”).

The Cisco ISE profiler reads all the remote attributes of LLDP capable network devices and associates them to the local attributes by using MIB data when creating endpoints.

For example, Cisco ISE creates an endpoint when it reads the lldpRemSysName (a remote attribute) of an endpoint and associates it to lldpLocSysName (a local attribute) that represents its own system name attribute.

The following are the local attributes that are collected from the lldpLocalSystemData group:

lldpLocalSystemData group(1.0.8802.1.1.2.1.3)—refers to iso(1). std(0). iso8802(8802). ieee802dot1(1). ieee802dot1mibs(1). lldpMIB(2). lldpObjects(1). lldpLocalSystemData(3)

lldpLocSysCapSupported	1.0.8802.1.1.2.1.3.5.0
lldpLocSysCapEnabled	1.0.8802.1.1.2.1.3.6.0

The following are the remote attributes that are collected from the lldpRemoteSystemsData group that refers to the attributes of LLDP capable remote network devices:

lldpRemoteSystemsData group(1.0.8802.1.1.2.1.4)—refers to iso(1). std(0). iso8802(8802). ieee802dot1(1). ieee802dot1mibs(1). lldpMIB(2). lldpObjects(1). lldpRemoteSystemsData(4)

lldpRemPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpRemPortDesc	1.0.8802.1.1.2.1.4.1.1.8
lldpRemSysName	1.0.8802.1.1.2.1.4.1.1.9
lldpRemSysDesc	1.0.8802.1.1.2.1.4.1.1.10
lldpRemSysCapSupported	1.0.8802.1.1.2.1.4.1.1.11
ldpRemSysCapEnabled	1.0.8802.1.1.2.1.4.1.1.12

Configuring the SNMP Trap Probe

Table 18-13 describes the fields that allow you to configure the SNMP Trap probe in the Edit Nodes page.

To enable the SNMP TRAP probe, configure the following fields:

Table 18-13 SNMP Trap Configuration

Field	Description
The Enable check box	To enable the SNMP Trap probe on a node, check the **Enable** check box. To disable the SNMP Trap probe on a node, uncheck the **Enable** check box.
Link Trap Query check box	To receive and interpret the linkup and linkdown notifications received through the SNMP Trap, check the **Link Trap Query** check box.
MAC Trap Query check box	To receive and interpret MAC notifications received through the SNMP Trap, check the **MAC Trap Query** check box.

Table 18-13 SNMP Trap Configuration

Field	Description
Interface	Click the drop-down arrow to choose the interface.
Port	Enter the port number.
Description	The description of the SNMP Trap probe.

The SNMP Trap receives information from the specific NADs that support MAC notification, linkup, linkdown, and informs. For SNMP Trap to be fully functional, you must enable SNMP Query also. The SNMP Trap probe receives information from the specific NADs when ports come up or go down and endpoints disconnect or connect to your network. The information received is not sufficient to create endpoints in Cisco ISE.

Note Cisco ISE does not support SNMP Traps that are received from the Wireless LAN Controllers (WLCs) and Access Points (APs).

For more information on supported MIBs in Cisco ISE, refer to the SNMP OID Mapping, page 18-31.

For SNMP Trap probe has to be fully functional and create endpoints in Cisco ISE, the SNMP Query must also be enabled so that the SNMP Query probe triggers a poll event on the particular port of the NAD when a trap is received. In order to make this feature to be fully functional you should configure the NAD and SNMP Trap.

For more information on configuring network devices, see Chapter 6, "Managing Network Devices."

To configure the NAD, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 Click **Add**.

Step 3 Enter the name of the network device.

Step 4 Enter the description of the network device.

Step 5 Check the **SNMP Settings** check box.

Step 6 Choose the SNMP version (mandatory field) from the drop-down list.

You can choose SNMP version 1, 2c, or 3.

Step 7 Configure other mandatory SNMP settings as required depending on the SNMP version you choose.

Step 8 From the **Polling interval field** (mandatory field), enter the SNMP polling interval in seconds.

Step 9 Enable **Link Trap Query**.

Step 10 Enable **MAC Trap Query**.

Step 11 Click **Summit**.

To configure the SNMP Trap, complete the following steps:

Step 1 Choose **Administration > System > Deployment > Deployment Nodes List > Edit Node > Profiling Configuration**.

Step 2 Enable **Link Trap Query**.

Step 3 Enable **Mac Trap Query**.

Step 4 Choose the **Interface** from the drop-down list.

For example, GigabitEthernet 0.

Step 5 Enter the **Port** number.

For example, 162.

Step 6 Enter the description of the SNMP Trap.

For example, SNMP TRAP.

Step 7 Click **Save**.

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. It is a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. It is used mostly in network-management systems (NMS) to monitor network-attached devices for conditions that warrant administrative attention.

SNMP exposes management data in the form of variables on the managed devices, which describe the system configuration. These variables can be queried, and at sometimes can also be set by the managing applications. SNMP permits active network management tasks such as modifying, and applying new configurations through remote modification of these variables. These variables, which are accessible via SNMP are all organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable) are described by Management Information Bases (MIBs). A MIB is a virtual database and the database is hierarchical (tree-structured). The entries are addressed through object identifiers (OID). An object identifier (or object ID or OID) uniquely identifies a managed object in the MIB hierarchy. The managed object (sometimes called a MIB object, or an object, or a MIB) is one of any number of the special characteristics of the managed device. Managed objects are made up of one or more object instances (identified by their OIDs), which are essentially variables.

For more information, refer to RFC 1155, “Structure and Identification of Management Information for TCP/IP based internets”, and its two companions, RFC 1213, “Management Information Base for Network Management of TCP/IP-based internets", and RFC 1157, “A Simple Network Management Protocol.”

For a network-management system to understand a trap sent to it by an agent, the management system must know what the object identifier (OID) defines. It must have the MIB for that trap loaded. This provides the correct OID information so that the network-management system can understand the traps sent to it.

1.3.6.1.2.1 is the base OID for MIB-2 defined SNMP variables, and 1.3.6.1.4.1 is the base OID for IANA-registered Private Enterprises, and IEEE8021-PAE-MIB: RFC IEEE 802.1X for managing IEEE 802.1X.

For more information on supported MIBs in Cisco ISE, refer to the SNMP OID Mapping, page 18-31.

An SNMP-managed network consists of three key components: managed devices, agents, and network-management systems (NMSs).

A managed device is a network node that implements an SNMP interface that allows unidirectional (read-only) or bidirectional access to node-specific information. Managed devices exchange node-specific information with the NMSs using SNMP. Sometimes called network elements, these managed devices can include, but not limited to, routers, access servers, switches, bridges, hubs, IP telephones, IP video cameras, computer hosts, and printers.

An agent is a network-management software module that resides on a managed device. An agent has local knowledge of management information, and translates this information into a form compatible with SNMP.

An NMS executes applications, which monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network-management. One or more NMSs must exist on any managed network.

SNMP OID Mapping

#IF-MIB
1.3.6.1.2.1.2.2.1.1=ifIndex
1.3.6.1.2.1.2.2.1.2=ifDescr
1.3.6.1.2.1.2.2.1.3=ifType
1.3.6.1.2.1.2.2.1.5=ifSpeed
1.3.6.1.2.1.2.2.1.6=ifPhysAddress
1.3.6.1.2.1.2.2.1.7=ifAdminStatus
1.3.6.1.2.1.2.2.1.8=ifOperStatus

#SNMPv2-MIB
1.3.6.1.2.1.1=system
1.3.6.1.2.1.1.1.0=sysDescr
1.3.6.1.2.1.1.2.0=sysObjectID
1.3.6.1.2.1.1.3.0=sysUpTime
1.3.6.1.2.1.1.4.0=sysContact
1.3.6.1.2.1.1.5.0=sysName
1.3.6.1.2.1.1.6.0=sysLocation
1.3.6.1.2.1.1.7.0=sysServices
1.3.6.1.2.1.1.8.0=sysORLastChange
1.3.6.1.2.1.1.9.0=sysORTable

#IP-MIB
1.3.6.1.2.1.4.20.1.2=ipAdEntIfIndex
1.3.6.1.2.1.4.20.1.3=ipAdEntNetMask
1.3.6.1.2.1.4.22.1.2=ipNetToMediaPhysAddress

#CISCO-CDP-MIB
1.3.6.1.4.1.9.9.23.1.2.1.1=cdpCacheEntry
1.3.6.1.4.1.9.9.23.1.2.1.1.1=cdpCacheIfIndex
1.3.6.1.4.1.9.9.23.1.2.1.1.2=cdpCacheDeviceIndex
1.3.6.1.4.1.9.9.23.1.2.1.1.3=cdpCacheAddressType
1.3.6.1.4.1.9.9.23.1.2.1.1.4=cdpCacheAddress
1.3.6.1.4.1.9.9.23.1.2.1.1.5=cdpCacheVersion
1.3.6.1.4.1.9.9.23.1.2.1.1.6=cdpCacheDeviceId
1.3.6.1.4.1.9.9.23.1.2.1.1.7=cdpCacheDevicePort
1.3.6.1.4.1.9.9.23.1.2.1.1.8=cdpCachePlatform
1.3.6.1.4.1.9.9.23.1.2.1.1.9=cdpCacheCapabilities

1.3.6.1.4.1.9.9.23.1.2.1.1.10=cdpCacheVTPMgmtDomain
1.3.6.1.4.1.9.9.23.1.2.1.1.11=cdpCacheNativeVLAN
1.3.6.1.4.1.9.9.23.1.2.1.1.12=cdpCacheDuplex
1.3.6.1.4.1.9.9.23.1.2.1.1.13=cdpCacheApplianceID
1.3.6.1.4.1.9.9.23.1.2.1.1.14=cdpCacheVlanID
1.3.6.1.4.1.9.9.23.1.2.1.1.15=cdpCachePowerConsumption
1.3.6.1.4.1.9.9.23.1.2.1.1.16=cdpCacheMTU
1.3.6.1.4.1.9.9.23.1.2.1.1.17=cdpCacheSysName
1.3.6.1.4.1.9.9.23.1.2.1.1.18=cdpCacheSysObjectID
1.3.6.1.4.1.9.9.23.1.2.1.1.19=cdpCachePrimaryMgmtAddrType
1.3.6.1.4.1.9.9.23.1.2.1.1.20=cdpCachePrimaryMgmtAddr
1.3.6.1.4.1.9.9.23.1.2.1.1.21=cdpCacheSecondaryMgmtAddrType
1.3.6.1.4.1.9.9.23.1.2.1.1.22=cdpCacheSecondaryMgmtAddr
1.3.6.1.4.1.9.9.23.1.2.1.1.23=cdpCachePhysLocation
1.3.6.1.4.1.9.9.23.1.2.1.1.24=cdpCacheLastChange

# CISCO-VTP-MIB
1.3.6.1.4.1.9.9.46.1.3.1.1.18.1=vtpVlanIfIndex
1.3.6.1.4.1.9.9.46.1.3.1.1.4.1=vtpVlanName
1.3.6.1.4.1.9.9.46.1.3.1.1.2.1=vtpVlanState

# CISCO-STACK-MIB
1.3.6.1.4.1.9.5.1.4.1.1.11=portIfIndex
1.3.6.1.4.1.9.5.1.9.3.1.3.1=vlanPortVlan

# BRIDGE-MIB
1.3.6.1.2.1.17.4.3.1.2=dot1dTpFdbPort
1.3.6.1.2.1.17.1.4.1.2=dot1dBasePortIfIndex

# OLD-CISCO-INTERFACE-MIB
1.3.6.1.4.1.9.2.2.1.1.20=locIfReason

# CISCO-LWAPP-AP-MIB
1.3.6.1.4.1.9.9.513.1.1.1=cLApEntry
1.3.6.1.4.1.9.9.513.1.1.1.1.1=cLApSysMacAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.2=cLApIfMacAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.3=cLApMaxNumberOfDot11Slots
1.3.6.1.4.1.9.9.513.1.1.1.1.4=cLApEntPhysicalIndex
1.3.6.1.4.1.9.9.513.1.1.1.1.5=cLApName
1.3.6.1.4.1.9.9.513.1.1.1.1.6=cLApUpTime
1.3.6.1.4.1.9.9.513.1.1.1.1.7=cLLwappUpTime
1.3.6.1.4.1.9.9.513.1.1.1.1.8=cLLwappJoinTakenTime
1.3.6.1.4.1.9.9.513.1.1.1.1.9=cLApMaxNumberOfEthernetSlots
1.3.6.1.4.1.9.9.513.1.1.1.1.10=cLApPrimaryControllerAddressType
1.3.6.1.4.1.9.9.513.1.1.1.1.11=cLApPrimaryControllerAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.12=cLApSecondaryControllerAddressType
1.3.6.1.4.1.9.9.513.1.1.1.1.13=cLApSecondaryControllerAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.14=cLApTertiaryControllerAddressType
1.3.6.1.4.1.9.9.513.1.1.1.1.15=cLApTertiaryControllerAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.16=cLApLastRebootReason
1.3.6.1.4.1.9.9.513.1.1.1.1.17=cLApEncryptionEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.18=cLApFailoverPriority
1.3.6.1.4.1.9.9.513.1.1.1.1.19=cLApPowerStatus
1.3.6.1.4.1.9.9.513.1.1.1.1.20=cLApTelnetEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.21=cLApSshEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.22=cLApPreStdStateEnabled

1.3.6.1.4.1.9.9.513.1.1.1.1.23=cLApPwrInjectorStateEnabled
1.3.6.1.4.1.9.9.513.1.1.1.1.24=cLApPwrInjectorSelection
1.3.6.1.4.1.9.9.513.1.1.1.1.25=cLApPwrInjectorSwMacAddr
1.3.6.1.4.1.9.9.513.1.1.1.1.26=cLApWipsEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.27=cLApMonitorModeOptimization
1.3.6.1.4.1.9.9.513.1.1.1.1.28=cLApDomainName
1.3.6.1.4.1.9.9.513.1.1.1.1.29=cLApNameServerAddressType
1.3.6.1.4.1.9.9.513.1.1.1.1.30=cLApNameServerAddress
1.3.6.1.4.1.9.9.513.1.1.1.1.31=cLApAMSDUEnable
1.3.6.1.4.1.9.9.513.1.1.1.1.32=cLApEncryptionSupported
1.3.6.1.4.1.9.9.513.1.1.1.1.33=cLApRogueDetectionEnabled

# CISCO-LWAPP-DOT11-CLIENT-MIB
1.3.6.1.4.1.9.9.599.1.3.1.1=cldcClientEntry
1.3.6.1.4.1.9.9.599.1.3.1.1.1=cldcClientMacAddress
1.3.6.1.4.1.9.9.599.1.3.1.1.2=cldcClientStatus
1.3.6.1.4.1.9.9.599.1.3.1.1.3=cldcClientWlanProfileName
1.3.6.1.4.1.9.9.599.1.3.1.1.4=cldcClientWgbStatus
1.3.6.1.4.1.9.9.599.1.3.1.1.5=cldcClientWgbMacAddress
1.3.6.1.4.1.9.9.599.1.3.1.1.6=cldcClientProtocol
1.3.6.1.4.1.9.9.599.1.3.1.1.7=cldcAssociationMode
1.3.6.1.4.1.9.9.599.1.3.1.1.8=cldcApMacAddress
1.3.6.1.4.1.9.9.599.1.3.1.1.9=cldcIfType
1.3.6.1.4.1.9.9.599.1.3.1.1.10=cldcClientIPAddress
1.3.6.1.4.1.9.9.599.1.3.1.1.11=cldcClientNacState
1.3.6.1.4.1.9.9.599.1.3.1.1.12=cldcClientQuarantineVLAN
1.3.6.1.4.1.9.9.599.1.3.1.1.13=cldcClientAccessVLAN
1.3.6.1.4.1.9.9.599.1.3.1.1.14=cldcClientLoginTime
1.3.6.1.4.1.9.9.599.1.3.1.1.15=cldcClientUpTime
1.3.6.1.4.1.9.9.599.1.3.1.1.16=cldcClientPowerSaveMode
1.3.6.1.4.1.9.9.599.1.3.1.1.17=cldcClientCurrentTxRateSet
1.3.6.1.4.1.9.9.599.1.3.1.1.18=cldcClientDataRateSet

# CISCO-AUTH-FRAMEWORK-MIB
1.3.6.1.4.1.9.9.656.1.2.1.1=cafPortConfigEntry
1.3.6.1.4.1.9.9.656.1.4.1.1.2=cafSessionClientMacAddress
1.3.6.1.4.1.9.9.656.1.4.1.1.5=cafSessionStatus
1.3.6.1.4.1.9.9.656.1.4.1.1.6=cafSessionDomain
1.3.6.1.4.1.9.9.656.1.4.1.1.10=cafSessionAuthUserName
1.3.6.1.4.1.9.9.656.1.4.1.1.12=cafSessionAuthorizedBy
1.3.6.1.4.1.9.9.656.1.4.1.1.14=cafSessionAuthVlan

# EEE8021-PAE-MIB: RFC IEEE 802.1X
1.0.8802.1.1.1.1.2.1.1.5=dot1xAuthAuthControlledPortStatus
1.0.8802.1.1.1.1.2.1.1.6=dot1xAuthAuthControlledPortControl
1.0.8802.1.1.1.1.2.4.1.9=dot1xAuthSessionUserName

SNMP version 1 PDUs

SNMP version 1 (SNMPv1) is the initial implementation of the SNMP protocol. SNMPv1 operates over protocols such as User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), and Novell Internet Packet Exchange (IPX). SNMPv1 is widely used network-management protocol in the internet community.

SNMPv1 specifies the following five core protocol data units (PDUs):

- GetRequest—a manager-to-agent request, which is used to retrieve the value of a variable, or list of variables. A Response with current values for the variables is returned.
- SetRequest—A manager-to-agent request, which is used to change the value of a variable, or list of variables. A Response with (current) new values for the variables is returned.
- GetNextRequest—A manager-to-agent request, which is used to discover available variables and their values. A Response with variable binding for the next variable in the MIB is returned. The entire MIB of an agent can be walked by iterative application of GetNextRequest starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.
- Response—It returns variable bindings, and acknowledgement from the agent to the manager for GetRequest, SetRequest, GetNextRequest, GetBulkRequest and InformRequest. Although it is used as a response to both GetRequest and SetRequest PDUs, this PDU is also called as GetResponse in SNMPv1.
- Trap—It is an asynchronous notification, which is sent from the agent to the manager. The format of the trap message is changed in SNMPv2, and this PDU is renamed as SNMPv2-Trap.

SNMP version 2c PDUs

SNMP version 2 (SNMPv2) is an evolution of the initial version SNMPv1, which includes improvements in the areas of performance, security, confidentiality, and manager-to-manager communications. It introduces GetBulkRequest, an alternative to iterative GetNextRequests of SNMP v1 for retrieving large amounts of management data in a single request. The Community-Based Simple Network Management Protocol version 2 (SNMP v2c) comprises of SNMP v2, which uses the simple community-based security scheme of SNMPv1.

Two other PDUs, GetBulkRequest and InformRequest are added in SNMPv2, and are carried over to SNMPv3.

- GetBulkRequest—It is introduced in SNMPv2. This is an optimized version of GetNextRequest, which is a manager-to-agent request for multiple iterations of GetNextRequest. It returns a Response with multiple variable bindings walked from the variable binding, or bindings in the request.
- InformRequest—It is introduced in SNMPv2. This is an acknowledged asynchronous notification from a manager-to-manager request. This PDU uses the same format as the SNMPv2 version of Trap (SNMPv2-Trap). The manager-to-manager notifications are already possible in SNMPv1 (using a Trap), but as SNMP protocol commonly runs over UDP where delivery is not assured, and dropped packets are not reported, and so the delivery of a Trap is not guaranteed. InformRequest fixes this by sending back an acknowledgement on receipt and the receiver replies with a Response parroting all information in the InformRequest.

SNMP version 3

Although SNMPv3 makes no changes to the protocol, SNMPv3 primarily has added security, and remote configuration enhancements to SNMP.

SNMPv3 provides the following important security features:

- Confidentiality—Encryption of packets to prevent snooping by an unauthorized source
- Integrity—Message integrity to ensure that a packet has not been tampered within transit including an optional packet replay protection mechanism
- Authentication—verifies that the message is from a valid source

Endpoint Profiling Policies

Endpoint profiling policies in Cisco ISE allow you to categorize discovered endpoints on your network, and assign them to specific endpoint identity groups. Cisco ISE creates three identity groups by default, and two other identity groups that are specific to Cisco IP phones and workstations in the system. It also allows you to create your own identity groups to which endpoints can be assigned dynamically or statically. Profiling policies are hierarchical, and they are applied at the endpoint identify groups level. By grouping endpoints to endpoint identity groups, and applying profiling policies to identity groups, Cisco ISE enables you to determine the mapping of endpoints to the endpoint profiles by checking corresponding endpoint profiling policies.

An endpoint profiling policy contains a single condition, or a combination of multiple single conditions that are logically combined against which you can categorize and group endpoints. Cisco ISE always considers a chosen policy for an endpoint rather than an evaluated policy, which is the matched policy when the profiling conditions that are defined in the profiling policy are met for profiling the endpoint in the system.

If the rules of an endpoint profiling policy match, then the profiling policy and the matched policy is the same for that endpoint, which is dynamically discovered on your network. The certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. The certainty factor for all the valid rules are added together and must exceed the minimum certainty factor that is defined in an endpoint profiling policy. Here, the status of static assignment for that endpoint is set to false in the system. But, this can be set to true after it is statically reassigned to an existing profiling policy in the system by using the static assignment feature during an endpoint editing.

Each rule in an endpoint profiling policy has a certainty metric (an integer value) associated to it. The certainty metric is a measure that is added for all the valid rules in an endpoint profiling policy. A rule can also have either an exception action or a network scan action associated to it and the exception action or the network scan action is used to trigger the configurable action while evaluating the profiling policies with respect to the overall classification of endpoints.

Create a Matching Identity Group

This option allows you to create a matching identity group for endpoints and it will be the child of the Profiled identity group when an endpoint profile matches an existing profile.

Use Hierarchy

This option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent endpoint identity group. Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.

Policy Enabled

This option allows you to associate a matching profiling policy, when you profile an endpoint.

Minimum Certainty Factor

Each policy has a minimum certainty metric (an integer value), which is associated to it.

Exception Action

This option allows to trigger an exception action (a single configurable action) that is associated to the endpoint profiling policy, when an endpoint profiling policy matches, and at least one of the exception rules matches.

Network Scan (NMAP) Action

This option allows you to trigger a network scan action (a single configurable action) that is associated to the endpoint profiling policy, when an endpoint profiling policy matches, and at least one of the network scan action rules matches.

To trigger a network scan action that you define in the rule, you must ensure that the Network Scan (NMAP) probe is enabled in the **Administration > System > Deployment > Edit Node > Profiling Configuration**.

Parent Policy

This option allows you to choose an endpoint profiling policy from which you can inherit conditions to its child.

Prerequisite:

Before you begin to configure endpoint profiling policies in Cisco ISE, you should have a basic understanding of the endpoint profiling policies. Review the following:

- Endpoint Profiling Hierarchy, page 18-36
- Unknown Profile, page 18-36
- Profiling Statically Added Endpoint, page 18-36
- Profiling a Static IP Device, page 18-37

Endpoint Profiling Hierarchy

The endpoint profiling policy is hierarchical, where you can inherit rules (one or more conditions) from a parent profiling policy to its child. You can create a generic policy for a device and inherit conditions into its child profiling policies. If an endpoint has to be classified, then the endpoint profile has to first match the parent, and its descendant (child) policies.

For example, if an endpoint has to be classified as a Cisco-IP-Phone 7960, then the endpoint profile for this endpoint has to first match the parent Cisco-Device policy, its child Cisco-IP-Phone policy, and then it matches the Cisco-IP-Phone 7960 profiling policy for better classification.

Unknown Profile

An unknown profile is the default system profile that is assigned to an endpoint, where an attribute or a set of attributes collected for that endpoint do not match with existing profiles in Cisco ISE. When an endpoint is dynamically discovered in Cisco ISE, and there is no matching endpoint profiling policy for that endpoint, it is assigned to the unknown profile. If there is no matching endpoint profiling policy for a statically added endpoint, then you can assign the unknown profile to an endpoint, and change it later.

Profiling Statically Added Endpoint

If you have an endpoint added statically to your network, the statically added endpoint is not profiled by the profiling service in Cisco ISE. For the statically added endpoint to be profiled, the profiling service computes a profile for the endpoint by adding a new MATCHEDPROFILE attribute to the endpoint. The

computed profile is the actual profile of an endpoint when dynamically assigned. This allows you to find the mismatches between in profiling the statically added endpoint by using the computed profile with an endpoint profile for that endpoint when it is dynamically assigned.

The endpoint profiling policy is never changed for the statically added endpoint. For the endpoint that is statically assigned, the profiling service computes the MATCHEDPROFILE. For all the endpoints that are dynamically assigned, the MATCHEDPROFILEs are identical to the endpoint profiles.

Profiling a Static IP Device

If you have an endpoint with a statically assigned IP address, you can create a profile for such static IP devices. If you have the RADIUS probe or SNMP Query and SNMP Trap probes enabled, then you can profile the endpoint.

This section describes the basic operations that allow you to manage endpoint profiling policies from the Endpoint Policies page.

Filtering, Creating, Editing, Duplicating, Importing, and Exporting Endpoint Profiling Policies

Related Topics

Configuring DACLs, page 17-33 section in Chapter 17, "Managing Authorization Policies and Profiles."

Filtering, Creating, Editing, Duplicating, Importing, and Exporting Endpoint Profiling Policies

The Endpoint Policies page allows you to manage endpoint profiling policies, and provides an option to filter profiling policies by their names and description. This page displays a list of predefined policies (default profiles) for Apple devices, notebooks, workstations, printers, access points, smart phones, and gaming consoles.

The procedures for managing endpoint profiling policies includes the following tasks:

- Filtering Endpoint Policies, page 18-37
- Creating an Endpoint Profiling Policy, page 18-40
- Editing an Endpoint Profiling Policy, page 18-49
- Deleting an Endpoint Profiling Policy, page 18-50
- Duplicating an Endpoint Profiling Policy, page 18-50
- Exporting Endpoint Profiling Policies, page 18-51
- Importing Endpoint Profiling Policies, page 18-51

Filtering Endpoint Policies

You can use the Show drop-down list, or click the filter icon to both invoke a quick filter and close it on the Endpoint Policies page. A quick filter is a simple filter that you can use to filter endpoint profiling policies on the Endpoint Policies page. The quick filter filters profiling policies based on field descriptions, such as the endpoint policy name and description on the Endpoint Policies page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, on the Endpoint Policies page. The advanced filter filters profiling policies based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results on the Endpoint Policies page. Once you have created and saved a preset filter, you can choose a preset filter from the list. You can also edit preset filters and remove them from the preset filters list.

To filter endpoint profiling policies, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling** (menu window).

The Profiling menu appears.

Step 2 From the Profiling menu window, choose **Profiling Policies**.

The Endpoint Policies page appears, which lists all the predefined profiling policies.

Step 3 From the Endpoint Policies page, click the Show drop-down arrow to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-14.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 18-38 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 18-38.

Note To return to the profiling policies list, choose **All** from the Show drop-down list to display all the profiling policies without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters profiling policies based on each field description on the Endpoint Policies page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Endpoint Policies page. If you clear the field, it displays the list of all the profiling policies on the Endpoint policies page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter profiling policies by using variables that are more complex. It contains one or more filters that filter profiling policies based on the values that match the field descriptions. A filter on a single row filters profiling policies based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter profiling policies by using any one or all of the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter, and click **Save**, or click **Cancel** to clear the filter.

Table 18-14 describes the fields that allow you to filter the endpoint profiling policies on the Endpoint Policies page.

Table 18-14 Filtering Endpoint Profiling Policies

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Endpoint Policy Name	This field enables you to filter endpoint profiling policies by the name of the endpoint profiling policy.
	Policy Enabled	This field enables you to filter endpoint profiling policies by their association to a matching profiling policy.
	Description	This field enables you to filter endpoint profiling policies by the description of the endpoint profiling policy.
Advanced Filter	Choose the field description from the following: • Endpoint Policy Name • Policy Enabled • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter endpoint profiling policies.
	Value	From the Value field, choose the value for the field description that you selected against, which the endpoint profiling policies are filtered.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Creating an Endpoint Profiling Policy

The Endpoint Policies page allows you to add a new endpoint profiling policy to the existing default profiles. The default profiles are predefined in Cisco ISE, and installed when deployed. As endpoint profiling policies are hierarchical, you can find that the Endpoint Policies page displays the list of generic (parent) policies for some devices such as Apple, Cisco, Aruba, Avaya and HP, and their child policies to which their parent polices are associated on this page. Other policies for all Android and BlackBerry smart phones are also available on this page, which include a set of devices.

Warning **When you choose to create an endpoint profiling policy on the Endpoint Policies page, do not use the Stop button on your web browsers. This action stops the loading of the New profiler Policy page in Cisco ISE. Cisco ISE also loads other list pages when you access them, as well as the menus within the list pages. But it prevents you from performing operations on all the menus within the list pages except the Filter menus. You will need to log out of Cisco ISE, and then log in again to perform operations on all the menus within the list pages.**

To create a profiling policy in the Endpoint Policies page, complete the following steps:

Step 1 Choose **Policy > Profiling**.

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears.

Step 3 From the Endpoint Policies page, choose **Create**.

Modify the values on the New Profiler Policy page, as shown in Table 18-15.

Step 4 Click **Submit.**

The profiling policy that you create appears on the Endpoint Policies page.

Step 5 Click the **Profiler Policy List** link from the New Profiler Policy page to return to the Endpoint Policies page.

Table 18-15 describes the fields on the Endpoint Policies page that allow you to create an endpoint profiling policy.

Table 18-15 Creating an Endpoint Profiling Policy

Field Name	Description
Name	From the Name field, enter the name of the endpoint profiling policy that you want to create.
Description	From the Description field, enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	To associate a matching profiling policy, check the **Policy Enabled** check box.
Minimum Certainty Factor	Enter the minimum value that you want to associate with the profiling policy.
Exception Action	To associate an exception action with the profiling policy, click the drop-down arrow to view exception actions that you have already defined. Choose an exception action.
Network Scan (NMAP) Action	To associate a network scan action with the profiling policy, click the drop-down arrow to view the network scan actions that you have already defined. Choose a network scan action.
Create matching identity group	When checked, this option creates a matching identity group as a child of the Profiled identity group when endpoint profiles match an existing profile. For example, the Xerox-Device endpoint identity group is created on the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile. To create a matching identity group, check the **Create matching identity group** check box.
Use Hierarchy	When checked, this option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Here, endpoints that match the Unknown profile are grouped under Unknown, and endpoints that match an existing profile are grouped under Profiled endpoint identity groups. If endpoints match the Cisco-IP-Phone profile, then they are grouped under Cisco-IP-Phone, and those match the Workstation profile are grouped under Workstation endpoint identity groups. The Cisco-IP-Phone and Workstation are associated to the Profiled endpoint identity group in the system. To assign endpoints to the matching parent endpoint identity group, check the **Use Hierarchy** check box.

Table 18-15 Creating an Endpoint Profiling Policy (continued)

Field Name	Description
Parent Policy	From the Parent Policy field, click the drop-down arrow to view parent policies that exist on the system. Choose a parent policy that you want to associate with the new profiling policy.
Rules	To define the rule, choose one or more profiling conditions from the library, and associate an integer value for the certainty factor for each condition, or associate an action either an exception action or a network scan action for that condition for the overall classification of an endpoint.
If Condition	Choose one or more conditions from the Conditions field. Here, you can save all the conditions that you create to the library by using the Save Icon button. **Note** If you select more than one condition to define an endpoint profiling policy, the conditions are logically combined by using an AND operator by default.
Conditions	Choose the **Select Existing Condition from Library** option or **Create New Condition** option.
Select Existing Condition from Library	If you choose, then you can define an expression by selecting pre-defined conditions from the policy elements library. Click the **Action Icon** button to do the following: • Add Attribute/Value • Add Condition from Library • Delete Here, you can use the AND or OR operator. You can add ad-hoc attribute/value pairs to your expression in the subsequent steps. Click the **Action Icon** button to do the following: • Add Attribute/Value • Add Condition from Library • Duplicate • Add Condition to Library • Delete

Table 18-15 Creating an Endpoint Profiling Policy (continued)

Field Name	Description
Create New Condition (Advance Option)	If you choose, then you can define an expression by selecting attributes from various system or user-defined dictionaries. Click the **Action Icon** button to do the following: • Add Attribute/Value • Add Condition from Library • Duplicate • Add Condition to Library • Delete Here, you can use the AND or OR operator. You can add pre-defined conditions from the policy elements library in the subsequent steps. Click the **Action Icon** button to do the following: • Add Attribute/Value • Add Condition from Library • Delete
Then	Click the drop-down arrow to view, and choose one of the following predefined settings to associate with the profiling condition: • Certainty Factor Increases • Take Exception Action • Take Network Scan Action
Value	If you select the Certainty Factor Increases option, then enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification.
Action Icon	Click the **Action Icon** button to do the following: • Insert new rule above • Insert new rule below • Delete

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

A Quick Reference to Creating a New Endpoint Profiling Policy in Cisco ISE

Cisco ISE provides you with a set of predefined default profiling policies for some endpoints, like workstations, notebooks, IP phones, smart phones, gaming consoles, printers, and fax machines.

Before you create a new endpoint profiling policy for an endpoint on the New Profiler Policy page, it is recommended that you review the following topics:

- Configuring the Probes, page 18-12—This section describes various attribute collection methods that are used in Cisco ISE.
- Endpoint Profiling Policies, page 18-35—This section describes endpoint profiling policies in detail and the fields that are used to configure an endpoint profiling policy.
- Endpoint Profiling, page 18-52—This section describes how to configure conditions (a check) that are necessary to create a rule. A rule contains one or more conditions that are associated with it, and an endpoint profiling policy contains one or more rules.
- Profiling Exception Actions, page 18-58—This section describes a single configurable action that is associated to an endpoint profiling policy.
- Profiling Network Scan Actions, page 18-62—This section describes a single configurable action that is associated to an endpoint profiling policy.
- Endpoints, page 4-15—This section describes on how endpoints are managed statically and dynamically in Cisco ISE.
- Endpoint Identity Groups, page 4-70—This describes on how to manage endpoints in Cisco ISE.

This section guides you on how to create a new endpoint profiling policy for an endpoint on the New Profiler Policy page.

Table 18-15 on page 18-41 describes the fields that you use to create a new endpoint profiling policy.

Cisco ISE provides you with options that allow you to make use of predefined policies, and their hierarchical construction by using the Policy Enabled, Use hierarchy, and Parent Policy options on the New Profiler Policy page. You can also categorize endpoints to a matching endpoint identity group when identified.

Cisco ISE recommends that you create a generic policy (a parent) for a set of endpoints from which its children can inherit the rules and conditions. An endpoint must match a child policy as well as its parent policy in the hierarchy when you are profiling an endpoint. For example, Apple-Device is a generic endpoint profiling policy for all Apple devices. and other policies for Apple devices are children of Apple-Device. You can also create a unique endpoint profiling policy for an endpoint. For example, SonyPS3 is an endpoint profiling policy for a Sony game console.

You must first identify the distinguishing characteristics of the newly identified endpoints in order to profile them appropriately in Cisco ISE. An unknown profile is a default system profile that is assigned to an endpoint, where an attribute or a set of attributes that are collected for that endpoint do not match with existing profiles in Cisco ISE. When an endpoint is dynamically discovered in Cisco ISE, and there is no matching endpoint profiling policy for that endpoint, it is assigned to an unknown profile. If there is no matching endpoint profiling policy for a statically added endpoint, then you can assign the unknown profile to an endpoint, and change it later.

To create an endpoint profiling policy on the New Profiler Policy page, complete the following steps:

Step 1 Go to **Policy > Profiling > Profiling Policies**.

Step 2 From the Endpoint Policies page, choose **Create**.

This section describes how to create an endpoint profile for devices.

Perform the following actions:

- Enter a policy name. You must create a generic (parent) policy for a set of devices, and then create children for the other devices that belong to this group.

  For example, use Apple as the prefix in the policy name for all the policies that you create for Apple devices. Create Apple-Device, a parent endpoint profiling policy for all Apple devices and then create policies for each Apple device, as its children.

- Enter a description for the endpoint profiling policy.

  For example, enter the description as “Generic policy for all Apple devices” for Apple-Device, and “Policy for all Apple MacBooks” for Apple notebooks.

- Check the **Policy Enabled** option.

  For example, Cisco ISE uses all policy enabled endpoint profiling policies and their children to match discovered endpoints.

- Enter a value for **Minimum Certainty Factor**. The certainty values for all the valid conditions are added together to form the matching certainty. It must exceed the minimum certainty factor as defined in the policy, for the policy to be considered as a match.

- Choose an **Exception Action**. The default value is NONE. For more information, see Profiling Exception Actions, page 18-58.

- Choose a **Network Scan (NMAP) Action**. The default value is NONE. For more information, see Profiling Network Scan Actions, page 18-62.

- Choose either to **Create Matching Identity Group** to assign profiled endpoints to an endpoint identity group or choose **Use Hierarchy**.

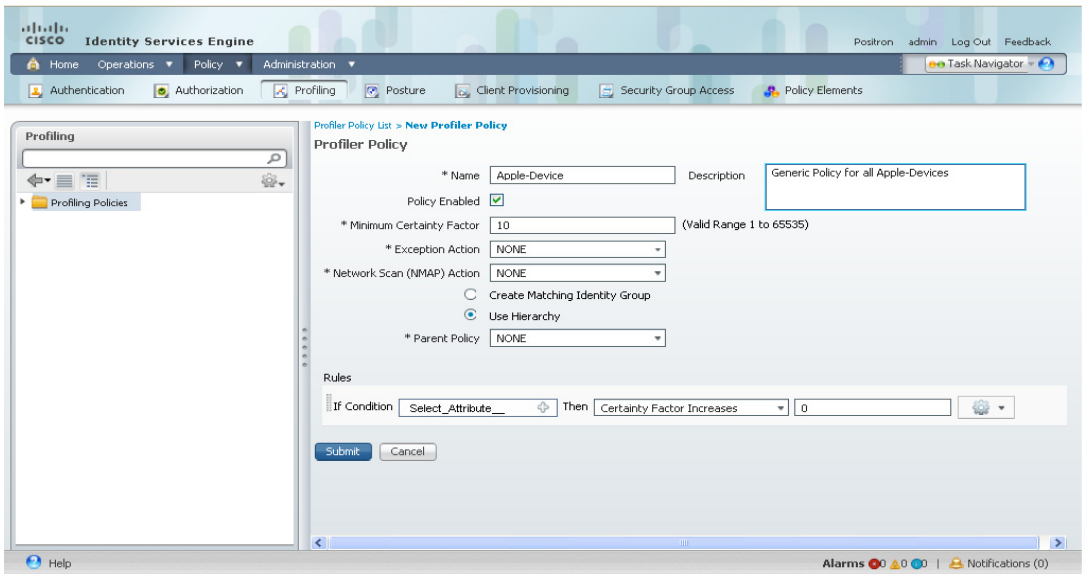
- Choose a **Parent Policy**. It is NONE when you create any parent policy. You can choose a parent endpoint profiling policy from the drop-down list for other policies.

  For example, Apple-Device is the parent policy for all other child policies of Apple devices.

- Define one or more rules for each policy. A rule comprises of one or more conditions that are logically combined using an AND or OR operator. Each rule can be associated with a certainty value, an exception action, or a network scan action. Cisco ISE adds certainty values for all the valid conditions to form the matching certainty from one or more rules, or it initiates an associated exception action or a network scan action when profiling an endpoint.

  When you create a new rule for an endpoint profiling policy, you can choose the existing conditions by using Select Existing Condition from Library. See Figure 18-1.

Figure 18-1 Creating a New Endpoint Profiling Policy



Cisco ISE provides you with a set of predefined checks that you can find in the **Administration > Policy Elements > Conditions > Profiling > Conditions** list page.

To create one or more rules for an endpoint profiling policy, perform the following actions:

- Choose the **Conditions** field. Click the plus [+] sign to expand the Conditions anchored overlay. To close the anchored overlay, click the minus [-] sign.
- Choose **Select Existing Condition from Library**.
- Choose the **Condition Name** field. From the Conditions Name field, click the **Select Condition Quick Picker** (down-arrow) icon. The Dictionaries widget appears, which contains all the checks that you have created and saved in the Administration > Policy Elements > Conditions > Profiling > Conditions list page.
- Choose **Apple-MacBookRuleCheck1**.
- Choose the **AND** or **OR** logical operator.
- Choose **Add Condition from Library** to add another existing condition from the policy elements library. Here, you can also create a new condition and save it to the policy elements library. Choose a new attribute from the list of profiler dictionaries, such as CDP, DHCP, IP, LLDP, MAC, NETFLOW, NMAP, and SNMP and enter a value for that new attribute. When it is saved to the policy elements library, you can use it from the library.
- Choose **Apple-MacBookRuleCheck2**.

  For example, the Apple-MacBook uses a single rule that contains Apple-MacBookRuleCheck1 and Apple-MacBookRuleCheck2 conditions in the rule with an associated certainty value. Both these checks use an IP User-Agent attribute having Mackintosh and Mac OS as values.

  See Figure 18-2 and Figure 18-3.

Figure 18-2 Creating A New Rule from Exiting Conditions -Step 1

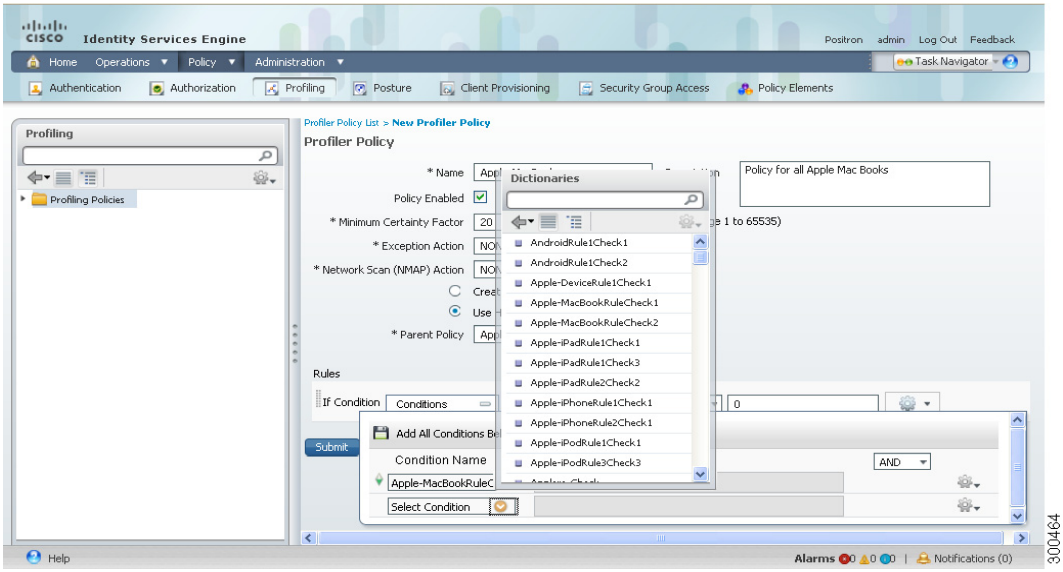
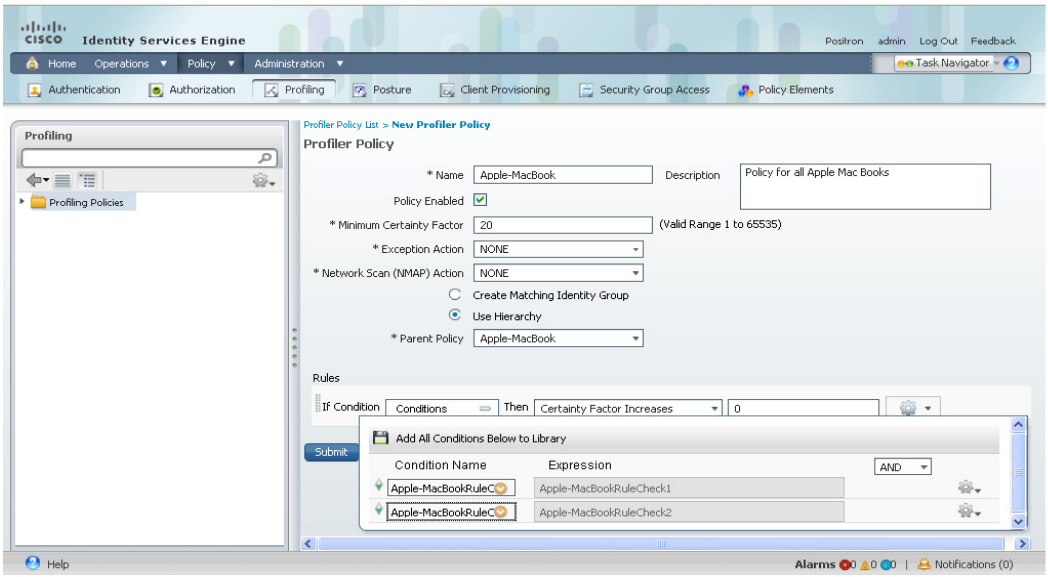


Figure 18-3 Creating A Rule with Existing Conditions-Step2



When you create a new rule for an endpoint profiling policy, you can choose an attribute from the available system dictionaries and associate a value to the attribute by using **Create New Condition (Advance Option)**.

To create a new condition in a rule, perform the following tasks:

- Choose the **Conditions** field. Click the plus [+] sign to expand the Conditions anchored overlay. To close the anchored overlay, click the minus [-] sign.
- Choose **Create New Condition (Advance Option)**.
- Choose the **Expression** field. From the Expression field, click the **Select Attribute Quick Picker** icon. The Dictionaries widget appears, which displays Profiler CDP, DHCP, IP, LLDP, MAC, NETFLOW, NMAP, and SNMP dictionaries. For more information, you can find system dictionaries in **Policy > Policy Elements > Dictionaries**.

For some products, the OUI (Organizationally Unique Identifier) is an unique attribute that you can use it first for identifying the manufacturing organization of devices. It is a component of the device MAC address. The MAC dictionary contains the MACAddress and OUI attributes.

For example, create an expression such as MAC:OUI CONTAINS Apple, which is a new condition, and save it as Apple-DeviceRule1Check1 in the rule. This rule contains Apple-DeviceRule1Check1, a single condition in the Apple-Device policy to check for Apple devices. If an endpoint is an Apple device, Apple-Device is a matching policy, which is a generic (parent) to all the Apple devices. Other Apple devices use the IP User-Agent and DHCP host name in the conditions for further refinement.

Xerox-Device is the parent policy for all Xerox Corporation devices. It uses MAC:OUI CONTAINS XEROX CORPORATION first in Xerox-DeviceRule1Check1in a single rule. You can refine endpoint profiling with the dhcp-class-identifier next in other conditions in its children for profiling other Xerox devices. It provides you device-specific information, such as device manufacturer, type of device, and model number. Xerox-Printer-Phaser3250 is a child of Xerox-Device. You must enable DHCP/DHCP SPAN probes. For example, you can create two expressions for a Xerox-Printer-Phaser3250 on the New Profiler Policy page.

Create an expression such as DHCP:dhcp-class-identifier CONTAINS Xerox and save it as Xerox-Printer-Phaser3250Rule1Check1. Create an expression such as DHCP:dhcp-class-identifier CONTAINS Phaser 3250 and save it as Xerox-Printer-Phaser3250Rule1Check2. See Figure 18-4 and Figure 18-5 that shows how to create new conditions from the New Profiler Policy page.

Figure 18-4 Creating a New Condition-Step1

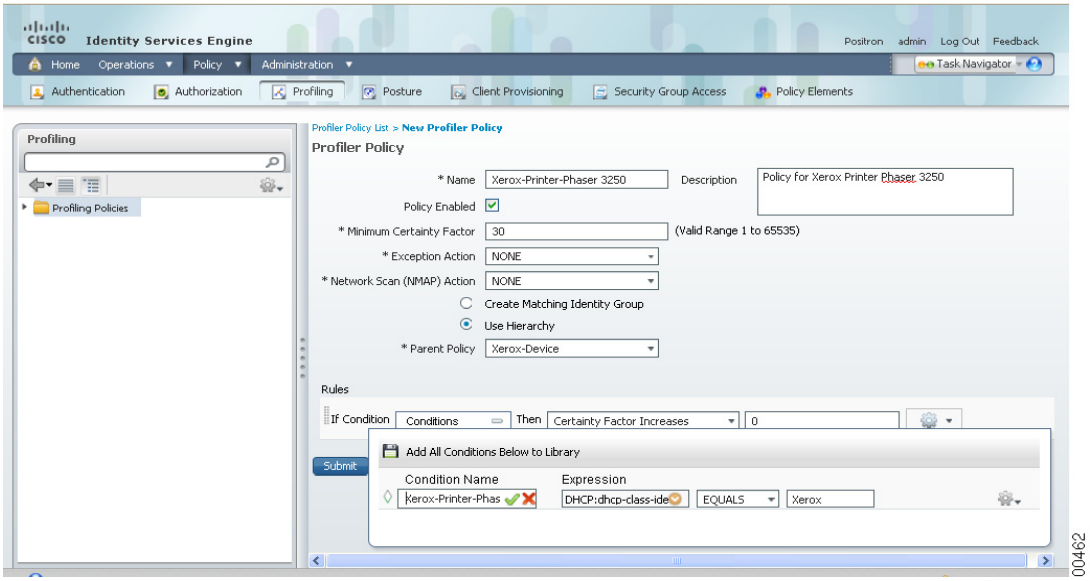
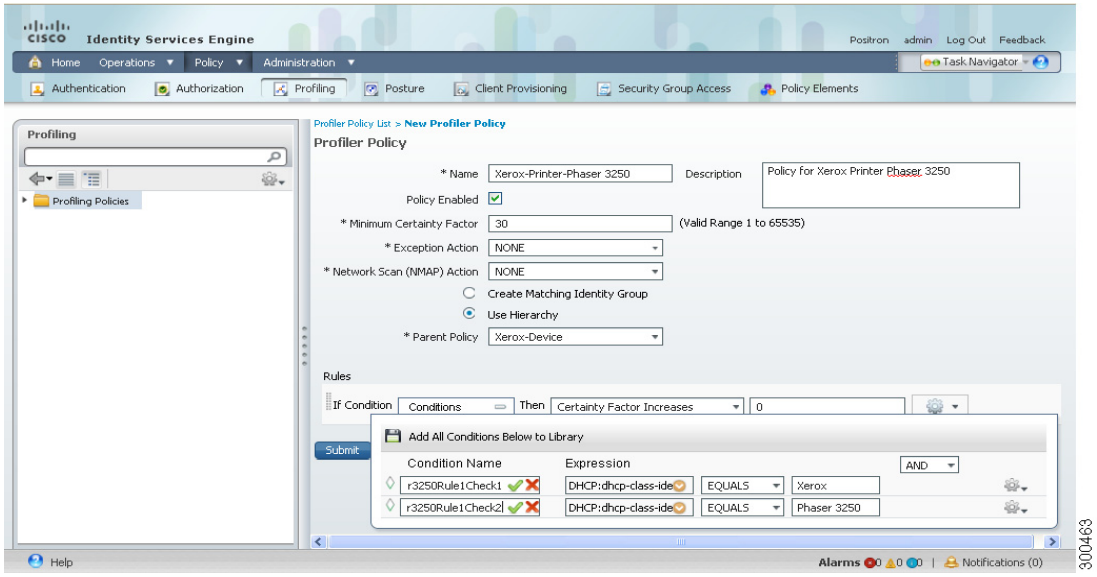


Figure 18-5 Creating a New Condition-Step2



  - For some products, you can also obtain MIB information through SNMP as a result of a Network (NMAP) Scan. If SNMP is enabled on the device, then you can use hrDeviceDescr, hrDeviceStatus, sysContact, sysDescr, sysLocation, sysName, sysObjectID, and sysUpTime attributes in new conditions. You must enable the SNMP Query probe and run the Network (NMAP) Scan.

- Choose from the following:
  - Certainty Factor Increases
  - Take Exception Action
  - Take Network Scan Action
- Click **Submit** to create a new endpoint profile.

Editing an Endpoint Profiling Policy

You can choose an endpoint profiling policy on the Endpoint Policies page in order to edit it.

Note During an upgrade, Cisco ISE overwrites any configuration that you have saved it on the predefined endpoint profiles. You must save all your configurations on a copy of the predefined endpoint profiles only.

To edit a profiling policy, complete the following steps:

Step 1 Choose **Policy > Profiling**.

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears. From the Endpoint Policies page, choose a profiling policy.

Step 3 Choose **Edit**.

Step 4 Modify the values of the fields on the edit page, as shown in Table 18-15 on page 18-41.

During an edit, you can click the **Reset** button without saving the current input data on the edit page. Here, you can retain the configuration without saving the current input data on the edit page. Click the **Profiler Policy List** link from the edit page to return to the Endpoint Policies page.

Step 5 Click **Save** to save the current input data on the edit page.

Step 6 Click the **Profiler Policy List** link from the edit page to return to the Endpoint Policies page after editing an endpoint profiling policy.

Deleting an Endpoint Profiling Policy

The Endpoint Policies page lists all the canned profiles that are already created in Cisco ISE for your deployment. You can choose an endpoint profiling policy to delete that you create on the Endpoint Policies page.

You can also select all the endpoint policies from the Endpoint Policies page to delete from your Cisco ISE deployment. To delete all the endpoint policies, you need to check the check box that appears in front of the Endpoint Policy Name title on the Endpoint Policies page.

When you select all the endpoint policies and try to delete them on the Endpoint Policies page, some of them may not be deleted. The endpoint policy may be a parent to other endpoint policies or mapped to an authorization policy and a parent to other endpoint policies.

Note You cannot delete a parent profile on the Endpoint Policies page when an endpoint profile is defined as a parent to other endpoint profiles. For example, Cisco-Device is a parent to other endpoint policies for Cisco devices. You cannot delete an endpoint profile when it is mapped to an authorization policy. For example, Cisco-IP-Phone is mapped to the Profiled Cisco IP Phones authorization policy and it is a parent to other endpoint policies for Cisco IP Phones.

To delete a profiling policy, complete the following steps:

Step 1 Choose **Policy > Profiling**.

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears. From the Endpoint Policies page, choose a profiling policy.

Step 3 Choose **Delete**.

If you choose to delete an endpoint profile from the Endpoint Policies page, Cisco ISE displays a confirmation dialog. Clicking **OK** from the dialog deletes the policy from the Endpoint Policies page. Clicking **Cancel** from the dialog returns to the Endpoint Policies page without deleting the policy.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Duplicating an Endpoint Profiling Policy

Duplicating an endpoint profiling policy allows you to quickly create a similar characteristic profiling policy that you can modify instead of creating a new profiling policy by redefining all conditions.

To duplicate a profiling policy, complete the following steps:

Step 1 Choose **Policy > Profiling**.

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears. From the Endpoint Policies page, choose a profiling policy.

Step 3 Choose **Duplicate**.

A copy of the profiling policy appears on the Endpoint Policies page.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Exporting Endpoint Profiling Policies

You can choose endpoint profiling policies on the Endpoint policies page to export them to other Cisco ISE deployments. Or, you can use it as a template for creating your own policies to import.

To export a profiling policy from the Endpoint Policies page, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling** (menu window).

Step 2 From the Profiling menu window, choose **Profiling Policies.**

The Endpoint Policies page appears. Choose one or more profiling policies that you want to export.

Step 3 Choose **Export**.

A dialog appears that prompts you to open the profiler_policies.xml with an appropriate application or save it. This is a file in XML format that you can open in a web browser, or in other appropriate applications. You can also download the file to your system in the default location, which can be used for importing later.

Step 4 Click **OK**.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Importing Endpoint Profiling Policies

You can import endpoint profiling polices from a file in XML by using the same format that you have previously created in the export function. If you import newly created profiling policies that has parent policies associated, then you must define parent policies before you define child policies. The imported file shows the hierarchy of endpoint profiling policies that contains the parent policy first, the profile that you imported next along with the rules and checks that are defined in the policy.

To import a profiling policy from the Endpoint Policies page, complete the following steps:

Step 1 Choose **Policy > Profiling > Profiling** (menu window).

Step 2 From the Profiling Policies menu window, choose **Profiling Policies.**

The Endpoint Policies page appears.

Step 3 Choose **Import**.

Step 4 Browse to locate the file that you previously exported and want to import.

Note Please note that the file should be in XML format as previously created in the export function.

Step 5 Click **Submit**.

Profiling policies, which are imported appear on the Endpoint Policies page.

Step 6 Click the **Profiler Policy List** link from the Import Profiler Policies page to return to the Endpoint Policies page.

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Endpoint Profiling

A profiling condition is a check that allows you to provision specific values that can be associated to a set of attributes of an endpoint. You can logically group one or more of these conditions into a rule that allows you to validate and classify endpoints to a category. You can create a condition that allows you to provision specific values to one or more attributes of the endpoint, which helps you to validate and classify endpoints in a category.

This section describes the basic operations that allow you to provision a specific value to an attribute of an endpoint. You can use the Conditions window from the Profiling menu to display and manage Cisco ISE profiling conditions.

The procedures for managing profiling conditions include the following topic:

Filtering, Creating, Editing, and Deleting a Profiling Condition

Related Topics

- Endpoint Profiling Policies, page 18-35
- Profiling Exception Actions, page 18-58
- Profiling Network Scan Actions, page 18-62

Troubleshooting Topics

- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- Cannot Authenticate on Profiled Endpoint, page D-17

Filtering, Creating, Editing, and Deleting a Profiling Condition

The Conditions page allows you to manage profiling conditions, which provides an option to filter profiling conditions. This page lists profiling conditions along with their names, description and the expression that you have defined in these conditions on the Conditions page.

The procedures for managing profiling conditions include the following tasks:

- Filtering Conditions, page 18-53
- Creating a Profiling Condition, page 18-55
- Editing a Profiling Condition, page 18-56
- Deleting a Profiling Condition, page 18-57

Filtering Conditions

You can use the Show drop-down list, or the filter icon both to invoke a quick filter and close it on the Conditions page. A quick filter is a simple filter that you can use to filter profiling conditions on the Conditions page. The quick filter filters conditions based on field descriptions, such as the name of the profiling check, the description, and the expression that is used in the condition on the Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, on the Conditions page. The advanced filter filters conditions based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime, which displays the filtered results on the Conditions page. Once you have created and saved a preset filter, you can choose a preset filter of filtered results on the Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter conditions from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Conditions** (menu window).

Step 2 Choose **Profiling**.

The Conditions page appears, which lists all the predefined conditions.

Step 3 From the Conditions page, click the Show drop-down arrow to list the filter options.

Here, you can choose a Quick Filter**,** an Advanced Filter for filtering or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-16.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 18-54 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 18-54.

Note To return to the conditions list, choose **All** from the Show drop-down list to display all the conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters profiling conditions based on each field description on the Conditions page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Conditions page. If you clear the field, it displays the list of all the conditions on the Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter profiling conditions by using variables that are more complex. It contains one or more filters that filter conditions based on the values that match the field descriptions. A filter on a single row filters conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter conditions by using any one or all of the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or click **Cancel** to clear the filter.

Table 18-16 describes the fields on the Conditions page that allow you to filter the profiling conditions.

Table 18-16 Filtering Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Profiler Check Name	This field enables you to filter conditions by the name of the profiling check (condition).
	Expression	This field enables you to filter conditions by an attribute and its attribute value within the profiling check.
	Description	This field enables you to filter conditions by the description of the profiling check.

Table 18-16 Filtering Conditions (continued)

Filtering Method	Filtering Field	Filtering Field Description
Advanced Filter	Choose the field description from the following: • Profiler Check Name • Expression • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter profiling conditions.
	Value	From the Value field, choose the value for the field description that you selected against, which the profiling conditions are filtered.

Creating a Profiling Condition

To create a profiling condition in the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Profiling** (menu window).

The Conditions page appears.

Step 2 From the Conditions page, choose **Create**.

You can create a condition of DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP and NMAP type.

Step 3 Modify the values on the New Profiler Condition page, as shown in Table 18-17.

Step 4 Click **Submit**.

The profiling condition that you create appears on the Conditions page.

Step 5 Click the **Profile Condition List** link on the New Profiler Condition page to return to the Conditions page.

Table 18-17 describes the fields on the Conditions page that allow you to create a profiling condition:

Table 18-17 Creating a Profiling Condition

Field Name	Description
Name	From the Name field, enter the name of the profiling condition that you want to create.
Description	From the Description field, enter the description of the profiling condition that you want to create.

Table 18-17 Creating a Profiling Condition (continued)

Field Name	Description
Type	From the Type field, click the drop-down arrow to view the following predefined profiling conditions types: • DHCP • MAC • SNMP • IP • RADIUS • Netflow • CDP • LLDP • NMAP Choose a type.
Attribute Name	From the Attribute Name field, click the drop-down arrow to view the predefined attributes for the type you have selected in the Type field.
Operator	Click the drop-down arrow to view the following predefined operators: • EQUALS • NOTEQUALS • GREATERTHAN • LESSTHAN • CONTAINS Choose an operator.
Attribute Value	Enter the value for the attribute name that you selected in the Attribute Name.

Editing a Profiling Condition

You can edit a profiling condition from the Conditions page.

To edit a condition from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Profiling** (menu window).

The Conditions page appears. From the Conditions page, choose a profiling condition.

Step 2 Choose **Edit**.

Step 3 Modify the values of the fields on the edit page, as shown in Table 18-17 on page 18-55.

During an edit, you can click **Reset** button without saving the current input data on the edit page. Here, you can retain the configuration without saving the current input data on the edit page. Click the **Profiler Condition List** link from the edit page to return to the Conditions page without saving the current input data.

Step 4 Click **Save** to save the current input data on the edit page.

Step 5 Click the **Profiler Condition List** link from the edit page to return to the Conditions page after editing a profiling condition.

Deleting a Profiling Condition

You can delete a profiling condition from the Conditions page.

To delete a condition from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Profiling** (menu window).

The Conditions page appears. From the Conditions page, choose a profiling condition.

Step 2 Choose **Delete**.

If you choose to delete a profiling condition from the Conditions page, Cisco ISE displays a confirmation dialog. Clicking **OK** from the dialog deletes the condition from the Conditions page. Clicking **Cancel** from the dialog returns to the Conditions page without deleting the profiling condition.

Profiling Results

Cisco ISE provides configurable network access to identities.

Cisco ISE policy model comprises of policy based services for authentication and authorization, profiling, posture, client provisioning, and Cisco security group access for identities in Cisco ISE.

Step 1 Choose **Policy > Policy Elements > Results > Results** (menu window).

Step 2 Choose **Profiling**.

Step 3 Click the right navigation arrow to list the profiling action types.

The Exception Actions and Network Scan (NMAP) Actions menus appear.

Step 4 Choose **Exception Actions**. See Profiling Exception Actions, page 18-58.

Here, you can create editable exception actions that you can use for profiling endpoints on a Cisco ISE network. Cisco ISE includes three noneditable exception actions, such as an EndpointDelete, FirstTimeProfile, and StaticAssignment.

Or

Step 5 Choose **Network Scan (NMAP) Actions**. See Profiling Network Scan Actions, page 18-62.

Here, you can create editable network scan actions that you can use for profiling endpoints on a Cisco ISE network. Cisco ISE includes three predefined network scan actions such as an OS-scan, an SNMPPortsAndOS-scan, and a CommonPortsAndOS-scan

Profiling Exception Actions

An exception action is a single configurable action that is associated to an endpoint profiling policy. You can define, and associate one or more exception rules to a single profiling policy. This association triggers an exception action, when the profiling policy matches, and at least one of the exception rules matches in profiling endpoints in Cisco ISE.

Cisco ISE triggers the following non-editable profiling exception actions from the system when profiling endpoints on a Cisco ISE network:

Endpoint Delete

An exception action is triggered in Cisco ISE, and a CoA is issued when an endpoint is deleted from the system on the Endpoints page, or reassigned to the unknown profile from the edit page on a Cisco ISE network.

Static Assignment

An exception action is triggered in Cisco ISE, and a CoA is issued upon when an endpoint has connected to your Cisco ISE network, but you statically assign an endpoint profile for that endpoint.

FirstTimeProfiled

An exception action is triggered in Cisco ISE, and a CoA is issued, when an endpoint is profiled in Cisco ISE for the first time, where the profile of that endpoint changes from an unknown profile to an existing profile, but that endpoint is not successfully authenticated on a Cisco ISE network.

The procedures for managing exception actions include the following topic:

Filtering, Creating, Editing, and Deleting a Profiling Exception Action, page 18-58

Related Topics

Endpoint Profiling Policies, page 18-35

Filtering, Creating, Editing, and Deleting a Profiling Exception Action

The Exception Actions page allows you to manage exception actions, and provides an option to filter them, which lists all the exception actions along with their names and descriptions.

The procedures for managing exception actions include the following tasks:

- Filtering Exception Actions, page 18-59
- Creating an Exception Action, page 18-61
- Editing an Exception Action, page 18-61
- Deleting an Exception Action, page 18-62

Filtering Exception Actions

You can use the Show drop-down list, or the filter icon both to invoke a quick filter and close it on the Exception Actions page. A quick filter is a simple filter that you can use to filter profiling exception actions on the Exception Actions page. The quick filter filters exception actions based on field descriptions, such as the name of the profiling exception action and the description on the Exception Actions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, on the Exception Actions page. The advanced filter filters exception actions based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter has a session lifetime which displays the filtered results on the Exception Actions page. Once created and saved a preset filter, you can choose a preset filter of filtered results on the Exception Actions page. You can also edit preset filters and remove them from the preset filters list.

To filter exception actions from the Exception Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Results** (menu window).

Step 2 Choose **Profiling**.

Step 3 Click the right navigation arrow to go to the profiling menu window.

Step 4 From the Profiling menu, choose **Exceptions Actions**.

The Exception Actions page appears.

Step 5 From the Exception Actions page, click the Show drop-down arrow to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-18.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 18-59 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 18-60.

Note To return to the exception actions list, choose **All** from the Show drop-down list to display all the exception actions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters profiling exception actions based on each field description on the Exception Actions page. When you click inside any field, and as you enter the search criteria in the field, the quick filter refreshes the page with the results on the Exception Actions page. If you clear the field, it displays the list of all the exception actions on the Exception Actions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter profiling exception actions by using variables that are more complex. It contains one or more filters that filter exception actions based on the values that match the field descriptions. A filter on a single row filters exception actions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter exception actions by using any one or all of the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or click **Cancel** to clear the filter.

Table 18-18 describes the fields on the Exception Actions page that allow you to filter exception actions.

Table 18-18 Filtering Exception Actions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Profiler Exception Action Name	This field enables you to filter exception actions by the name of the profiling exception action.
	Description	This field enables you to filter exception actions by the description of the profiling exception action.
Advanced Filter	Choose the field description from the following: • Profiler Exception Action Name • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter exception actions.
	Value	From the Value field, choose the value for the field description that you selected against, which the exception actions are filtered.

Creating an Exception Action

To create an exception action on the Exception Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Exception Actions**.

The Exception Actions page appears.

Step 4 From the Exception Actions page, click **Create**.

Step 5 Modify the values on the New Profiler Exception Action page, as shown in Table 18-19

Step 6 Click **Submit**.

The exception action that you created appears on the Exception Actions page.

Table 18-19 describes the fields on the New Profiler Exception Actions page that allow you to create an exception action:

Table 18-19 Creating an Exception Action

Field Name	Field Description
Name	From the Name field, enter the name of the exception action that you want to create.
Description	From the Description field, enter the description of the exception action that you want to create.
CoA Action check box to enforce CoA	To enforce CoA, check the **CoA Action** check box. If you associate excepion actions in the endpoint profiling policies, you must configure CoA globally in Cisco ISE, which can be done in the following location: Administration > System > Settings > Profiling. For more information, see the Change of Authorization, page 18-8.
Policy Assignment	Click the drop-down arrow to view the endpoint profiles that are configured and choose the profile against which the endpoint will be profiled when the exception action is triggered, regardless of its matched value.

Editing an Exception Action

You can edit an exception action from the Exception Actions page.

To edit an exception action on the Exception Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Exception Actions**.

The Exception Actions page appears. From the Exception Actions page, choose an exception action.

Step 4 Choose **Edit**.

Step 5 Modify the values of the fields on the edit page, as shown in Table 18-19 on page 18-61.

During an edit, click **Reset** without saving the current input data on the edit page. Here, you can retain the configuration without saving the current input data. Click the **Profiler Exception Action List** link from the edit page to return to the Exception Actions page without saving the current input data.

Step 6 Click **Save** to save the current input data on the edit page.

Step 7 Click the **Profiler Exception Action List** link from the edit page to return to the Exception Actions page after editing an exception action.

Deleting an Exception Action

You can delete an exception action from the Exception Actions page.

To delete an exception action on the Exception Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Exception Actions**.

The Exception Actions page appears. From the Exception Actions page, choose an exception action.

Step 4 Choose **Delete**.

If you choose to delete a profiling exception action from the Exception Actions page, Cisco ISE displays a confirmation dialog. Clicking **OK** from the dialog deletes the exception action from the Exception Actions page. Clicking **Cancel** from the dialog returns you to the Exception Actions page without deleting the exception action.

Profiling Network Scan Actions

A network scan action is a single configurable action that is associated to an endpoint profiling policy. You can define, and associate one or more network scan rules in a single endpoint profiling policy. You can also define the type of scanning in each network scan actions. This association triggers a network scan action, when the profiling policy matches, and at least one of the network scan rules matches in profiling endpoints in Cisco ISE.

Note When scanning an operating system for endpoints, the NMAP OS-scan results may be unreliable. This is due to the limitations of the NMAP tool that you use for an OS-scan. For example, when scanning an operating system of network devices such as switches and routers, the NMAP OS-scan may provide an incorrect operating-system attribute for those devices. For these devices, you can configure endpoint policies that use the NMAP operating-system attribute in their rules to have low certainty value conditions (Certainty Factor values).

The following section describes how to manage network scan actions:

Filtering, Creating, Editing, and Deleting a Profiling Network Scan Action, page 18-63.

Related Topics

Endpoint Profiling Policies, page 18-35.

Filtering, Creating, Editing, and Deleting a Profiling Network Scan Action

The Network Scan Actions page allows you to manage network scan actions, and provides with an option to filter them that lists all the network scan actions, along with their names and descriptions.

The procedures for managing network scan actions include the following tasks:

- Filtering Network Scan Actions, page 18-63
- Creating a Network Scan Action, page 18-65
- Editing a Network Scan Action, page 18-66
- Deleting a Network Scan Action, page 18-67

Filtering Network Scan Actions

You can use the Show drop-down list, or the filter icon both to invoke a quick filter and close it on the Network Scan Actions page. A quick filter is a simple filter that you can use to filter profiling network scan actions on the Network Scan Actions page. The quick filter filters network scan actions based on field descriptions, such as the name of the profiling network scan action and the description on the Network Scan Actions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, on the Network Scan Actions page. The advanced filter filters network scan actions based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter from the list has a session lifetime, which displays the filtered results on the Network Scan Actions page. Once created and saved a preset filter, you can choose a preset filter of filtered results on the Network Scan Actions page. You can also edit preset filters and remove them from the preset filters list.

To filter network scan actions from the Network Scan Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Results** (menu window).

Step 2 Choose **Profiling**.

Step 3 Click the right navigation arrow to go to the profiling menu.

Step 4 From the Profiling menu, choose **Network Scan (NMAP) Actions**.

The Network Scan Actions page appears.

Step 5 From the Network Scan Actions page, click the Show drop-down arrow to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-18.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 18-64 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 18-64.

Note To return to the network scan actions list, choose **All** from the Show drop-down list to display all the network scan actions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters profiling network scan actions based on each field description on the Network Scan Actions page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Network Scan Actions page. If you clear the field, it displays the list of all the exception actions on the Network Scan Actions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter profiling network scan actions by using variables that are more complex. It contains one or more filters that filter network scan actions based on the values that match the field descriptions. A filter on a single row filters network scan actions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter network scan actions by using any one or all of the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or click **Cancel** to clear the filter.

Table 18-20 describes the fields on the Network Scan Actions page that allow you to filter exception actions.

Table 18-20 Filtering Network Scan Actions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Profiler Network Scan Action Name	This field enables you to filter network scan actions by the name of the profiling network scan action.
	Description	This field enables you to filter network scan actions by the description of the profiling network scan action.
Advanced Filter	Choose the field description from the following: • Profiler Network Scan Action Name • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter network scan actions.
	Value	From the Value field, choose the value for the field description that you selected against, which the network scan actions are filtered.

Creating a Network Scan Action

To add a network scan action on the Network Scan Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Network Scan (NMAP) Actions**.

The Network Scan Actions page appears.

Step 4 From the Network Scan Actions page, click **Add**.

Step 5 Modify the values on the New Network Scan Action page, as shown in Table 18-21.

Step 6 Click **Submit**.

The network scan action that you created appears on the Network Scan Actions page.

Table 18-21 describes the fields on the Network Scan Actions page that allow you to add an exception action.

Table 18-21 Creating a Network Scan Action

Field Name	Field Description
Name	From the Name field, enter the name of the network scan action that you want to create.
Description	From the Description field, enter the description of the network scan action that you want to create.
Scan	Choose options to scan from the following: • Scan OS—Scans an operating system. • Scan SNMP Port—Scans SNMP ports (161, 162). • Scan Common Port—Scans common ports. See Table 18-22.

Editing a Network Scan Action

You can edit a network scan action from the Network Scan Actions page.

To edit a network scan action on the Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Network Scan (NMAP) Actions**.

The Network Scan Actions page appears. From the Network Scan Actions page, choose a network scan action.

Step 4 Choose **Edit**.

Step 5 Modify the values of the fields on the edit page, as shown in Table 18-21 on page 18-66.

During an edit, click **Reset** without saving the current input data on the edit page. Here, you can retain the configuration without saving the current input data. Click the **Network Scan Action List** link from the edit page to return to the Network Scan Actions page without saving the current input data.

Step 6 Click **Save** to save the current input data on the edit page.

Step 7 Click the **Network Scan Action List** link from the edit page to return to the Network Scan Actions page after editing a network scan action.

Deleting a Network Scan Action

You can delete a network scan action from the Network Scan Actions page.

To delete a network scan action on the Network Scan Actions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results** (menu window).

The Results menu window appears.

Step 2 From the Results menu window, choose **Profiling**.

Click the right navigation arrow to go to the Profiling menu.

Step 3 Choose **Network Scan (NMAP) Actions**.

The Network Scan Actions page appears. From the Network Scan Actions page, choose a network scan action.

Step 4 Choose **Delete**.

If you choose to delete a profiling network scan action from the Network Scan Actions page, Cisco ISE displays a confirmation dialog. Clicking **OK** from the dialog deletes the network scan action from the Network Scan Actions page. Clicking **Cancel** from the dialog returns you to the Network Scan Actions page without deleting the network scan action.

Endpoint Profiling by Integrating Network Mapper in Cisco ISE

Network Mapper (NMAP) is a free, open source utility that can be used to explore networks and perform other network related tasks. It is designed to rapidly scan large networks, and works on a single host. NMAP uses raw IP packets for many network-related tasks, such as identifying endpoints (hosts that are available), the operating systems (and OS versions) they run, and the services (application name and version) they offer.

NMAP is a powerful tool that you can use to scan huge networks of y hundreds of thousands of machines. NAMP is portable and supports many operating systems. In addition to its command-line executable, the NMAP suite includes an advanced graphical user interface, a results viewer, a flexible data transfer redirection, and debugging tool, a utility for comparing scan results, and a packet generation and response analysis tool. It is highly flexible that supports advanced techniques for mapping out networks where devices such as IP filters, firewalls, routers are present, including port scanning mechanisms (both TCP and UDP), operating system detection, version detection, ping sweeps, and more.

For more information on NMAP, see Network Mapper (NMAP) and the NMAP documentation that is available at http://nmap.org/docs.html.

NMAP is integrated with the Cisco ISE profiler to augment its profiling capability for better endpoint classification, particularly iDevices and other mobile devices. You can either perform a manual subnet scan on a specific subnet by using the Network Scan probe, or you can associate a network scan action to an endpoint profile (a specific profile) to perform a scan on an endpoint.

For more information on the network scanning, see the "A Network Scan" section on page 18-22.

For more information on the endpoint scanning, see the "Endpoint Scan" section on page 18-68.

Endpoint Scan

An endpoint scan is used to scan endpoints in order to limit resources usage on the Cisco ISE system. A network scan action scans a single endpoint as compared to resource intensive network scans. It improves the overall classification of endpoints, and redefines an endpoint profile for an endpoint. Endpoint scans can be processed only one at a time.

You can associate a single network scan action to an endpoint profiling policy. Cisco ISE predefines three scanning types for a network scan action, which can include one, or all three scanning types, for instance, an OS-scan, an SNMPPortsAndOS-scan, and a CommonPortsAndOS-scan. You can also create a new network scan action of your own. Once an endpoint is appropriately profiled, the configured network scan action cannot be used against that endpoint.

For example, scanning an Apple-Device allows you to classify the scanned endpoint to an Apple device. Once an OS-scan determines the operating system that an endpoint is running, it is no longer matched to an Apple-Device profile, but it is matched to an appropriate profile for an Apple device.

The following are the scanning types that are predefined in any network scan action for an endpoint scan.

OS-scan

This type scans an operating system (and OS version) that an endpoint is running. It is a resource intensive scan.

SNMPPortsAndOS-scan

This type scans an operating system (and OS version) that an endpoint is running, as well as triggers an SNMP Query when SNMP ports (161 and 162) are open. It can be used for endpoints that are identified and matched initially with an Unknown profile for better classification.

CommonPortsAndOS-scan

This type scans an operating system (and OS version) that an endpoint is running, as well as common ports (TCP and UDP), but not SNMP ports.

Table 18-22 lists the total of 30 common ports (15 TCP and 15 UDP ports) that NMAP uses for scanning.

Table 18-22 Common Ports

TCP Ports		UDP Ports	
Ports	**Service**	**Ports**	**Service**
21/tcp	ftp	53/udp	domain
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds

Table 18-22 Common Ports (continued)

TCP Ports		UDP Ports	
Ports	**Service**	**Ports**	**Service**
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3306/tcp	mysql	631/udp	ipp
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

Endpoint Profiling by Using an IOS Sensor on a Network Access Device

Cisco ISE enforces certain configurations on the DHCP probe. For example, you can collect DHCP packets from one or more interfaces only when you configure the DHCP IP helper by using the ip helper - address command on the network devices, or on a specific interface, by using DHCP SPAN. The Cisco ISE profiler receives these DHCP packets and parses them to capture other attributes of endpoints, along with DHCP attributes. Similarly, you can collect the CDP/LLDP attributes of all the connected endpoints only when the SNMP Query probe is enabled. You must ensure that CDP and LLDP are enabled on all the ports of the network devices.

Cisco ISE, Release 1.1 addresses these configuration restrictions by implementing a functionality to work with an IOS based sensor that is embedded in the switch. The IOS sensor integration resolves any topology restriction on your deployment that you might have experienced in previous releases, due to the nature of event collection of endpoint attributes from various probes. IOS sensor integration allows Cisco ISE runtime and the Cisco ISE profiler to collect any or all of the attributes that are sent from the switch. You can collect DHCP, CDP, and LLDP attributes directly from the switch by using an already existing RADIUS protocol. The attributes that are collected for DHCP, CDP, and LLDP are then parsed and mapped to attributes in the Cisco ISE dictionaries.

For more information on Cisco ISE system dictionaries and the attributes that are defined in the dictionaries, you can navigate to **Policy > Policy Elements > Dictionaries** from the administration user interface.

Cisco ISE, Release 1.1 contains the list of default profiles that are updated for LLDP, as well as new profiles. For more information on the list of default profiles in Cisco ISE, navigate to **Policy > Profiling > Endpoint Profiling**.

For more information on IOS sensor supported network access devices, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

Integrating an IOS Sensor with Cisco ISE

Integrating an IOS sensor enabled switch with Cisco ISE, Release 1.1 involves an IOS sensor, the data collector that is embedded in the network device (switch) for gathering DHCP, CDP, and LLDP data, and analyzers for processing the data and determining the device-type of endpoints. The distinct advantage of embedding a sensor in the switch is that the sensor is the closest point present to the source of the data.

There are two ways of deploying an analyzer, but they are not expected to be used in conjunction with each other:

- An analyzer can be deployed in Cisco ISE

- Analyzers can be embedded in the switch as the sensor

The choice of deploying an analyzer in either way depends on your implementation. Both deployments use the same classification rule-set, but the analyzer deployed in Cisco ISE provides a functional superset of the embedded capabilities of the analyzers deployed in the switches. Both analyzers are the clients of the IOS sensor component-set and require the same information from the sensor. With the embedded analyzers in the switch, this deployment can be used where Cisco ISE is not available either for a visibility-only deployment or in conjunction with an OEM AAA server.

An IOS Sensor and Analyzers

A network access device (switch) has an IOS sensor embedded, and the sensor has both internal clients (analyzers) and one external client (Cisco ISE analyzer).

The IOS sensor lets you to specify attribute filters using the CLI to define the target data-set. The attribute filters must be applied as close to the source of the attributes as possible to minimize redundant memory usage and processing across the system.

The filter commands must include the following capabilities:

- An all option per protocol (default)
- A none option per protocol
- An include list per protocol
- An exclude list per protocol

The internal clients, including the Device Classifier (local analyzer), use the session API as exposed by the session management (identity) infrastructure. Apart from the Device Classifier (DC), ASP, MSI-Proxy, and EnergyWise components are the other illustrated internal clients that are primarily interested in the device-type of the connected endpoints. Once the device-type is determined, it can be returned back to the session management infrastructure by using the same session API and stored against the appropriate session, and in the form of a RADIUS CoA in the future. It is also available to any client of the Session API (through notification and/or in response to a direct query). The same session management infrastructure can accommodate both the cases where endpoint profiling can be configured in conjunction with access-control for a typical identity deployment, or for a visibility-only deployment.

The external client, the Cisco ISE analyzer, initially uses the RADIUS accounting messages to receive the additional endpoint data. The existing RADIUS Accounting message types (start and interim) are augmented with the profiling data. Additional accounting messages can be generated if the profiling data changes in the middle of the session.

When appropriately configured, a switch with the sensor capability captures endpoint information from CDP, LLDP, DHCP, and MAC OUI, and (subject to statically configured filters that can be dynamically configured in future phases of implementation) makes this information available to its registered clients in the context of an access session (which represents an endpoint's connection to the network device). Notifications can only be generated if a change is detected in the information provided by an endpoint (subject to statically configured filters).

Endpoint Profiling in Cisco ISE with an IOS Sensor Enabled on NADs

You can create endpoints and classify them according to the endpoint profiling policies that are currently available by default in Cisco ISE with DHCP, CDP, and LLDP attributes, by using IOS sensor enabled switches. This allows you to overcome the earlier configuration restrictions on DHCP and SNMP Query probes, by using the existing RADIUS probe alone.

You must configure network access devices that allow the IOS sensor to collect DHCP, CDP, and LLDP information from the endpoints that connect to your network and to send them through the RADIUS accounting messages to Cisco ISE. Cisco ISE receives these RADIUS accounting messages from the switches, and the runtime protocol parses and forwards these messages as syslogs to the RADIUS probe of the profiler. The RADIUS probe populates DHCP, CDP, and LLDP attributes for the endpoints from the syslogs and contributes to the classification of endpoints. The result of this classification can also be returned in the form of the RADIUS CoA, with attributes in future releases.

Prerequisites:

You must ensure that the network access devices (switches) and Cisco ISE are properly configured.

This section summarizes a list of tasks that you must perform on the switches and Cisco ISE.

Review the following:

- Ensure that the RADIUS probe is enabled in Cisco ISE.
- Ensure that network access devices support an IOS sensor for collecting DHCP, CDP, and LLDP information.
- Ensure that network access devices run the following CDP and LLDP commands to capture CDP and LLDP information from endpoints:

  ```
  cdp enable
  lldp run
  ```
- Ensure that session accounting is enabled separately, by using the standard AAA and RADIUS commands.

  For example, use the following commands:

  ```
  aaa new-model
  aaa accounting dot1x default start-stop group radius

  radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
  radius-server vsa send accounting
  ```
- Ensure that you run IOS sensor-specific commands.

  Enabling Accounting Augmentation

  You must enable network access devices to add IOS sensor protocol data to the RADIUS accounting messages, as well as to generate additional accounting events when it detects new sensor protocol data. This means that any RADIUS Accounting message should include all CDP, LLDP, and DHCP attributes.

  Enter the following (new) global command:

  ```
  device-sensor accounting
  ```

  Disabling Accounting Augmentation

  To disable (accounting) network access devices and add IOS sensor protocol data to the RADIUS accounting messages for sessions that are hosted on a given port (if the accounting feature is globally enabled), enter the following command at the appropriate port:

  ```
  no device-sensor accounting
  ```

  TLV Change Tracking

By default, for each supported peer protocol, client notifications and accounting events are only generated where an incoming packet includes a TLV (type, length, and value) that has not been received previously in the context of a given session.

You must enable client notifications and accounting events for all TLV changes where there are either new TLVs, or where previously received TLVs have different values. Enter the following command:

```
device-sensor notify all-changes
```

- Be sure that you disable the IOS Device Classifier (local analyzer) in the network access devices.

  Enter the following command:

  ```
  no macro auto monitor
  ```

Note This command prevents network access devices from sending two identical RADIUS accounting messages per change.

Auto Smartports Configuration in Cisco ISE

You can configure Auto Smartports in an authorization profile in Cisco ISE, with an event trigger that enables the VSA cisco-av-pair with the value, "auto-smart-port=event trigger". The event trigger is used to map the Auto Smartports macro to the source port of the event.

For example, when you connect a Cisco IP phone to a port, Auto Smartports automatically applies the Cisco IP phone macro. The Cisco IP phone macro enables quality of service (QoS), security features, and a dedicated voice VLAN to ensure proper treatment of delay-sensitive voice traffic.

The macros that are embedded in the switch software are groups of command-line interface (CLI) commands.

Auto Smartports Macros

Auto Smartports macros dynamically configure ports based on the device type that is detected on the port. When the switch detects a new device on a port, it applies the appropriate macro on that port. When there is a link-down event on the port, the switch removes the macro. Auto Smartports uses event triggers to map devices to port macros.

Static Smartports Macros

Static Smartports macros provide port configurations that you manually apply based on the device connected to the port. When you apply a static macro, the macro CLI commands are added to the existing port configuration. When there is a link-down event on the port, the switch does not remove the static macro configuration.

Event Triggers

Auto Smartports uses event triggers to map macros to the source port of the event. The most common triggers are based on Cisco Discovery Protocol (CDP) messages that are received from a connected device.

A CDP event trigger occurs when these devices are detected:

- Cisco switch
- Cisco router
- Cisco IP Phone

- Cisco Wireless Access Point, including autonomous and lightweight access points
- Cisco IP video surveillance camera

Additional event triggers for Cisco and third-party devices are user-defined MAC address groups, MAC authentication bypass (MAB) messages, IEEE 802.1x authentication messages, and Link Layer Discovery Protocol (LLDP) messages.

LLDP supports a set of attributes that are used to discover neighbor devices. These type, length, and value attributes and descriptions are referred to as TLVs. LLDP-supported devices use TLVs to receive and send information. This protocol advertises details such as device configuration information, capabilities, and identity. Auto Smartports uses the LLDP system capabilities TLV as the event trigger. You can use the event trigger control feature whether specify if the switch applies a macro based on the detection method, device type, or configured trigger.

For devices that do not support CDP, MAB, or 802.1x authentication, such as network printers, LLDP, or legacy Cisco Digital Media Players, you can configure a MAC address group with a MAC operationally unique identifier (OUI)-based trigger. You map the MAC address to a built-in or user-defined macro that has the desired configuration.

macro auto execute

To replace built-in macro default values and to configure mapping from an event trigger to a built-in or user-defined macro, use the **macro auto execute** command in global configuration mode.

macro auto execute *event trigger* {[***builtin*** *built-in macro name*]} [*parameter=value*]

Syntax Description

macro auto execute	Configures mapping from an event trigger to a built-in macro.
event trigger	Specifies the event trigger that is used for mapping an Auto Smartports macro to the source port of the event.
builtin	Defines mapping from an event trigger to a built-in macro.
built-in macro name	Specifies a built-in macro name.
parameter=value	Replaces default values for parameter values shown for the builtin-macro name. Enter new values in the form of a name value pair separated by a space: [<name1>=<value1> <name2>=<value2>...].

Defaults

.This command has no default setting.

Command Modes

Global configuration

Usage Guidelines

Use the **macro auto execute** global configuration command to replace the built-in macro default values with values that are specific to your switch.

The switch automatically maps from event triggers to built-in macros. The built-in macros are system-defined macros in the software image. You can also create user-defined macros by using the Cisco IOS shell scripting capability.

Examples

This example shows how to use two built-in macros for connecting Cisco switches and Cisco IP phones to the switch.

Example 1

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#!!! the next command modifies the access and voice vlans
Switch(config)#!!! for the built in Cisco IP phone auto smartport macro
Switch(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config)#
```

Example 2

```
Switch(config)#
Switch(config)#!!! the next command maps the switch event to the built in Cisco switch
Switch(config)#!!! auto smartport macro
Switch(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
Switch(config)#
```

RADIUS Accounting Reports

The RADIUS_Accounting report has enhanced options to run the report for intervals of less than an hour. The Run button provides a list of short intervals starting with a minimum of a minute. This allows you to view accounting records at short intervals that are less than an hour so that you can view a fewer number of records depending on the interval.

You can choose the Query and Run option to run the RADIUS_Accounting report for every minute past and thereafter at other intervals including the past 5 minutes, 15 minutes, 30 minutes, one hour and so on. When you choose to run the report by using the Query and Run option from the Run button, you can view the **RADIUS_Accounting > Query and Run** page. This page displays the Time Range field, where you can choose intervals in minutes for time ranges that are less than an hour.

Excluding Static Endpoints in Advanced Licenses

In Cisco ISE, licensing enables you to provide coverage for increasing numbers of endpoints and to offer more complex policy services, depending on the capabilities of the license or licenses that you choose to apply. Cisco ISE licenses are available in Base, Advanced, and Wireless packages. Each package includes a number of SKUs that is equal to the number of licenses that are included in the package. To use Cisco ISE, you must have a valid Base, Base and Advanced, or Wireless license package

Cisco ISE licensing is based on the number (a count value) of concurrent endpoints across the entire deployment for both the Base, Advanced and Wireless licenses. This defines how Cisco ISE determines the number of endpoints that utilize the licenses against the number of endpoints that are defined in the current licensing scheme that you are using.

Cisco ISE implements a change where Cisco ISE cannot consume Advanced licenses when endpoints are statically assigned to a profile. The number of endpoints that are dynamically profiled, and the profile of those endpoints is used in an authorization policy can be compared only with the limit of the Advanced licenses.

The endpoints that are statically assigned to a profile are now excluded from utilizing licenses that are included in the Advanced license package, but they are still compared against the limit of Base licenses. Earlier, it compares the total number of concurrent endpoints across the entire deployment against the limit of the Advanced licenses.

For more information on how licenses are used in the Cisco ISE profiling service, see Licenses for the Profiling Service, page 18-4.

For more information on managing licenses in Cisco ISE, see Chapter 12, "Managing Licenses."

For more information on the license types that are available in the Cisco ISE licensing scheme, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1.*

IP Address and MAC Address Binding in Cisco ISE

You can only create or update endpoints by using their MAC addresses in an enterprise network. If you do not find an entry in the ARP cache, then you can create or update endpoints by using the L2 MAC address of an HTTP packet and IN_SRC_MAC of a NetFlow packet in the Cisco ISE, Release 1.1.

Earlier, the profiling service is dependent on L2 adjacency when endpoints are only a hop away. When endpoints are L2 adjacent, the IP addresses and MAC addresses of endpoints are already mapped, and there is no need for IP-MAC cache mapping. If endpoints are not L2 adjacent and are multiple hops away, there may not be a reliable mapping.

Some of the known attributes of NetFlow packets that you collect are PROTOCOL, L4_SRC_PORT, IPV4_SRC_ADDR, L4_DST_PORT, IPV4_DST_ADDR, IN_SRC_MAC, OUT_DST_MAC, IN_SRC_MAC and OUT_SRC_MAC. When endpoints are not L2 adjacent and are multiple L3 hops away, the IN_SRC_MAC attributes carry only the MAC addresses of L3 network devices.

When the HTTP probe is enabled in Cisco ISE Release 1.1, you can only create endpoints by using the MAC addresses of HTTP packets, as the HTTP request messages do not carry IP addresses and MAC addresses of endpoints in the payload data.

The Cisco ISE, Release 1.1 implements an ARP cache in the profiling service, so that you can reliably map IP addresses and MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry IP addresses and MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and the Framed-IP-address attribute in the RADIUS probe carry the IP addresses of endpoints, along with their MAC addresses, which can be mapped and stored in the ARP cache.

A network scan may or may not return the MAC addresses of endpoints. It uses an IP-MAC address binding for those endpoints from the IP addresses received.

Integrating Cisco ISE with Cisco Network Admission Control Appliance

Cisco ISE supports integration with Cisco Network Admission Control (NAC) Appliance, Release 4.9 when you have installed an Advanced or Wireless license in Cisco ISE.

Integrating Cisco ISE with Cisco NAC Appliance, Release 4.9 allows you to utilize the Cisco ISE profiling service in a Cisco NAC deployment. The Cisco ISE profiler is similar to the Cisco Network Admission Control (NAC) Profiler in a Cisco NAC deployment, which manages endpoints in an enterprise network. This integration allows you to replace the existing Cisco NAC Profiler that is installed in a Cisco NAC deployment. It allows you to synchronize profile names from the Cisco ISE profiler, as well as the result of endpoint classification, into the Cisco Clean Access Manager (CAM).

Prerequisites:

You must have installed the Cisco NAC Appliance and performed initial configuration to introduce the Clean Access Manager (CAM) and Clean Access Server (CAS) into the network.

Note You must export the contents of X509 Certificate from the Clean Access Manager in Administration > Clean Access Manager > SSL, and import the same into the primary Administration ISE node in the Cisco ISE under Administration > System > Certificates > Certificate Authority Certificate for a proper secure communication between Cisco ISE and CAM.

For more information on installing Cisco NAC Appliance hardware, see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9*. You must also use the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9* and *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9* to install, configure and administer the Cisco NAC Appliance, Release 4.9.

Refer to the compatible set of documents for Cisco NAC Appliance, Release 4.9 in the following locations:

- http://www.cisco.com/en/US/products/ps6128/prod_installation_guides_list.html
- http://www.cisco.com/en/US/products/ps6128/products_installation_and_configuration_guides_list.html
- http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html

For more information on configuring CAMs in Cisco ISE, see the Configuring Cisco Clean Access Managers in Cisco ISE, page 18-76.

Configuring Cisco Clean Access Managers in Cisco ISE

The primary Administration ISE node is responsible for all the communication between Cisco ISE and the Cisco NAC Appliance. You can have only one primary Administration ISE node in a distributed deployment, and it must assume the Administration persona. You can also have a maximum of two Administration ISE nodes that assume the Administration persona, one being the primary node and the other being the secondary node for high availability. This allows a failover support in a high-availability configuration of a Cisco ISE distributed deployment. There is no automatic failover for the Administration ISE nodes.

In a high-availability configuration, the primary Administration ISE node is in the active state, to which all configuration changes are made. The secondary Administration ISE node is in the standby state, to which all configuration changes are updated from the primary Administration ISE node. When the primary Administration ISE node goes down, you must log into the user interface of the secondary Administration ISE node and make it the primary node. Therefore, you always have a complete copy of the configuration from the primary Administration ISE node.

For more information, see Chapter 9, “Setting Up Cisco ISE in a Distributed Environment.”

You can configure CAMs only on the primary Administration ISE node in Cisco ISE. The credentials that are used at the time of registering one or more CAMs on the primary Administration ISE node are used to authenticate connectivity with CAMs.

The communication between Cisco ISE and the Cisco NAC Appliance is secure over Secure Sockets Layer (SSL). It is also bidirectional in nature, as Cisco ISE pushes the profiler configuration changes to CAMs, and CAMs periodically pull the list of MAC addresses of endpoints and their corresponding profiles, as well as the list of all the profile names, from Cisco ISE.

The Cisco ISE profiler notifies the profiler configuration changes to all the registered CAMs from the primary Administration ISE node. It avoids duplicating notification in a Cisco ISE distributed deployment. It uses the REST APIs to notify the profiler configuration changes when there are endpoints added or removed, and endpoint policies changed, in the Cisco ISE database. During an import of endpoints, the Cisco ISE profiler notifies CAMs only after the import is complete.

The following REST API flows are implemented to push the profiler configuration changes to CAMs:

- Cisco ISE profiler endpoint change push—When endpoints are profiled and there are changes in the profiles of endpoints in Cisco ISE, then the Cisco ISE profiler notifies all the registered CAMs about the changes in the endpoint profiles.

You can also configure Cisco ISE in CAMs, which allows you to synchronize CAMs with Cisco ISE, depending on your Sync Settings in CAMs. You must create rules, where you can select one or more matching profiles from the list of Cisco ISE profiles and map endpoints to any one of the Access Types in CAMs. CAMs periodically retrieve endpoints and their corresponding profiles, as well as the list of all the profile names, from the Cisco ISE profiler.

The following REST API flows are implemented to pull the profiler configuration changes from the Cisco ISE profiler:

- NAC Manager endpoint pull—Pulls the list of MAC addresses of endpoints and their corresponding profiles of known endpoints.
- NAC Manager profile pull—Pulls the profile names from the Cisco ISE profiler.

The Cisco ISE profiler notifies the Cisco ISE Monitoring persona of all the events that can be used to monitor and troubleshoot Cisco ISE and Cisco NAC Appliance, Release 4.9 integration.

The Cisco ISE profiler log captures the following events for monitoring and troubleshooting integration:

- Configuration changes for NAC Settings (Information)
- NAC notification event failure (Error)

Filtering, Adding, Editing, and Deleting Clean Access Managers in Cisco ISE

Cisco ISE allows you to register multiple CAMs on a primary Administration ISE node in a distributed deployment for REST APIs communication settings. The list of CAMs that is registered in Cisco ISE is the list to which all the profiler configuration changes are notified. When registering CAMs in Cisco ISE, you must provide the IP addresses of CAMs, usernames, and passwords that allow you to log into the CAMs.



Note You can use the virtual service IP address that a pair of CAMs share in a high-availability configuration. This allows a failover support of CAMs in a high-availability configuration. For more information on how to set up a pair of CAMs for high availability, see the compatible link for Cisco NAC Appliance, Release 4.9.
http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/49/hi_ha.html#wp1084663.

The NAC Managers page allows you to configure multiple CAMs, which provides an option to filter the CAMs that you have registered. This page lists the CAMs along with their names, descriptions, IP addresses, and the status that displays whether endpoint notification is enabled or not for those CAMs.

The procedure for managing Cisco CAMs includes the following tasks:

- Filtering Cisco Clean Access Managers in Cisco ISE, page 18-78

- Adding Cisco Clean Access Managers to Cisco ISE, page 18-80
- Editing Cisco Clean Access Managers in Cisco ISE, page 18-80
- Deleting Cisco Clean Access Managers in Cisco ISE, page 18-81

Filtering Cisco Clean Access Managers in Cisco ISE

You can use the Show drop-down list, or click the filter icon both to invoke a quick filter and close it on the NAC Managers page. A quick filter is a simple filter that you can use to filter CAMs on the NAC Managers page. The quick filter filters CAMs based on field descriptions, such as the names, the descriptions, and IP addresses on the NAC Managers page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that you can preset for use later and retrieve, along with the results, on the NAC Managers page. The advanced filter filters CAMs based on a specific value that is associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can manage preset filters by using the Manage Preset Filters option, which lists all the preset filters. A preset filter from the list has a session lifetime, which displays the results on the NAC Managers page. Once created and saved a preset filter, you can choose a preset filter of filtered results on the NAC Managers page. You can also edit preset filters and remove them from the preset filters list.

To filter CAMs on the NAC Managers page, complete the following steps:

Step 1 Choose **Administration > Network Resources > NAC Managers**.

The NAC Managers page appears, which lists all the CAMs that are registered in Cisco ISE.

Step 2 From the NAC Managers page, click the Show drop-down arrow to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or the Manage Preset Filters option, which allows you to manage preset filters for filtering. See Table 18-23.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 18-78 and the "To filter by using the Advanced Filter option, complete the following steps:" section on page 18-79.

Note To return to the list of CAMs, choose **All** from the Show drop-down list to display all the CAMs without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters CAMs based on each field description on the NAC Managers page. When you click inside any field, and as you enter the search criteria in the field, it refreshes the page with the results on the NAC Managers page. If you clear the field, it displays the list of all the CAMs on the NAC Managers page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter CAMs by using variables that are more complex. It contains one or more filters, which filter CAMs based on the values that match the field descriptions. A filter on a single row filters CAMs based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter the CAMs by using any one or all of the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or choose **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or click **Cancel** to clear the filter.

Table 18-23 describes the fields that allow you to filter CAMs on the NAC Managers page.

Table 18-23 Filtering Clean Access Managers

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter CAMs by using the name of the CAM.
	IP Address	This field enables you to filter CAMs by using the IP address that is registered with Cisco ISE.
	Description	This field enables you to filter CAMs by using the description of the CAM.
Advanced Filter	Choose the field description from the following: • Name • IP Address • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that you can use to filter CAMs.
	Value	From the Value field, choose the value for the field description that you selected against, which the CAMs are filtered.

Adding Cisco Clean Access Managers to Cisco ISE

To add CAMs on the NAC Managers page, complete the following steps:

Step 1 Choose **Administration > Network Resources > NAC Managers**.

The NAC Managers page appears.

Step 2 From the NAC Managers page, choose **Add**.

Warning **Once created and saved, the IP Address of the CAM is not editable.**

The New NAC Manager page appears.

Step 3 Modify the values on the New NAC Manager page, as shown in Table 18-24.

Step 4 Click **Save**.

The Cisco Clean Access Manager that you configured appears on the NAC Managers page.

Step 5 Click the **NAC Manager List** link on the New NAC Manager page to return to the NAC Managers page.

Table 18-24 describes the fields on the New NAC Manager page that allow you to create a CAM.

Table 18-24 Adding NAC Managers

Field Name	Description
Name	From the Name field, enter the name of the Cisco Access Manager (CAM).
Status	From the Status field, click the check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.
Description	From the Description field, enter the description of the CAM.
IP Address	From the IP Address field, enter the IP address of the CAM. Once you have created and saved a CAM on Cisco ISE, the IP address of the CAM cannot be edited. You cannot use 0.0.0.0 and 255.255.255.255, as they are excluded when validating the IP addresses of the CAMs in Cisco ISE, and so, they are not valid IP addresses that you can use in the IP Address field for the CAM.
Username	From the Username field, enter the username of the CAM administrator that allows you to log on to the CAM.
Password	From the Password field, enter the password of the CAM administrator that allows you to log on to the CAM.

Editing Cisco Clean Access Managers in Cisco ISE

You can edit the details of CAMs from the NAC Managers page, except for the IP address of the CAM.

To edit a CAM on the NAC Managers page, complete the following:

Step 1 Choose **Administration > Network Resources > NAC Managers**.

The NAC Managers page appears. From the NAC Managers page, choose a CAM.

Step 2 Choose **Edit**.

Step 3 Modify the values of the fields on the edit page, as shown in Table 18-24 on page 18-80.

Click the **NAC Manager List** link from the edit page to return to the NAC Managers page without saving the current input data. During an edit, you can also click the **Reset** button without saving the current input data on the edit page. Here, you can retain the configuration without saving the current input data on the edit page.

Step 4 Click **Save** to save the current input data on the edit page.

Step 5 Click the **NAC Manager List** link from the edit page to return to the NAC Managers page after editing a CAM.

Deleting Cisco Clean Access Managers in Cisco ISE

You can delete a CAM from the NAC Managers page.

To delete a CAM on the NAC Managers page, complete the following:

Step 1 Choose **Administration > Network Resources > NAC Managers**.

The NAC Managers page appears. From the NAC Managers page, choose a CAM.

Step 2 Choose **Delete**.

If you choose to delete a CAM from the NAC Managers page, Cisco ISE displays a confirmation dialog. Clicking **Delete** from the dialog deletes the CAM from the NAC Managers page. Clicking **Cancel** from the dialog returns to the NAC Managers page without deleting the CAM.



CHAPTER 19

Configuring Client Provisioning Policies

This chapter describes how to manage client provisioning resources and create client provisioning policies for your network.

- Client Provisioning Overview, page 19-1
- Adding and Removing Agents and Other Resources, page 19-4
- Setting Up Global Client Provisioning Functions, page 19-26
- Configuring Client Provisioning Resource Policies, page 19-28
- Client-side Installation and Log-In, page 19-30

Client Provisioning Overview

Cisco Identity Services Engine (ISE) looks at various elements when classifying the type of login session through which users access the internal network, including:

- Client machine operating system and version
- Client machine browser type and version
- Group to which the user belongs
- Condition evaluation results (based on applied dictionary attributes)

After Cisco ISE classifies a client machine, it uses client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles, if necessary.

Cisco ISE Agents

Cisco NAC Agent for Windows Clients

The Cisco NAC Agent provides the posture assessment and remediation for client machines.

Users can download and install the Cisco NAC Agent (read-only client software), which can check the host registry, processes, applications, and services. The Cisco NAC Agent can be used to perform Windows updates or antivirus and antispyware definition updates, launch qualified remediation programs, distribute files uploaded to the Cisco ISE server, distribute web site links to web sites in order for users to download files to fix their system, or simply distribute information and instructions.

Warning **The NAC Agents cannot communicate with the Cisco ISE server securely and the Cisco ISE server throws an error when the Windows XP clients do not have the latest Windows hotfixes and patches installed in them. You must ensure that the latest Windows hotfixes and patches are installed on Windows XP clients so that NAC Agents can establish a secure and encrypted communication with the Cisco ISE server (SSL over TCP).**

Uninstalling Cisco NAC Agent for Windows Clients

The Agent installs to **C:\Program Files\Cisco\Cisco NAC Agent** on the Windows client. You can uninstall the Agent in the following ways:

- By double-clicking the **Uninstall Cisco NAC Agent** desktop icon
- By going to **Start Menu > Programs > Cisco Systems > Cisco Clean Access > Uninstall Cisco NAC Agent**
- By going to **Start Menu > Control Panel > Add or Remove Programs > Cisco NAC Agent**

To uninstall Cisco NAC Agent in a Windows 8 client, execute the following:

Step 1 Switch to Metro Mode.

Step 2 Right-Click **Cisco NAC Agent** tile.

Step 3 Select **Un-Install** from the options available at the bottom of the screen.

Step 4 The system automatically switches to Desktop mode and opens **Add/Remove** control panel.

Step 5 In the **Add/Remove** control panel, perform one of the following:

- Double Click **Cisco NAC Agent**.
- Select **Cisco NAC Agent** and click **Uninstall**.
- Right Click **Cisco NAC Agent** and select **Uninstall**.

Cisco NAC Agent for Macintosh Clients

The Macintosh NAC Agent provides the posture assessment and remediation for client machines.

Users can download and install the Cisco NAC Agent (read-only client software), which can check antivirus and antispyware definition updates.

After users log into the Cisco NAC Agent, the Agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client, the user is allowed network access. If requirements are not met, the Agent presents a dialog to the user for each requirement that is not satisfied. The dialog provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept the restricted network access while they try to remediate the client system so that it meets requirements for the user login role.

Uninstalling Cisco NAC Agent for Macintosh Clients

You can uninstall the NAC Agent for Mac OS X clients by running the uninstall script as follows:

Step 1 Open the navigator pane and navigate to *<local drive ID>* > **Applications**.

Step 2 Highlight and right-click the **CCAAgent** icon to bring up the selection menu.

Step 3 Choose **Show Package Contents** and double-click **NacUninstall**.

Step 4 This will uninstall the Agent on Mac OS X.

NAC Web Agent

The Cisco NAC Web Agent provides temporal posture assessment for client machines.

Users can launch the Cisco NAC Web Agent executable, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet.

After users log into the Cisco NAC Web Agent, the Web Agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks the host registry, processes, applications, and services for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client, the user is allowed network access. If requirements are not met, the Web Agent presents a dialog to the user for each requirement that is not satisfied. The dialog provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept the restricted network access while they try to remediate the client system so that it meets requirements for the user login role.

Agent and Client Machine Operating System Compatibility

For a complete list of supported client machine operating systems and agents, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

Adding and Removing Agents and Other Resources

- Viewing and Displaying Client Provisioning Resources, page 19-4
- Adding Client Provisioning Resources to Cisco ISE, page 19-5
- Creating Agent Profiles, page 19-12
- Deleting Client Provisioning Resources, page 19-24
- Provisioning Client Machines with the Cisco NAC Agent MSI Installer, page 19-24

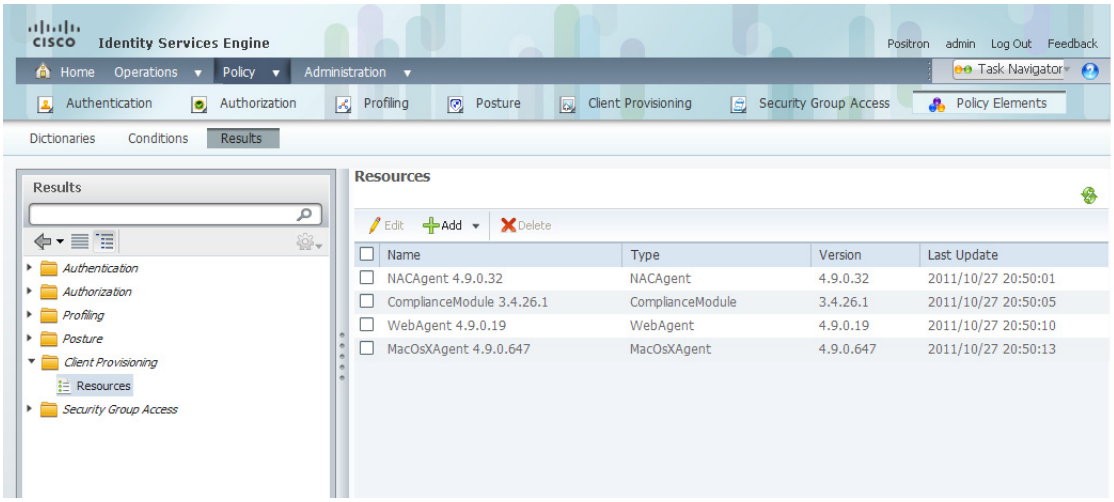
Viewing and Displaying Client Provisioning Resources

To display the list of existing resources that are available to configure client provisioning resource policies, open the Cisco ISE web console user interface and choose **Policy > Policy Elements > Results > Client Provisioning > Resources**. The Client Provisioning Resources List page displays the following types of resources:

- Persistent and temporal agents:
  - Windows and Mac OS X Cisco Network Admission Control (NAC) Agents
  - Cisco NAC Web Agent
- Agent profiles
- Agent compliance modules
- Agent customization packages

Figure 19-1 shows the Client Provisioning Resources List page.

Figure 19-1 Policy > Policy Elements > Results > Client Provisioning > Resources



If this display is empty (that is, if there are no client provisioning resources that are available on Cisco ISE), you can add resources using the procedures in Adding and Removing Agents and Other Resources, page 19-4.

Adding Client Provisioning Resources to Cisco ISE

Before you can configure client provisioning resource policies that enable users to download and install resources on client machines, you must ensure that those resources are already present on the Cisco ISE appliance. You can use the resource download and creation functions described here to ensure the following Cisco ISE resources are available in Cisco ISE:

- Persistent and temporal agents (Windows and Mac OS X Cisco NAC Agents, Cisco NAC Web Agent). For detailed information on agent types available in Cisco ISE, see Cisco ISE Agents, page 19-1.
- Agent profiles
- Agent compliance modules
- Agent customization packages

The following topics describe how to add client provisioning resources from a remote source or from a local machine:

- Adding Client Provisioning Resources from a Remote Source, page 19-5
- Adding Client Provisioning Resources from a Local Machine, page 19-6
- Creating Agent Customization Files to Add to Cisco ISE, page 19-7

Note You can also configure Cisco ISE to automatically update client provisioning resources. For details, see Downloading Client Provisioning Resources Automatically, page 19-27.

Adding Client Provisioning Resources from a Remote Source

Prerequisites

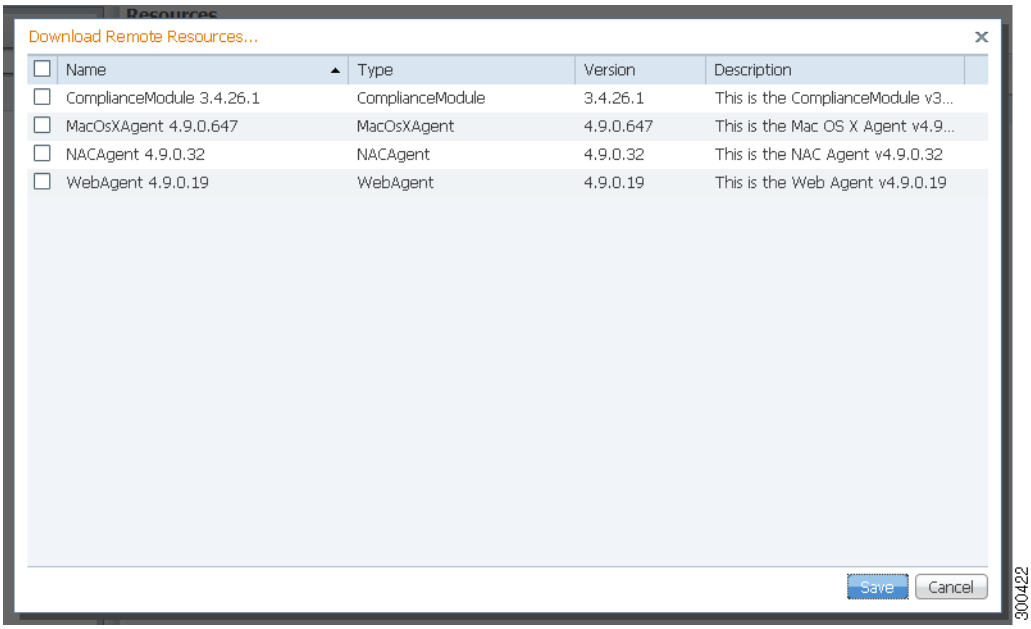
To ensure you are able to access the appropriate remote location from which you can download client provisioning resources to Cisco ISE, you may need to verify that you have the correct proxy settings configured for your network as described in Specifying Proxy Settings in Cisco ISE, page 8-17.

To add client provisioning resources from a remote source like Cisco.com, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > Add resources from Cisco site** (Figure 19-2).

Figure 19-2 Add resources from Cisco site



Step 3 Select one or more required resources from the list available in the Downloaded Remote Resources dialog box that appears.

Step 4 Click **Save** to download the selected resources to Cisco ISE.

Depending on the type and number of resources that you select, and available network bandwidth, Cisco ISE can take a few seconds (or even a few minutes, depending on the size and type of resource) to download the new resources and display them in its list of available client provisioning resources.

Next Steps

After you have successfully added client provisioning resources to Cisco ISE, you can begin to configure resource policies, as described in Configuring Client Provisioning Resource Policies, page 19-28.

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

Adding Client Provisioning Resources from a Local Machine

Caution Be sure to upload only current, supported resources to Cisco ISE. Older, unsupported resources (older versions of the Cisco NAC Agent, for example) will likely cause serious issues for client access. For details, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

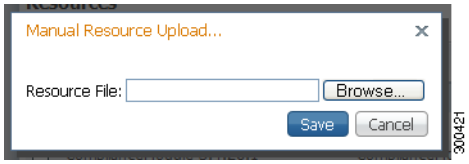
For downloading the resource files manually from the CCO, refer to “Cisco ISE Offline Updates” section in the *Release Notes for the Cisco Identity Services Engine, Release 1.1*.

To add existing client provisioning resources from a local machine (for example, files that you may have already downloaded from CCO to your laptop), complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > Add resource from local disk** (Figure 19-3).

Figure 19-3 Add resources from local disk



Step 3 Click **Browse** and navigate to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.

Step 4 Highlight the resource file in the search window, and click **Save**.

Depending on the type of resource file that you select, and the available network bandwidth between Cisco ISE and your local machine, Cisco ISE can take a few seconds to a few minutes to download the new resource file and display it in its list of available client provisioning resources.

Next Steps

After you have successfully added client provisioning resources to Cisco ISE, you can begin to configure resource policies, as described in Configuring Client Provisioning Resource Policies, page 19-28.

Creating Agent Customization Files to Add to Cisco ISE

A customization package is a zip file that contains an XML descriptor file and another zip with the contents of the customized options. There are three steps required for creating a new customization package.

Step 1 After modifying the required files like **logo.gif**, create a zip file called **brand-win.zip**. For example, in a Linux or Unix environment, execute the following:

zip -r brand-win.zip nacStrings_en.xml nac_login.xml nac_logo.gif nacStrings_cy.xml nacStrings_el.xml

The **brand-win.zip** file usually contains the following files:

- nac_logo.gif
- nac_login.xml
- nacStrings_xx.xml

The following parameters can be customized:

- Logo
- Agent Login Screen
- Predetermined Set of Agent Strings and Fields

Logo

The Cisco logo that appears in all the Cisco NAC Agent screens can be replaced with your brand logo. The image should be a .gif file, not exceeding 67 x 40 pixels. The logo image should be named **nac_logo.gif**.

Agent Login Screen

By default, the Cisco NAC Agent Login screen appears as shown in Figure 19-4.

Figure 19-4 Cisco NAC Agent Login—Default Screen



The elements that appear on the Cisco NAC Agent Login screen can be customized by using either one of the following methods:

- Modify the **nac_login.xml** file
- Modify the **nacStrings_xx.xml** file

Note You can replace the default logo by using the **nac_logo.gif** file.

In a system that has the Cisco NAC Agent installed at the default location, you can find the above files in the following directories:

- The **nac_login.xml** file is available in the "C:\Program Files\Cisco\Cisco NAC Agent\UI\nac_divs\login" directory.
- In the **nacStrings_xx.xml** file, the "xx" indicates the locale. You can find a complete list of the files in the "C:\Program Files\Cisco\Cisco NAC Agent\UI\cues_utility" directory.

Note The files are available in the directories mentioned above when the Agent is installed at the default location. If the Agent is installed at a different location, then the files would be available at "<*Agent Installed path*>\Cisco\Cisco NAC Agent\UI\nac_divs\login" and "<*Agent Installed path*>\Cisco\Cisco NAC Agent\cues_utility".

Tip Cisco recommends making changes in the **nacStrings_xx.xml** file.

The following example shows a part of contents of the **nac_login.xml** file. The customized text is shown in boldface.

```
<tr class="nacLoginMiddleSectionContainerInput">
   <td colspan="2">
      <fieldset width="100%" id="nacLoginCustomAlert"
                style="display:block" class="nacLoginAlertBox">
          <table width="100%">
             <tr>
                <td id="nacLoginCustomAlert.img" valign="top" width="32px">
                  <img src="./cues_icons/Status_warning_icon.png" align="absmiddle"
onload="cuesFixPNG(null,this)"></img>
                </td>
                <td id="nacLoginCustomAlert.content" class="nacLoginAlertText">
                  <cues:localize key="login.customalert"/>
                </td>
              </tr>
          </table>
       </fieldset>
    </td>
</tr>
<tr id="nacLoginRememberMe" style="visibility:hidden">
    <td>
       <cues:localize key="cd.nbsp"/>
    </td>
    <td class="cuesLoginField" >
      <nobr>
      <input type="checkbox" alt="" title="" name="rememberme"
             id="rememberme" checked="true" />
            <cues:localize key="login.remember_me"/>
      </nobr>
    </td>
</tr>
```

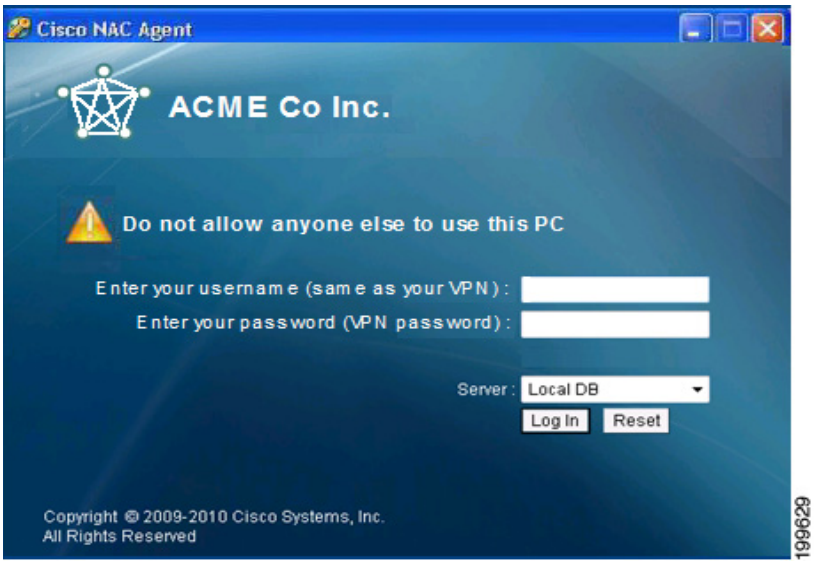
The following example shows a part of contents of the **nacStrings_xx.xml** file. The customized text is shown in boldface.

```
<cueslookup:name key="login.productname"> ACME Co Inc. </cueslookup:name>
<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.username"> Enter your username (same as your VPN)
</cueslookup:name>
<cueslookup:name key="login.password">Enter your password (VPN password)</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
<cueslookup:name key="login.customalert">Do not allow anyone else to use this
PC</cueslookup:name>
```

```
<cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
<cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
<cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>
```

The above file has been modified to customize the login screen as shown in Figure 19-5.

Figure 19-5 Cisco NAC Agent Login—Customized Screen



Notice that the “Remember Me” check box has been removed. In addition, you can find more text for the “Username” and “Password” fields.

Note Though there is no limit for the number of characters used for the customized text, Cisco recommends restricting them so that they are not occupying too much of space in the Login screen.

Predetermined Set of Agent Strings and Fields

Modify the **nacStrings_xx.xml** file to replace the Device Posture Status (DPS) details. The following is a part of the **nacStrings_xx.xml** file with DPS values.

Example nacStrings_xx.xml File:

```
<cueslookup:name key="dp.status.fullNetAccess">Full Network Access</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">Your device conforms with all the
security policies for this protected network</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">Only optional requirements are
failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">Refreshing IP address. Please
Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">Refreshing IP address
succeeded.</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">Connecting to protected
Network. Please Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">Guest Network Access</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">Network Access Denied</cueslookup:name>
```

```
<cueslookup:name key="dp.status.noNetAccess.verbose">There is at least one mandatory
requirement failing. You are required to update your system before you can access the
network.</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">Network Usage Terms and
Conditions are rejected. You will not be allowed to access the network.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">Restricted Network Access
granted.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">You have been granted
restricted network access because your device did not conform with all the security
policies for this protected network and you have opted to defer updating your system. It
is recommended that you update your system at your earliest convenience.</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">Temporary Network
Access</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">Please be patient
while your system is checked against the network security policy.</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">There is at least one
mandatory requirement failing. You are required to update your system otherwise your
network access will be restricted.</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">Only optional requirements
are failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">Temporary Access to the network
has expired.</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose"> </cueslookup:name>
```

Step 2 Create an XML descriptor file like the following:

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:update="http://www.cisco.com/cpm/update/1.0">
      <title>Provisioning Update</title>
      <updated>2011-12-21T12:00:00Z</updated>
      <id>https://www.cisco.com/web/secure/pmbu/provisioning-update.xml</id>
      <author>
            <name>Cisco Support</name>
            <email>support@cisco.com</email>
      </author>

      <!-- Custom Branding -->
        <entry>
                <id>http://foo.foo.com/foo/AgentCustomizationPackage/1/1/1/1</id> -- This
id can be anything, but should be unique within an ISE deployment
                <title>Agent Customization Package</title>
                <updated>2010-06-07T12:00:00Z</updated>
                <summary>This is the agent customization package </summary> - Can be
anything
                <link rel="enclosure" type="application/zip" href="brand-windows.zip"
length="18884" />
                <update:type>AgentCustomizationPackage</update:type>
                <update:version>1.1.1.0</update:version> -- Important to have this as 4
digit
                <update:os>Win</update:os>
        </entry>
</feed>
```

Step 3 Create another zip file that contains the descriptor file above and the zip file created in Step 1. For example, in a Linux or Unix environment, execute the following:

zip -r custom.zip updateFeed.xml brand-win.zip

Step 4 Upload the new custom.zip file to Cisco ISE using the guidelines described in Adding Client Provisioning Resources from a Local Machine, page 19-6.

Creating Agent Profiles

- Creating Windows Agent Profiles in Cisco ISE, page 19-12
- Creating Mac OS X Agent Profiles in Cisco ISE, page 19-14
- Modifying Windows and Mac OS X Agent Profiles in Cisco ISE, page 19-15
- Agent Profile Parameters and Applicable Values, page 19-16

Cisco recommends configuring agent profiles to control remediation timers, network transition delay timers, and the timer that is used to control the login success screen on client machines so that these settings are policy based. However, when there are no agent profiles configured to match client provisioning policies, you can use the settings in the **Administration > System > Settings > Posture > General Settings** configuration page to accomplish the same goal. See Posture General Settings, page 20-10 for more details.

Note Once you configure and upload an agent profile to a client machine via policy enforcement or other method, that agent profile remains on the client machine and affects the client machine login and operation behavior until you change it to something else. Therefore, deleting an agent profile from Cisco ISE does not remove that behavior from previously affected client machines. To alter the login and operational behavior, you must define a new agent profile that *overwrites* the values of existing agent profile parameters on the client machine and upload it via policy enforcement.

Creating Windows Agent Profiles in Cisco ISE

Prerequisites

Before you create a Windows agent profile, Cisco recommends you upload agent software to Cisco ISE per the guidelines at:

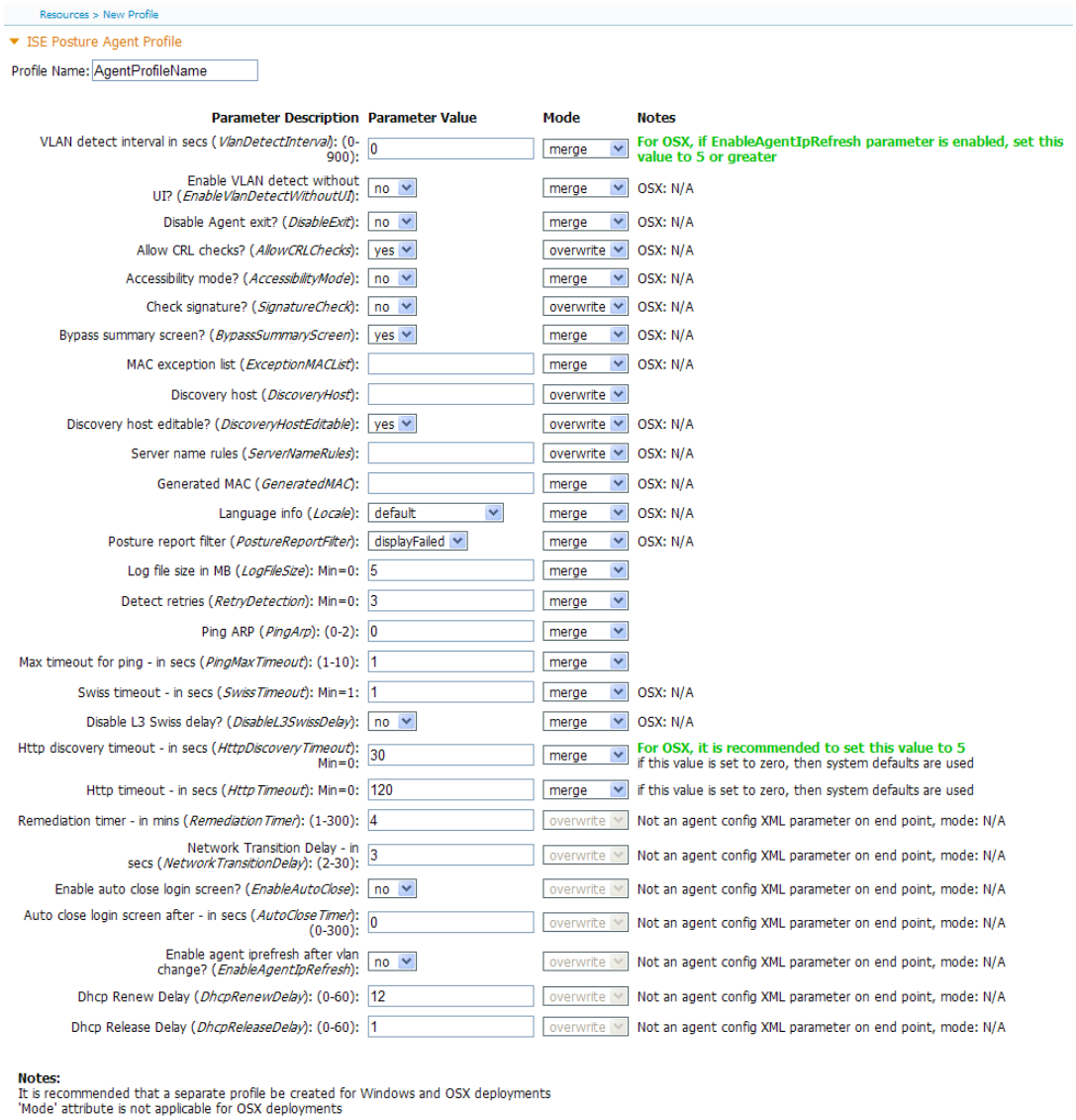
- Adding Client Provisioning Resources from a Remote Source, page 19-5
- Adding Client Provisioning Resources from a Local Machine, page 19-6

To create a Windows agent profile, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > ISE Posture Agent Profile** (Figure 19-6).

Figure 19-6 ISE Posture Agent Profile



Step 3 Specify a name for the Windows agent profile.

Step 4 Specify values for parameters, and specify whether these settings should merge with or overwrite existing profile settings as necessary to appropriately configure Windows client machine agent behavior.

When you set one or more of the parameters to merge with any existing agent profile, new (previously undefined) parameters are set according to the merged value, but existing parameter settings in an agent profile are maintained. For details regarding the various parameters and their settings, see Agent Profile Parameters and Applicable Values, page 19-16.

Step 5 Click **Submit** to save the agent profile to Cisco ISE. The new file now appears in the list of available client provisioning resources.

Next Steps

After you have successfully added client provisioning resources to Cisco ISE and configured one or more optional agent profiles, you can begin to configure resource policies, as described in Configuring Client Provisioning Resource Policies, page 19-28.

Example XML File Generated Using the Create Profile Function

```
<?xml version="1.0" ?>
<cfg>
   <VlanDetectInterval>0</VlanDetectInterval>
   <RetryDetection>3</RetryDetection>
   <PingArp>0</PingArp>
   <PingMaxTimeout>1</PingMaxTimeout>
   <EnableVlanDetectWithoutUI>0</EnableVlanDetectWithoutUI>
   <SignatureCheck>0</SignatureCheck>
   <DisableExit>0</DisableExit>
   <PostureReportFilter>displayFailed</PostureReportFilter>
   <BypassSummaryScreen>1</BypassSummaryScreen>
   <LogFileSize>5</LogFileSize>
   <DiscoveryHost></DiscoveryHost>
   <DiscoveryHostEditable>1</DiscoveryHostEditable>
   <Locale>default</Locale>
   <AccessibilityMode>0</AccessibilityMode>
   <SwissTimeout>1</SwissTimeout>
   <HttpDiscoveryTimeout>30</HttpDiscoveryTimeout>
   <HttpTimeout>120</HttpTimeout>
   <ExceptionMACList></ExceptionMACList>
   <GeneratedMAC></GeneratedMAC>
   <AllowCRLChecks>1</AllowCRLChecks>
   <DisableL3SwissDelay>0</DisableL3SwissDelay>
   <ServerNameRules></ServerNameRules>
</cfg>
```

Note This file also contains two static (that is, uneditable by the user or Cisco ISE administrator) “AgentCfgVersion” and “AgentBrandVersion” parameters used to identify the current version of the agent profile and agent customization file, respectively, on the client machine. If Cisco ISE has a different agent profile than what is present on the client machine (determined using MD5 checksum), then Cisco ISE downloads the new agent profile to the client machine. If the agent customization file originating from Cisco ISE is different, Cisco ISE downloads the new agent customization file to the client machine, as well.

Creating Mac OS X Agent Profiles in Cisco ISE

The parameters available to configure for Mac OS X client machines are only a subset of those available for Windows client machines. Cisco recommends you avoid specifying settings for any parameters that feature a note reading “Mac platform: N/A,” as these settings have no effect on agent behavior on Mac OS X client machines.

Prerequisites

Before you create a Mac OS X agent profile, Cisco recommends you upload agent software to Cisco ISE per the guidelines at:

- Adding Client Provisioning Resources from a Remote Source, page 19-5
- Adding Client Provisioning Resources from a Local Machine, page 19-6

To create a Mac OS X agent profile, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Choose **Add > Profile**.

Step 3 Specify a name for the agent profile.

Step 4 Specify values for parameters, and specify whether these settings should merge with or overwrite existing profile settings as necessary to appropriately configure Mac OS X client machine agent behavior.

When you set one or more of the parameters to merge with any existing agent profile, new (previously undefined) parameters are set according to the merged value, but existing parameter settings in an agent profile are maintained. For details regarding the various parameters and their settings, see Agent Profile Parameters and Applicable Values, page 19-16.

Step 5 Click **OK** to save the Mac OS X agent profile to Cisco ISE. The new file now appears in the list of available client provisioning resources.

Next Steps

After you have successfully added client provisioning resources to Cisco ISE and configured one or more optional agent profiles, you can begin to configure resource policies, as described in Configuring Client Provisioning Resource Policies, page 19-28.

Modifying Windows and Mac OS X Agent Profiles in Cisco ISE

Prerequisites

To modify a Windows or Mac OS X agent profile, you must have already manually created one or more agent profiles according to the guidelines in:

- Creating Windows Agent Profiles in Cisco ISE, page 19-12
- Creating Mac OS X Agent Profiles in Cisco ISE, page 19-14

To modify an existing Windows or Mac OS X agent profile, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Step 2 Select an existing agent profile entry and click **Edit**.

Step 3 Make any necessary changes in the existing agent profile and click **Save**. For details regarding the various parameters and their settings, see Agent Profile Parameters and Applicable Values, page 19-16.

Note If you choose the **Reset** option, all parameter values are automatically reset to their respective default settings.

Next Steps

After you have successfully added client provisioning resources to Cisco ISE and configured or modified one or more existing optional agent profiles, you can begin to configure resource policies, as described in Configuring Client Provisioning Resource Policies, page 19-28.

Agent Profile Parameters and Applicable Values

This section provides descriptions, default values, and allowable ranges for the agent profile parameters used to customize login, operational, and logout behavior for agents that are installed on a client machine. Agent configuration parameters are grouped by function and appear in the following tables:

- Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs
- Customize Agent Login/Logout Dialog Behavior
- Manage Client-side MAC Address and Agent Discovery Host
- Specify Agent Localization Settings
- Report and Log Display Settings
- Recurring Client Machine Connection Verification
- Additional SWISS Discovery Customization
- HTTP Discovery Customization
- Remediation Timeout Customization
- Agent Dialog Behavior on User Logout or Shutdown
- IP Address Behavior Settings for Client Machines

Table 19-1 Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs

Parameter	Default Value	Valid Range	Description or Behavior
Vlan detect interval	0 [1], 5 [2]	0, 5-900	• If this setting is 0, the Access to Authentication VLAN change feature is disabled. • If this setting is 1-5, the agent sends ICMP or ARP queries every 5 sec. • If this setting is 6-900, an ICMP or ARP query is sent every *x* sec.
Enable VLAN detect without UI?	no	yes or no	• If this value is set to no, the VLAN detect feature is disabled. • If this value is set to yes, the VLAN detect feature is enabled. **Note** This setting does not apply to Mac OS X client machine agents.

1. For the Cisco NAC Windows Agent, the default value is 0. By default, the Access to Authentication VLAN change feature is disabled for Windows.
2. For the Mac OS X Agent, the default value is 5. By default, the Access to Authentication VLAN change feature is enabled with VlanDetectInterval as 5 seconds for Mac OS X.

Table 19-2 Customize Agent Login/Logout Dialog Behavior

Parameter	Default Value	Valid Range	Description or Behavior
Disable Agent Exit?	no	yes or no	If this parameter is set to yes, users cannot exit the agent via the system tray icon. **Note** This setting does not apply to Mac OS X client machine agents.
Allow CRL Checks?	yes	yes or no	Setting this parameter to no turns off certificate revocation list (CRL) checking for the agent during discovery and negotiation with the Cisco ISE node. **Note** This setting does not apply to Mac OS X client machine agents.
Accessibility mode?	no	yes or no	• If this setting is 1, the agent is compatible with the Job Access with Speech (JAWS) screen reader. • If this setting is 0, the agent does not interact with the JAWS screen reader. **Note** Users may experience a slight impact on performance when this feature is enabled. The agent still functions normally if this feature is enabled on a client machine that does not have the JAWS screen reader installed. **Note** This setting does not apply to Mac OS X client machine agents.
Check signature?	no	yes or no	The Check signature setting looks for a digital signature that the agent uses to determine whether Windows can trust the executable before launching. For more information, see Adding, Duplicating, Editing, and Deleting a Launch Program Remediation, page 20-135. **Note** This setting does not apply to Mac OS X client machine agents.
Bypass summary screen?	yes	yes or no	If you are employing autoremediation for agent requirements, this setting enables you to make the agent session dialog more automated by skipping the agent posture assessment summary screen and proceeding directly to the first autoremediation function. Avoidance of this step reduces or eliminates user interaction during the agent login and remediation session. **Note** This setting does not apply to Mac OS X client machine agents.

Table 19-3 Manage Client-side MAC Address and Agent Discovery Host

Parameter	Default Value	Valid Range	Description or Behavior
MAC Exception list	—	Valid MAC address	If you specify one or more MAC addresses in this setting, the agent does not advertise those MAC addresses to Cisco ISE during login and authentication to help prevent sending unnecessary MAC addresses over the network. The text string that you specify must be a comma-separated list of MAC addresses including colons. For example: `AA:BB:CC:DD:EE:FF,11:22:33:44:55:66` **Note** This setting does not apply to Mac OS X client machine agents.
Discovery host	—	IP address or fully qualified domain name (FQDN)	This setting specifies the Discovery Host address or resolvable domain name that the agent uses to connect to Cisco ISE in a Layer 3 deployment.
Discovery host editable?	yes	yes or no	If this parameter is set to yes (the default value), then the user can specify a custom value in the Discovery Host field in the agent Properties dialog box. You can change this entry to no to ensure that the user cannot update the value in the Discovery Host field on the client machine. **Note** This setting does not apply to Mac OS X client machine agents.
Server name rules	—	FQDN	This parameter consists of comma-separated names of associated Cisco ISE nodes. The agent uses the names in this list to authorize Cisco ISE access points. If this list is empty, then the authorization is not performed. If any of the names are not found, then an error is reported. The server names should be FQDN names. The wildcard character (an asterisk [*]) can be used to specify Cisco ISE node names with similar characters. For example, ***.cisco.com** matches all the servers in the Cisco.com domain. **Note** This setting does not apply to Mac OS X client machine agents.
Generated MAC	—	Valid MAC address	This parameter supports Evolution-Data Optimized (EVDO) connections on the client machine. If the client machine does not have an active network interface card (NIC), the agent creates a dummy MAC address for the system. **Note** This setting does not apply to Mac OS X client machine agents.

Table 19-4 Specify Agent Localization Settings

Parameter	Default Value	Valid Range	Description or Behavior
Language Info	OS setting (“**default**”)	—	• If this setting is default, the agent uses the locale settings from the client operating system. • If this setting is either the ID, abbreviated name, or full name of a supported language, the agent automatically displays the appropriate localized text in agent dialogs on the client machine. **Note** This setting does not apply to Mac OS X client machine agents.

Language	ID	Abbreviated Name	Full Name
English US	1033	en	English
Catalan	1027	ca	Catalan (Spain)
ChineseSimplified	2052	zh_cn	Chinese (Simplified)
ChineseTraditional	1028	zh_tw	Chinese (Traditional)
Czech	1029	cs	Czech
Danish	1030	da	Danish
Dutch	1043	nl	Dutch (Standard)
Finnish	1035	fi	Finnish
French	1036	fr	French
FrenchCanadian	3084	fr-ca	French-Canadian
German	1031	de	German
Hungarian	1038	hu	Hungarian
Italian	1040	it	Italian
Japanese	1041	ja	Japanese
Korean	1042	ko	Korean (Extended Wansung)
Norwegian	1044	no	Norwegian
Portuguese	2070	pl	Portuguese
Russian	1049	ru	Russian
SerbianLatin	2074	sr	Serbian (Latin)
SerbianCyrillic	3098	src	Serbian (Cyrillic)
Spanish	1034	es	Spanish (Traditional)
Swedish	1053	sv	Swedish
Turkish	1055	tr	Turkish

Table 19-5 Report and Log Display Settings

Parameter	Default Value	Valid Range	Description or Behavior
Posture Report Filter	displayFailed	—	This parameter controls the level and type of results that appear to the user when the client machine undergoes posture assessment. • If this setting is displayAll, the client posture assessment report appears, displaying all results when the user clicks Show Details in the agent dialog. • If this setting is displayFailed, the client posture assessment report only displays remediation errors when the user clicks Show Details in the agent dialog. **Note** This setting does not apply to Mac OS X client machine agents.
Log file size in MB	5	0 and above	This setting specifies the file size (in megabytes) for agent log files on the client machine. • If this setting is 0, the agent does not record any login or operation information for the user session on the client machine. • If the administrator specifies any other integer, the agent records login and session information up to the number of megabytes that is specified.[1]

1. Agent log files are recorded and stored in a directory on the client machine. After the first agent login session, two files reside in this directory: one backup file from the previous login session, and one new file containing login and operation information from the current session. If the log file for the current agent session grows beyond the specified file size, the first segment of agent login and operation information automatically becomes the backup file in the directory, and the agent continues to record the latest entries in the current session file.

Table 19-6 Recurring Client Machine Connection Verification

Parameter	Default Value	Valid Range	Description or Behavior
Detect Retries	3	0 and above	If Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) polling fails, this setting configures the agent to retry *x* times before refreshing the client IP address.
Ping ARP	0	0-2	• If this value is set to 0, poll using ICMP. • If this value is set to 1, poll using ARP. • If this value is set to 2, poll using ICMP first, then (if ICMP fails) use ARP.
Max Timeout for Ping	1	1-10	Poll using ICMP, and if no response in *x* sec, then declare an ICMP polling failure.

Table 19-7 Additional SWISS Discovery Customization

Parameter	Default Value	Valid Range	Description or Behavior
Swiss timeout	1	1 and above	• If this setting is 1, the agent performs SWISS discovery as designed and no additional UDP response packet delay timeout value is introduced. • If the setting is an integer greater than 1, the agent waits the additional number of seconds for a SWISS UDP discovery response packet from Cisco ISE before sending another discovery packet. The agent takes this action to ensure that network latency is not delaying the response packet en route. **Note** SwissTimeout works only for UDP SWISS timeouts. **Note** This setting does not apply to Mac OS X client machine agents.
Disable L3 Swiss Delay?	no	yes or no	If this setting is yes, the agent disables its ability to increase the transmission interval for Layer 3 discovery packets. Therefore, the Layer 3 discovery packets repeatedly go out every 5 sec, just like Layer 2 packets. The default setting is no. **Note** This setting does not apply to Mac OS X client machine agents.

Table 19-8 HTTP Discovery Customization

Parameter	Default Value	Valid Range	Description or Behavior
Http discovery timeout	30	0, 3 and above	• Windows—Set by default at 30 sec, the Http discovery timeout is the time for which the HTTPS discovery from agent waits for the response from Cisco ISE. If there is no response for the specified time, then the discovery process times out. The valid range is 3 secs and above. Entering a value of 1 or 2 automatically sets the parameter value to 3. • Mac OS X—Cisco recommends setting this value to 5 secs for Mac OS X client machine agent profiles. If this value is set to 0, then default client machine operating system timeout settings are used.

Table 19-8 HTTP Discovery Customization (continued)

Parameter	Default Value	Valid Range	Description or Behavior
Http timeout	120	0, 3 and above	Set by default at 120 sec, the Http timeout is the time for which the HTTP request from the agent waits for a response. If there is no response for the specified time, the request times out. If there is no response for the specified time, then the discovery process times out. The valid range is 3 secs and above. Entering a value of 1 or 2 automatically sets the parameter value to 3. If this value is set to 0, then default client machine operating system timeout settings are used.

Table 19-9 Remediation Timeout Customization

Parameter	Default Value	Valid Range	Description or Behavior
Remediation timer	4	1-300	Specifies the number of minutes the user has to remediate any failed posture assessment checks on the client machine before having to go through the entire login process over again.
Network Transition Delay	3	2-30	Specifies the number of seconds the agent should wait for network transition (IP address change) before beginning the remediation timer countdown. **Note** When you use the "Enable agent IP refresh after VLAN change" option, Cisco ISE sends "DHCP release delay" and "DHCP renew delay" settings (as specified below) instead of using the "Network transition delay" setting used for Windows agent profiles. If you do not use the "Enable agent IP refresh after VLAN change" option, Cisco ISE sends "Network transition delay" timer settings to client machines, but Cisco ISE will not send *both*.

Table 19-10 Agent Dialog Behavior on User Logout or Shutdown

Parameter	Default Value	Valid Range	Description or Behavior
Enable auto close login screen?	no	yes or no	Allows you to determine whether or not the agent login dialog into which the client machine user enters their login credentials closes automatically following authentication.
Auto close login screen after <*x*> sec	0	0-300	Specifies the number of seconds the agent waits to automatically close following user credential authentication on the client machine.

Note When there are no agent profiles configured to match client provisioning policies, you can use the settings specified in the **Administration > System > Settings > Posture > General Settings** page to perform the same functions. See Posture General Settings, page 20-10 for more information.

Table 19-11 IP Address Behavior Settings for Client Machines

Parameter	Default Value	Valid Range	Description or Behavior
Enable agent IP refresh after VLAN change?	no	yes or no	**Caution** Cisco does not recommend enabling this option for Windows client machines accessing the network via native Windows, Cisco Secure Services Client, or AnyConnect supplicants. Specify whether or not the client machine should renew its IP address after the switch or WLC changes the VLAN for the login session of the client on the respective switch port. Check the "Enable agent IP refresh after VLAN change" parameter to refresh Windows client IP address in both wired and wireless environments for MAB with posture. To ensure the Mac OS X client IP address is refreshed when the assigned VLAN changes, this parameter is required for Mac OS X client machines accessing the network via the native Mac OS X supplicant in both wired and wireless environments. **Note** When you use the "Enable agent IP refresh after VLAN change" option, Cisco ISE sends "DHCP release delay" and "DHCP renew delay" settings (as specified below) instead of using the "Network transition delay" setting used for Windows agent profiles. If you do not use the "Enable agent IP refresh after VLAN change" option, Cisco ISE sends "Network transition delay" timer settings to client machines, but Cisco ISE will not send *both*.
DHCP renew delay	0	0-60	The number of seconds the client machine waits before attempting to request a new IP address from the network DHCP server.
DHCP release delay	0	0-60	The number of seconds the client machine waits before releasing its current IP address.

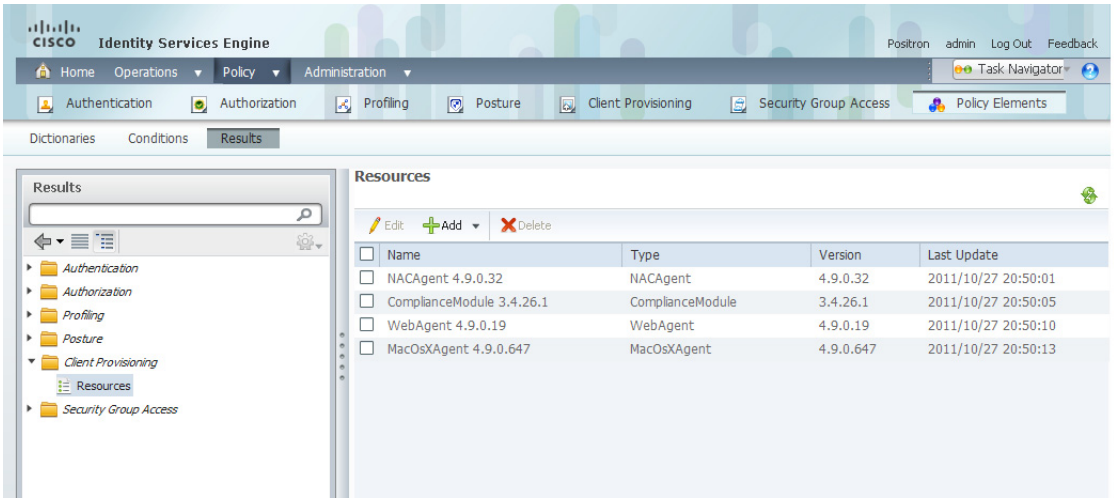
Deleting Client Provisioning Resources

Caution Before you delete an existing resource from Cisco ISE, ensure that none of your client provisioning resource policies requires that resource.

To remove an existing client provisioning resource from Cisco ISE, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

Figure 19-7 Policy > Policy Elements > Results > Client Provisioning > Resources



Step 2 Select one or more existing resources from the client provisioning resources list, and click **Delete**.

Step 3 Confirm that you want to remove the specified resource (or resources) in the confirmation pop-up that appears. The resources that you specify no longer appear in the client provisioning resources list.

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

Provisioning Client Machines with the Cisco NAC Agent MSI Installer

Cisco provides an MSI (Microsoft Installer format) installer for the Cisco NAC Agent (called **nacagentsetup-win.msi**) on Windows client machines. There is also a zip version of the same installer package that uses up less local memory on file transfer. You can download the MSI and/or zip package from the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml. When you have obtained the Cisco NAC Agent MSI or zip package, you can place the MSI installer in a

directory on the client machine along with an Agent configuration XML file (named **NACAgentCFG.xml**) containing the appropriate Agent profile information required to coincide with your network.

Step 1 Download the **nacagentsetup-win.msi** or **nacagentsetup-win.zip** installer file from the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml.

Step 2 Place the **nacagentsetup-win.msi** file in a specific directory on the client machine (for example, C:\temp\nacagentsetup-win.msi):

- If you are copying the MSI installer directly over to the client, place the **nacagentsetup-win.msi** file into a directory on the client machine from which you plan to install the Cisco NAC Agent.
- If you are using the **nacagentsetup-win.zip** installer, extract the contents of the zip file into the directory on the client machine from which you plan to install the Cisco NAC Agent.

Step 3 Place an Agent configuration XML file in the same directory as the Cisco NAC Agent MSI package. For information on the Agent configuration XML file and its parameters and syntax, see Creating Windows Agent Profiles in Cisco ISE, page 19-12, and Example XML File Generated Using the Create Profile Function, page 19-14.

If you are not connected to ISE, you can copy the **NACAgentCFG.xml** file from a client that has already been successfully provisioned. The file is located at **C:\Program Files\Cisco\Cisco NAC Agent\NACAgentCFG.xml.**

As long as the Agent configuration XML file exists in the same directory as the MSI installer package, the installation process automatically places the Agent configuration XML file in the appropriate Cisco NAC Agent application directory so that the Agent can point to the correct Layer 3 network location when it is first launched.

Note The Discovery Host field can be made editable or not by changing the DiscoveryHostEditable parameter in the Agent configuration XML file. See Agent Profile Parameters and Applicable Values, page 19-16, for more details.

Step 4 Open a Command prompt on the client machine and enter the following to execute the installation:

```
msiexec.exe /i NACAgentSetup-win.msi /qn /l*v c:\temp\agent-install.log
```

Note The `/qn` qualifier installs the Cisco NAC Agent completely silently. The `/l*v` logs the installation session in verbose mode.

The Cisco NAC Agent is installed on the client machine and automatically launches in the background using the Discovery Host supplied in the Agent configuration XML file to contact the Cisco ISE network.

If you are using Altiris/SMS to distribute the MSI installer, perform the following to enforce Agent Customization:

- Place the Agent customization files in a sub-directory named “brand” in the directory “%TEMP%/CCAA”.
- When the Cisco NAC Agent is installed in the client, the customization is applied to the Agent.
- To remove the customization, send a plain MSI without the customization files.

Setting Up Global Client Provisioning Functions

- Enabling and Disabling the Client Provisioning Service, page 19-26
- Downloading Client Provisioning Resources Automatically, page 19-27

Enabling and Disabling the Client Provisioning Service

Prerequisites

To ensure you are able to access the appropriate remote location from which you can download client provisioning resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network as described in Specifying Proxy Settings in Cisco ISE, page 8-17.

To configure Cisco ISE to automatically discover and download client provisioning resources, complete the following steps:

Step 1 Choose **Administration > System > Settings > Client Provisioning**.

Figure 19-8 Administration > System > Settings > Client Provisioning



Step 2 Click the **Enable Provisioning** drop-down menu and choose **Enable** or **Disable**.

Step 3 Click **OK**.

When you choose to disable this function of Cisco ISE, users who attempt to access the network will receive a warning message indicating that they are not able to download client provisioning resources.

Next Steps

Set up system-wide client provisioning functions according to the guidelines in:

- Adding and Removing Agents and Other Resources, page 19-4

- Configuring Client Provisioning Resource Policies, page 19-28

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

Downloading Client Provisioning Resources Automatically

Note Cisco recommends that you manually upload resources whenever possible according to the guidelines in Adding Client Provisioning Resources to Cisco ISE, page 19-5, rather than opting to upload them automatically. This function automatically uploads *all* available software from Cisco, many items of which may not be pertinent to your deployment.

Prerequisites

To ensure you are able to access the appropriate remote location from which you can download client provisioning resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network as described in Specifying Proxy Settings in Cisco ISE, page 8-17.

To configure Cisco ISE to automatically discover and download all known available client provisioning resources, complete the following steps:

Step 1 Choose **Administration > System > Settings > Client Provisioning**.

Figure 19-9 Administration > System > Settings > Client Provisioning



Step 2 Click the **Enable Automatic Download** drop-down menu and choose **Enable**.

Step 3 When enabling automatic downloads, be sure to specify the URL where Cisco ISE searches for system updates in the Update Feed URL field. The default URL for downloading client provisioning resources is https://www.cisco.com/web/secure/pmbu/provisioning-update.xml.

If you choose not to use the **Enable Automatic Download** function, you can manually download the client provisioning resource files to a local system before importing them into Cisco ISE via the guidelines described in Adding Client Provisioning Resources from a Local Machine, page 19-6.

Step 4 Click **Save**. Cisco ISE automatically checks for updated resources every 24 hours, based on the time Cisco ISE was first installed.

Next Steps

Set up system-wide client provisioning functions according to the guidelines in:

- Adding and Removing Agents and Other Resources, page 19-4
- Configuring Client Provisioning Resource Policies, page 19-28

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

Configuring Client Provisioning Resource Policies

Client provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and/or agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

When you download the agent compliance module, it always overwrites the exisiting one, if any, available in the system.

Prerequisites

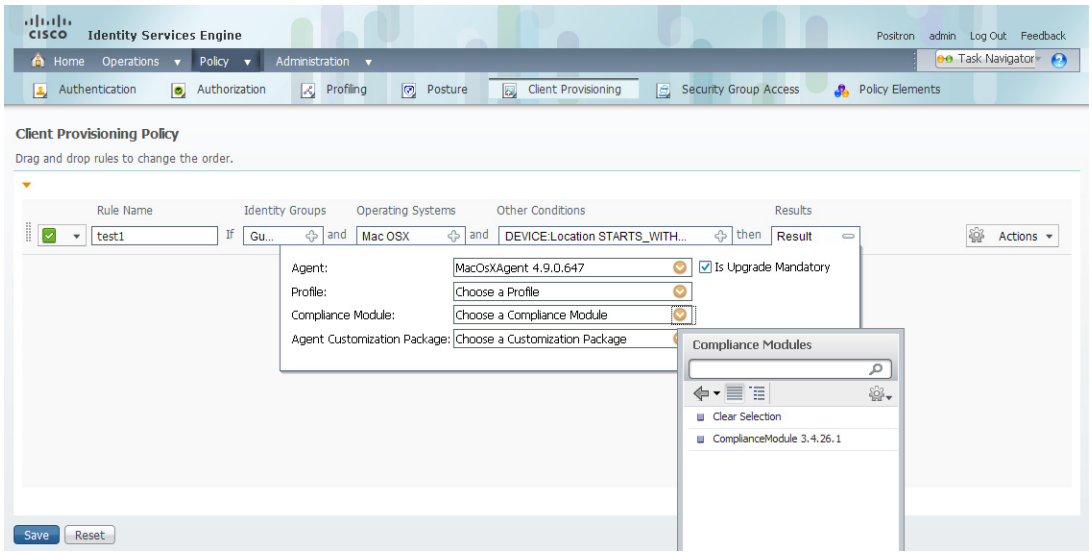
Before you can create effective client provisioning resource policies, ensure that you have set up system-wide client provisioning functions according to the following topics:

- Specifying Proxy Settings in Cisco ISE, page 8-17.
- Setting Up Global Client Provisioning Functions, page 19-26
- Adding and Removing Agents and Other Resources, page 19-4

To configure a client provisioning resource policy, complete the following steps:

Step 1 Choose **Policy > Client Provisioning**.

Figure 19-10 Policy > Client Provisioning



Enable or Disable the Resource Policy

Step 2 Select the **Enable**, **Disable**, or **Monitor** option from the behavior drop-down menu on the left side of the client provisioning policy configuration window:

- **Enable**—Ensures Cisco ISE uses this policy to help fulfill client provisioning functions when users log in to the network and conform to the client provisioning policy guidelines.
- **Disable**—Cisco ISE does not use the specified resource policy to fulfill client provisioning functions.
- **Monitor**—Disables the policy and "watches" the client provisioning session requests to see how many times Cisco ISE tries to invoke based on the "Monitored" policy.

Define the Resource Policy

Step 3 Enter a name for the new resource policy in the Rule Name field.

Categorize the Client Machine

Step 4 Specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.

You can choose to specify the *Any* identity group type, or choose one or more groups from a list of existing Identity Groups you have configured (for example, "Guest," sponsor-created, or administrator-created groups) at Configuring User Identity Groups, page 4-40.

Step 5 Use the Operating System field to specify one or more operating systems that might be running on the client machine through which the user is logging into Cisco ISE.

You can choose to specify a single operating system like "Mac OS X," or an umbrella operating system designation that addresses a number of client machine operating systems like "Windows XP (All)" or "Windows 7 (All)." For a complete list of supported client machine operating systems, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

Step 6 In the Other Conditions portion of the client provisioning resource policy, specify a new expression you want to create for this particular resource policy. When you develop a new condition for this resource policy, specify the components of the new expression for this resource policy per the guidelines outlined in Dictionary and Attribute User Interface, page 7-2.

Define Which Resources to Distribute

Step 7 Specify which agent type, compliance module, customization package, and/or profile to make available and provision on the client machine based on the categorization defined above.

a. Specify whether the agent upgrade (download) defined here is mandatory for the client machine by enabling or disabling the **Is Upgrade Mandatory** option, as appropriate.

Note The Is Upgrade Mandatory setting only applies to agent downloads. Agent profile, compliance module, and customization package updates are always mandatory.

b. Choose an available agent from the Agent drop-down list.

c. Choose an existing agent profile from the Profile drop-down list.

d. Choose an available agent compliance module to download to the client machine using the Compliance Module drop-down list.

Note You can also use the policy configuration process to download agent resources "on the fly" for the three resource types above by clicking the gear-shaped widget and selecting **Download Resource** or **Upload Resource** from the resulting pop-up menu. This method takes you to the Downloaded Remote Resources or Manual Resource Upload dialog box, respectively, where you can download one or more resources to Cisco ISE as described in Adding Client Provisioning Resources to Cisco ISE, page 19-5.

e. Choose an available agent customization package for the client machine from the Agent Customization Package drop-down list.

Step 8 Click **Save**.

Next Steps

Once you have successfully configured one or more client provisioning resource policies, you can start to configure Cisco ISE to perform posture assessment on client machines during login according to the topics in Chapter 20, "Configuring Client Posture Policies."

Client-side Installation and Log-In

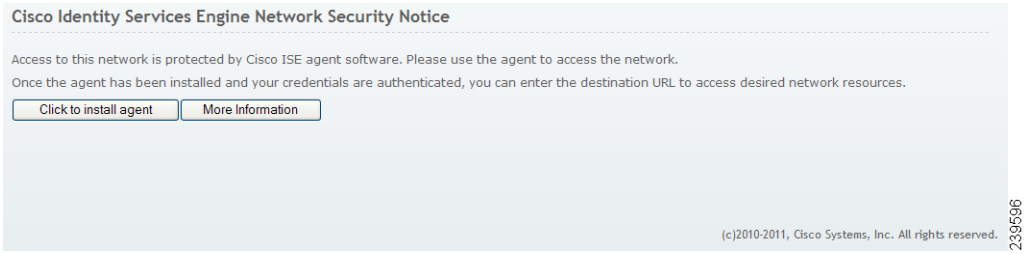
When users first log into a network that is managed by Cisco ISE and requires access via an agent, they are prompted to install temporal or persistent agents (as well as possible associated client provisioning resources) on the client machine to facilitate network access, client posture assessment, and other Cisco ISE network services.

To download agents and other client provisioning resources, users must have administrator privileges on their client machines and the browser session through which they are attempting to log into Cisco ISE. In addition, to successfully install the agent, users will likely need to explicitly accept ActiveX or Java applet installer functions.

Once the browser session from that client machine reaches the specified access portal, Cisco ISE prompts the user to download and install a persistent agent (like the Cisco NAC Agent or Mac OS X Agent) or temporal agent (like the Cisco NAC Web Agent).

Figure 19-11 shows a Cisco ISE welcome screen, prompting the user to download and install the Cisco NAC Agent on the client machine.

Figure 19-11 Cisco ISE Agent Download and Installation

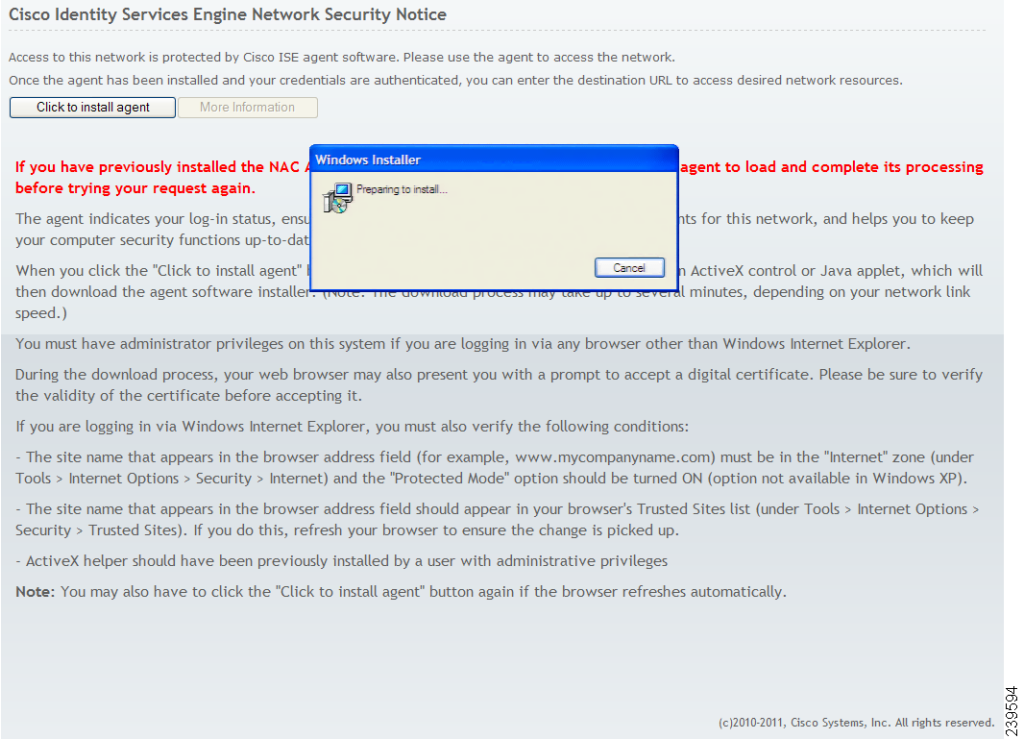


Note During Cisco ISE hardware and software installation, you can test network connectivity from remote client machines. You can perform this test by launching a browser window on a test client machine that is connected to the user access part of your Cisco ISE network and navigating to a dummy IP address like https://1.1.1.1. For detailed information on testing Cisco ISE installation, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

Once the user validates and accepts any certificate (or certificates) required to facilitate agent download and installation on the client machine, the ActiveX or Java applet installer process launches and provisions the agent installation package on the client machine.

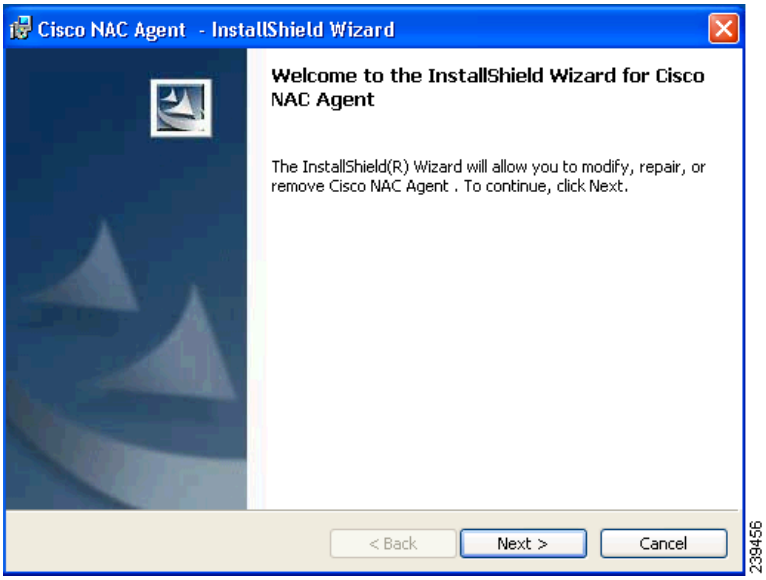
Figure 19-12 shows an example of the user Cisco ISE browser session when the agent installation files have been downloaded, and the installer is preparing to install the Cisco NAC Agent application files on the client machine.

Figure 19-12 Preparing to Install Cisco NAC Agent



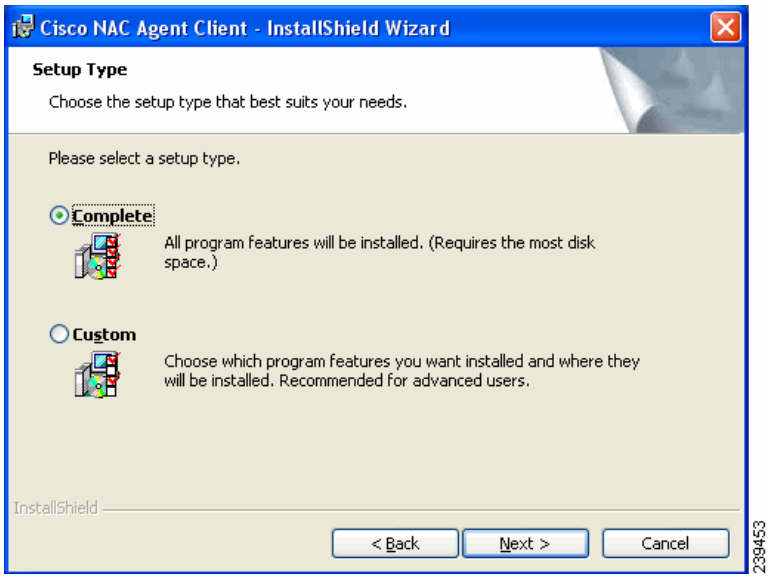
The agent **InstallShield Wizard** dialog appears (Figure 19-13).

Figure 19-13 Cisco NAC Agent InstallShield Wizard—Welcome



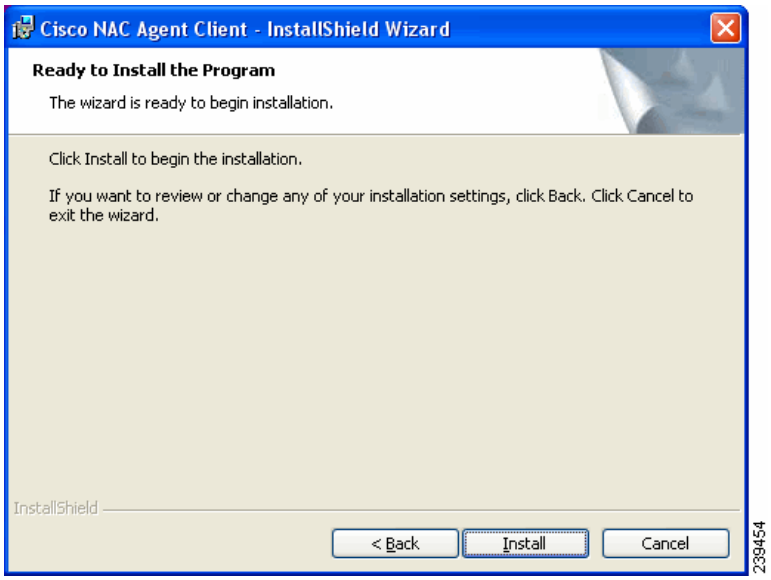
The user has the option to install the complete collection of agent files or specify one or more items by choosing the **Custom** option and clicking **Next** (Figure 19-14).

Figure 19-14 Cisco NAC Agent Installation—Setup Type



The agent **InstallShield Wizard** dialog appears (Figure 19-15).

Figure 19-15 Cisco NAC Agent InstallShield Wizard—Ready to Install



The setup wizard prompts the user through the short installation steps to install the agent to the **C:\Program Files\Cisco\Cisco NAC Agent** directory on the client machine.

Figure 19-16 Cisco NAC Agent Installation In Progress

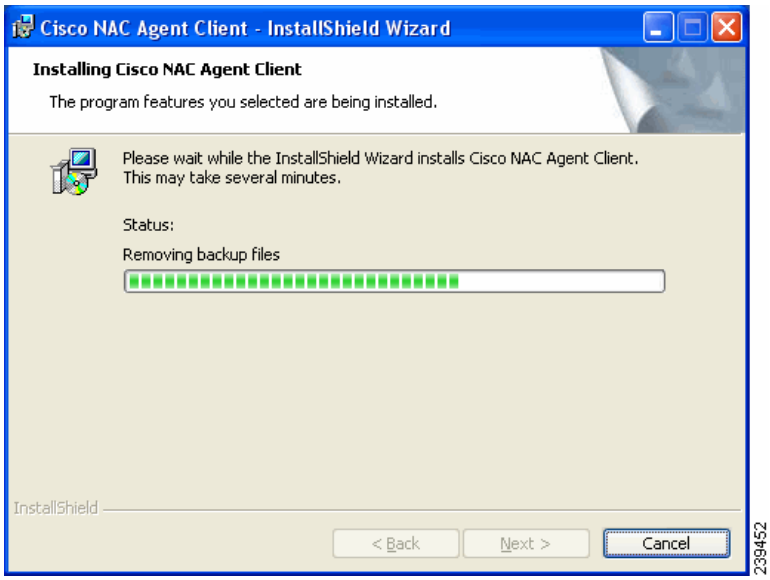
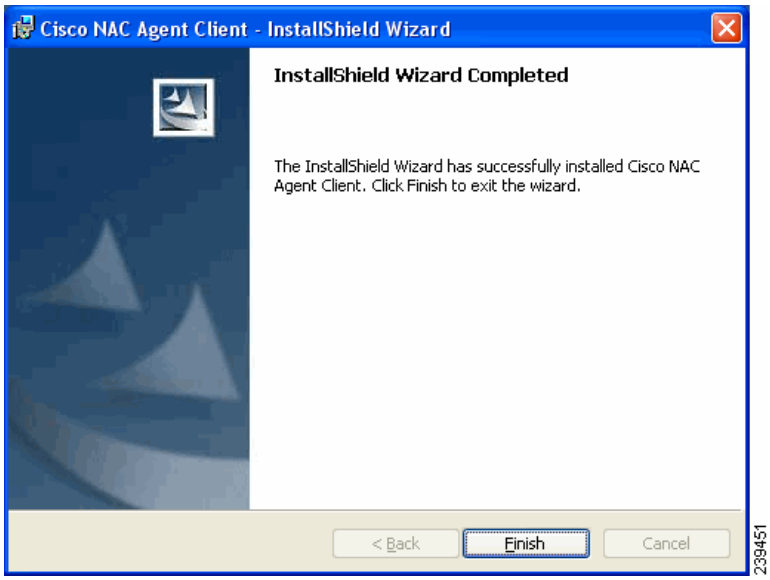


Figure 19-17 Cisco NAC Agent Installation Complete



When the InstallShield Wizard completes and the user clicks **Finish**, the agent automatically transmits the native operating system login credentials of the user to Cisco ISE for authentication and access to the internal network.

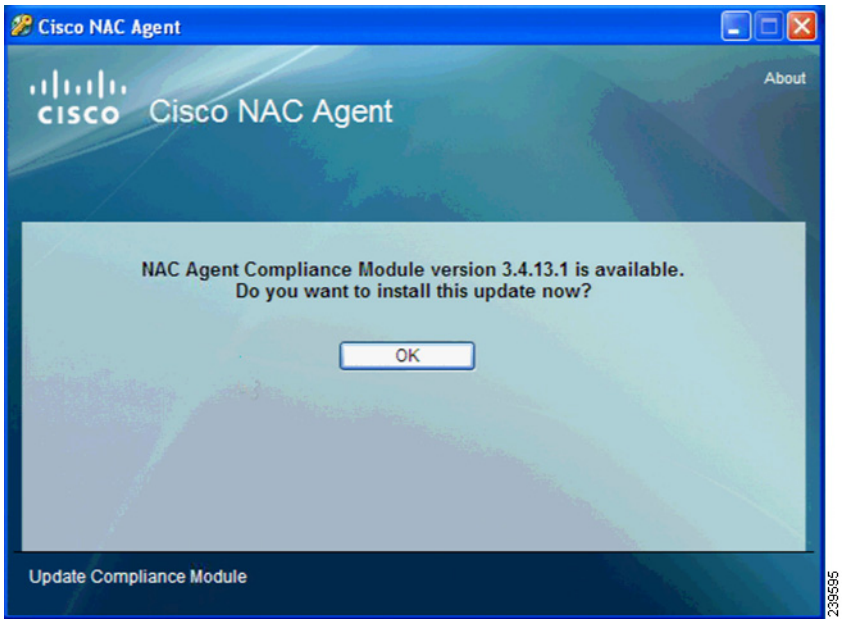
Note The server certificate on the client helps ensure the client machine can perform DNS resolution, allowing services like Cisco ISE client provisioning and posture assessment. If you change the Cisco ISE domain name (by logging into the Cisco ISE CLI and manually specifying a new domain name, for example), you must generate a new server certificate to reflect the same domain name change.

If you have associated any posture assessment or profiling policies with the user role to which the user in question is assigned, those services initiate at this time. Users accessing the network via Cisco ISE (except for registered "guests") must also agree to the Acceptable Use Policy each time they log in. Additionally, these other client provisioning resources that you may have specified for the user role are now downloaded to the client machine to help facilitate network access:

- Agent profiles
- Agent compliance modules
- Agent customization packages

Figure 19-18 displays an example of an agent compliance module update (which is always mandatory) at the time of agent installation on the client machine.

Figure 19-18 Cisco NAC Agent—Updating Agent Compliance Module

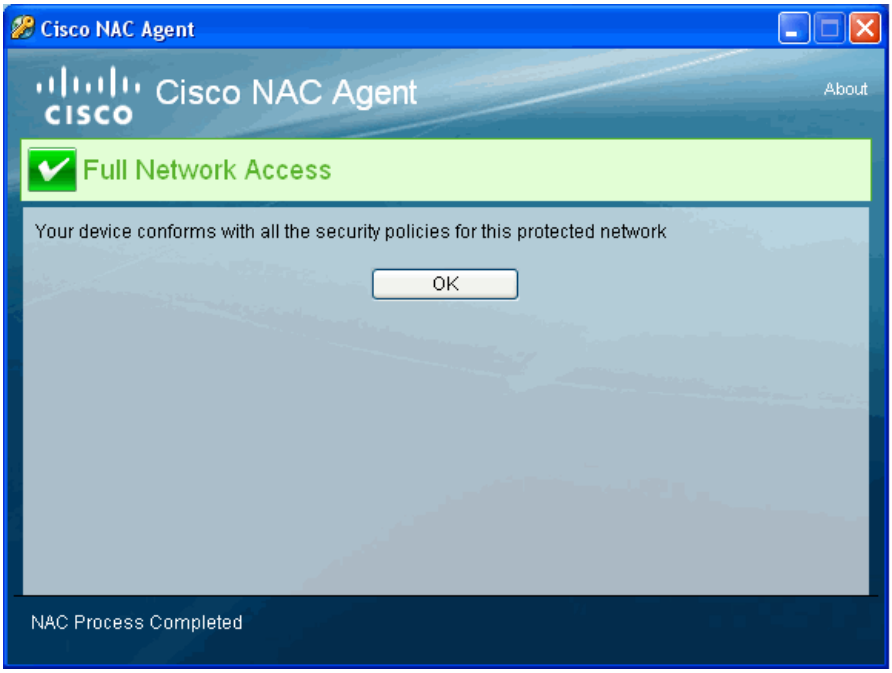


If you have not enabled the Is Upgrade Mandatory setting in the client provisioning resource policy, then the agent upgrade dialog would display a Cancel button as well as the **OK** button. This allows end users the option to cancel an agent upgrade if a more current version is available.

For details, see Configuring Client Provisioning Resource Policies, page 19-28.

Following successful agent installation, client posture assessment, and remediation, the agent notifies the user that their login session is complete and they are granted access to the network based on the assigned user role.

Note If the agent is not able to reach the primary Discovery Host address configured in the associated client provisioning policy (after attempting to connect per the number of retries configured in the agent profile), the agent automatically tries the Discovery Host address received from the access switch via URL redirection to successfully connect to the network.



Viewing Client Provisioning Reports and Events

- Viewing Client Provisioning Reports in Cisco ISE, page 19-36
- Viewing Client Provisioning Event Logs in Cisco ISE, page 19-40

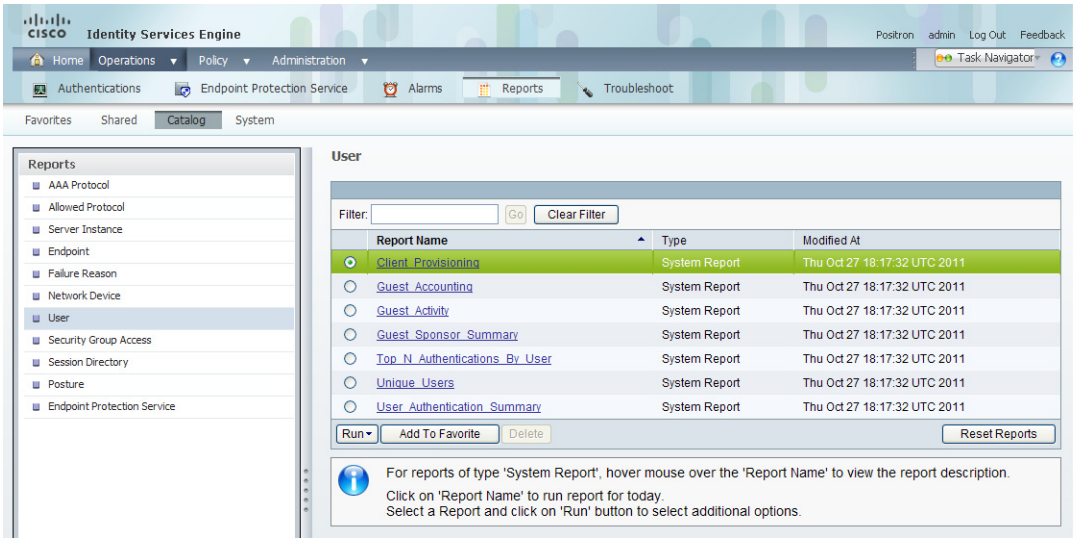
Viewing Client Provisioning Reports in Cisco ISE

As a network administrator, you may need to access the Cisco ISE monitoring and troubleshooting functions to check on overall trends for successful or unsuccessful user login sessions, gather statistics about the number and types of client machines logging into the network during a specified time period, or check on any recent configuration changes in client provisioning resources.

The following examples provide a couple of common scenarios, however you should see Chapter 23, "Monitoring and Troubleshooting" for more details on using the Cisco ISE monitoring and troubleshooting capabilities to maximize the tools within your network deployment.

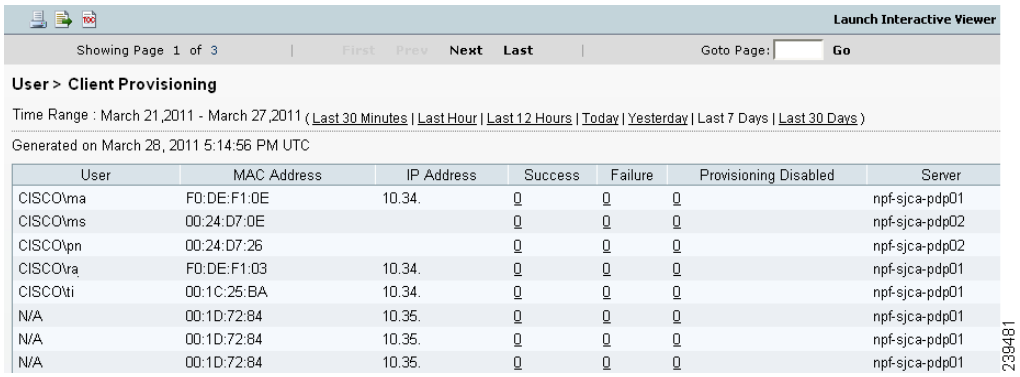
The **Operations > Reports > Catalog > User > Client Provisioning** window displays statistics about successful and unsuccessful client provisioning requests (Figure 19-19).

Figure 19-19 Operations > Reports > Catalog > User > Client Provisioning



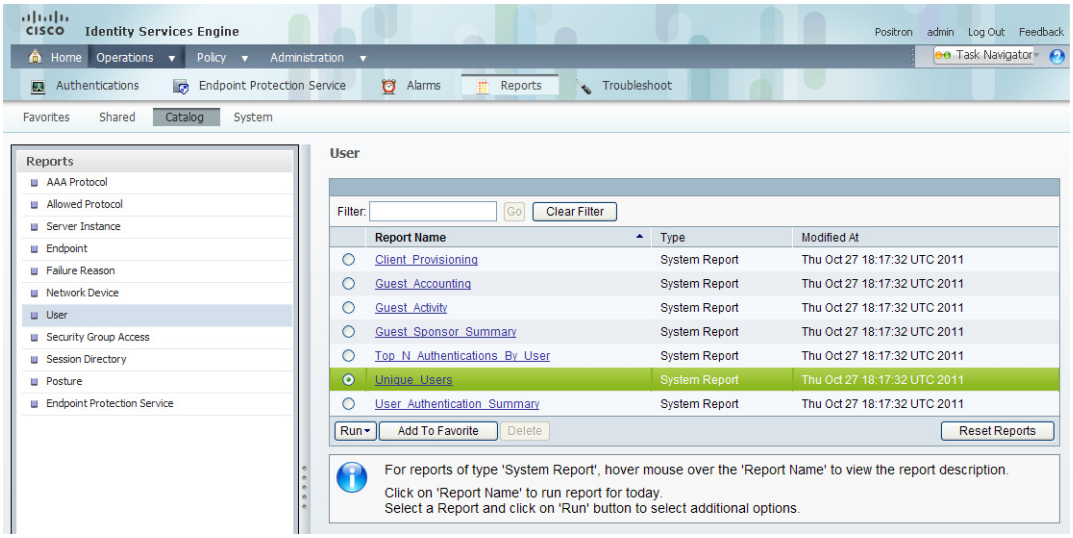
When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client provisioning data (Figure 19-20).

Figure 19-20 Client Provisioning Report Results



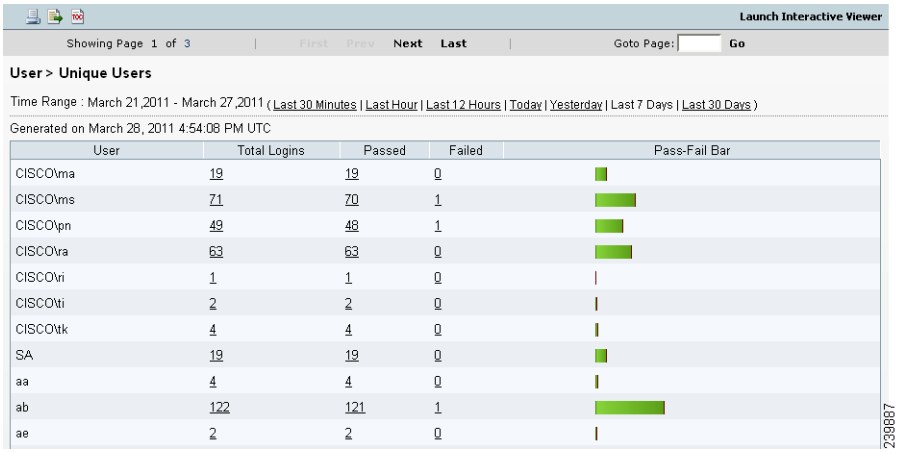
The **Operations > Reports > Catalog > User > Unique Users** window displays statistics about known specific client access sessions initiated during the specified time period (Figure 19-21).

Figure 19-21 Operations > Reports > Catalog > User > Unique Users



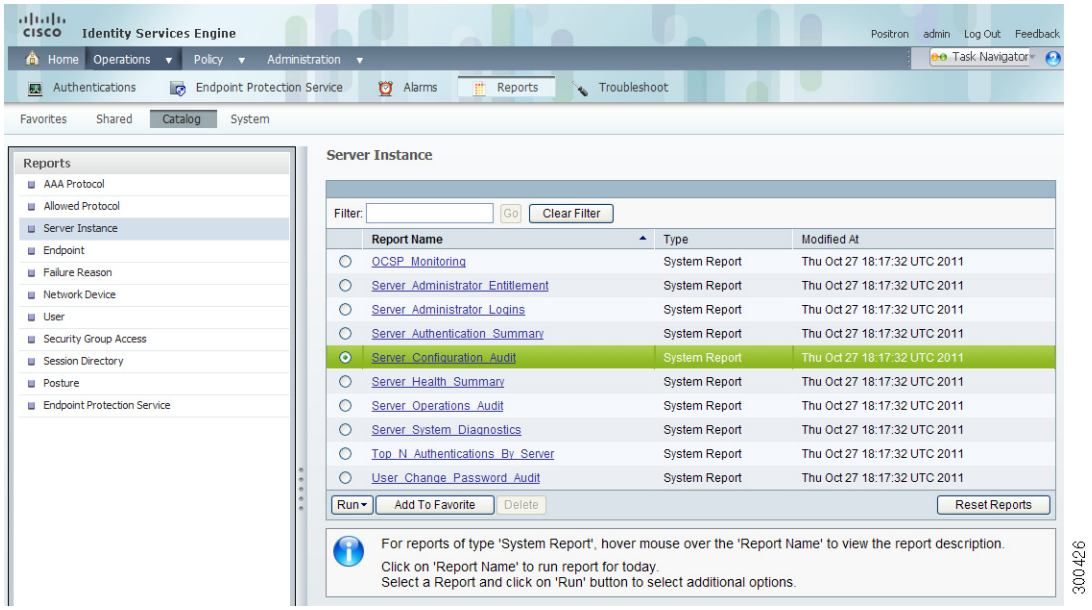
When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client provisioning data (Figure 19-22).

Figure 19-22 Unique Users Report Results



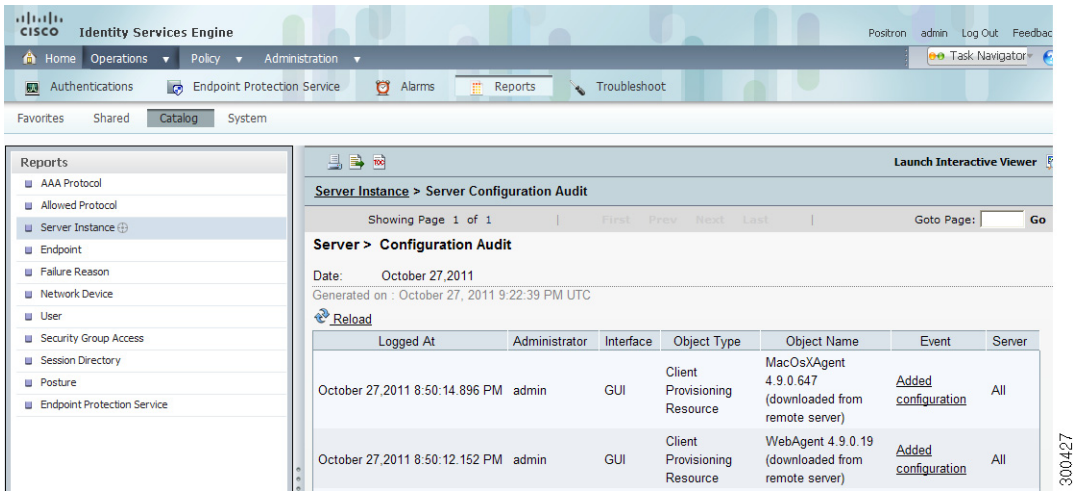
The **Operations > Reports > Catalog > Server Instance > Server Configuration Audit** window displays information about recent client provisioning resource configuration changes (Figure 19-23).

Figure 19-23 Operations > Reports > Catalog > Server Instance > Server Configuration Audit



Choosing Run and specifying one of the preset time periods displays any configuration changes to client provisioning resources in Cisco ISE (for example, a newly uploaded agent version) within the time period specified (Figure 19-24).

Figure 19-24 Server Configuration Audit Report Results

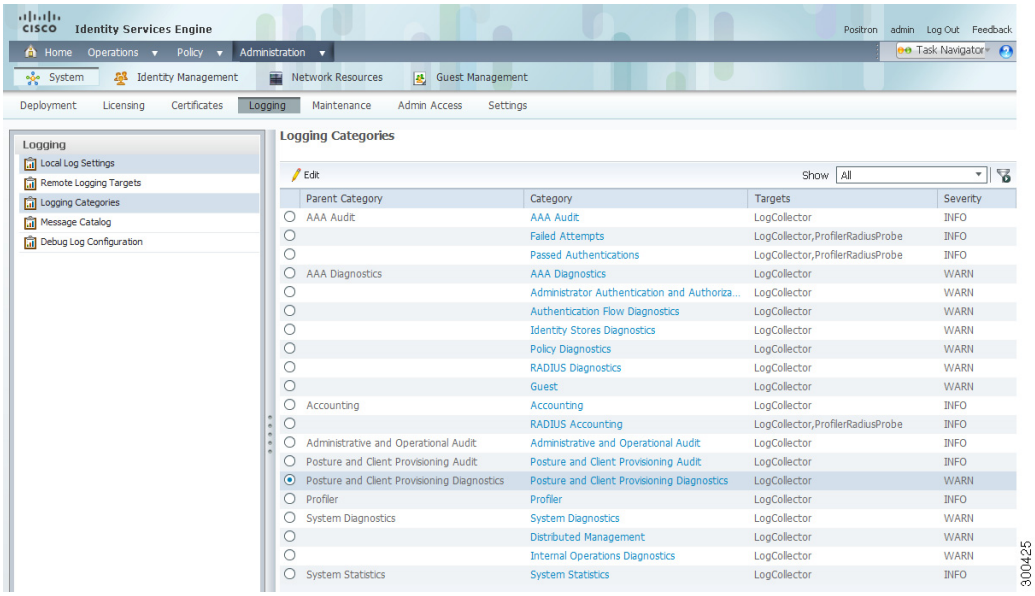


Viewing Client Provisioning Event Logs in Cisco ISE

During Cisco ISE operation, you may need to search event log entries in order to help diagnose a possible problem with client login behavior. For example, you may need to determine the source of an issue where client machines on your network are not able to get client provisioning resource updates upon login.

You can compile and view logging entries for Client Provisioning and Posture audit messages as well as diagnostics. See Chapter 14, "Logging" for more specific information on using the Cisco ISE log compilation capabilities to maximize the tools within your network deployment.

Figure 19-25 Administration > System > Logging > Logging Categories > Posture and Client Provisioning Diagnostics





CHAPTER 20

Configuring Client Posture Policies

This chapter describes the posture service in the Cisco Identity Services Engine (Cisco ISE) appliance that allows you to check the state (posture) for all the endpoints that are connecting to your Cisco ISE enabled network with your corporate security policies for compliance before clients access protected areas of your network.

This chapter guides you through the features of the Cisco ISE posture service in detail.

- Posture Service, page 20-2
  - Understanding the Posture Service, page 20-3
  - Posture Compliance Dashlet, page 20-8
  - Viewing Posture Reports, page 20-8
- Posture Administration Settings in Cisco ISE, page 20-9
  - Posture General Settings, page 20-10
  - Posture Reassessments, page 20-12
  - Posture Updates, page 20-22
  - Posture Acceptable Use Policy, page 20-24
- Client Posture Assessments in Cisco ISE, page 20-32
  - Client Posture Assessment Policies, page 20-33
  - Simplified Posture Policy Configuration, page 20-34
- Posture Assessment and Remediation Options in Cisco ISE, page 20-41
- Custom Conditions for Posture, page 20-42
- Posture Results, page 20-111
  - Custom Posture Remediation Actions, page 20-112
  - Client Posture Assessment Requirements, page 20-155
- Custom Authorization Policies for Posture, page 20-162
- Custom Permissions for Posture, page 20-167

Posture Service

The Network Admission Control (NAC) Agents that are installed on the clients interact with the posture service to enforce security policies on all the endpoints that attempt to gain access to your protected network. At the same time, the NAC Agents enforce security policies on noncompliant endpoints by blocking network access to your protected network. They assist you in evaluating clients against posture policies, and as well as enforce clients to meet requirements that are required for compliance with your organization's security policies.

The posture service checks the state (posture) of the clients for compliance with your corporate security policies before the client gains the privileged network access. The Client Provisioning service ensures that the clients are setup with appropriate Agents that provide posture assessment and remediation for the clients.

The NAC Agent for ISE does not support Windows Fast User Switching when using the Native Supplicant. This is because there is no clear disconnect of the older user. When a new user is sent, the Agent is hung on the old user process and session ID, and hence a new posture cannot take place. As per the Microsoft Security policies, it is recommended to disable Fast User Switching.

For information on the posture service in detail, see the "Understanding the Posture Service" section on page 20-3.

For information on Posture Compliance dashlet, see the "Posture Compliance Dashlet" section on page 20-8.

For information on posture reports, see the "Viewing Posture Reports" section on page 20-8.

SWISS Protocol

The SWISS protocol is a stateless request response protocol that allows NAC Agents which are running on managed clients to discover the Cisco ISE server, and retrieve configuration and operational information. The NAC Agent connects to the Cisco ISE server by sending SWISS unicast discovery packets out on User Datagram Protocol (UDP) port 8905 until a Cisco ISE node that assumes the Policy Service persona sends a response to the client. The SWISS protocol uses TCP transport for all the messages and UDP transport for periodical requests. The NAC Agent tunnels all the SWISS requests over HTTPS and pings the Cisco ISE SWISS UDP server for changes to its authentication and posture state.

The SWISS request message that comes from the client machine includes information pertaining to resource types for the following items:

- Agent profiles
- Agent compliance modules
- Agent customization package

In addition to answering the above request items, the SWISS response from the Cisco ISE server can also contain prompts to update the current Agent and URL or URLs that are required to perform posture assessment and remediation on the client machine.

For descriptions of the various types of agents available in Cisco ISE, see Cisco ISE Agents, page 19-1.

Understanding the Posture Service

Cisco ISE posture service primarily includes the posture administration services and the posture run-time services. If you do not have the advanced license package installed on your Cisco ISE deployment, then the posture administration services user interface will not be available for you to use in Cisco ISE.

Posture Administration Services

The administration services provide the back-end support for posture specific custom conditions, and remediation actions that are associated to the requirements and authorization policies that are configured for posture service on your Cisco ISE deployment.

Posture Run-time Services

The posture run-time services encapsulates the SWISS protocol services, and all the interactions that happen between the NAC Agents and the Cisco ISE server for posture assessment and remediation of clients.

Validating a Posture Requirement Request

Once the client (an endpoint) is authenticated on the network, the client can be granted limited access on the network. For example, the client can access remediation-only resources on the network. The NAC Agent that is installed on the client validates the requirements for an endpoint and the endpoint is moved to a compliant state upon successful validation of the requirements. If the endpoint satisfies the requirement, a compliance report will be sent to the Cisco ISE node that assumes the Policy Service persona and the run-time services triggers a Change of Authorization (CoA) for the posture compliant status. If the endpoint fails to satisfy the requirement, a noncompliance report will be sent to the Cisco ISE node that assumes the Policy Service persona and the run-time services triggers a CoA for the posture noncompliant status.

Now, the Agent gets its session ID from the redirect URL and sends it along with its MAC address and IP address in a SWISS request. The posture run-time services looks up in the session cache using the session ID first, MAC address, and then the IP address, if required. If the posture run-time services finds the same session using the session ID in the session cache, then it queries the posture policies in Cisco ISE and tries to match the posture policies. Once matched, it generates the specified XML format that contains the matched requirements and sends to the NAC Agents. The NAC Agents send the posture report to the posture run-time services.

Generating a Posture Requirement

The run-time services requests for the posture requirement for the endpoint by looking up at the role to which the user belongs to and the operating system on the client. If you do not have a policy associated with the role, then the run-time services communicate to the NAC Agent with an empty requirement. If you have a policy associated with the role, then the run-time services run through the posture policies through one or more requirements associated with the policies and for each requirement through one or more conditions. Once the posture policy is retrieved for the endpoint, the posture run-time services communicate the requirement to the NAC Agent in a specified XML format.

Processing the Posture Report from the Cisco NAC Agent

The NAC Agent validates the endpoint for compliance based on the requirements that are sent from the Cisco ISE server and determines the posture of the endpoint. If the endpoint is not compliant with the requirement, then the NAC Agent prompts to remediate the endpoint for compliance. Any failures during posture evaluation results in the noncompliance of the endpoint. The NAC Agent sends the appropriate compliance report to the Cisco ISE server once postured compliant or noncompliant.

Issuing a CoA Based on the Posture Report Evaluation

Upon evaluating the posture report received from the NAC Agent, an endpoint may be identified as compliant or noncompliant. If the endpoint is compliant or noncompliant, then the posture run-time services triggers a CoA for that endpoint session. Based on the profile configured for compliant or noncompliant, the end user gets the appropriate level of access privileges to the network.

Logging

Upon processing the posture request and report, the run-time services sends audit log messages to the Cisco ISE node that assumes the Monitoring persona.

For information on how posture and client provisioning session services work in Cisco ISE, see the "Posture and Client Provisioning Services" section on page 20-4.

For information on licenses for the posture service, see the "Licenses for the Posture Service" section on page 20-5.

For information on how to deploy the posture service in detail, see the "Deploying the Posture Service" section on page 20-6.

Posture and Client Provisioning Services

Prerequisites:

Before you begin, you should have an understanding of the available client provisioning resources in Cisco ISE that you can configure for the clients.

For information on how to configure client provisioning resource policies, see the "Configuring Client Provisioning Resource Policies" section on page 19-28.

Before you begin, you should have an understanding of the Client Provisioning session service in Cisco ISE. Cisco ISE manage client provisioning resources for your clients and uses the client provisioning resource policies to ensure that the client systems are set up with an appropriate Agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles.

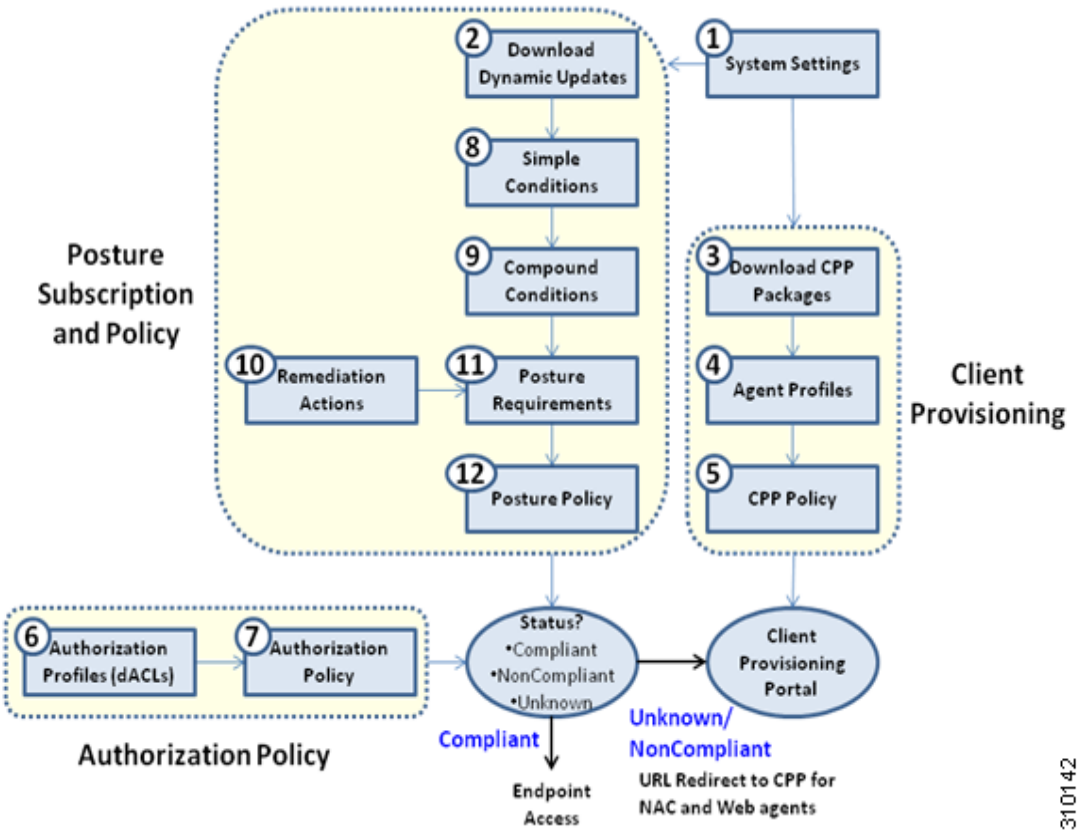
For information on the Client Provisioning session service, see Chapter 19, "Configuring Client Provisioning Policies."

For information on the NAC Agent that is installed on the client and the client operating system compatibility, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

Posture and Client Provisioning Policies Flow

Figure 20-1 shows the flow of posture and client provisioning policies in Cisco ISE posture service.

Figure 20-1 Posture and Client Provisioning Policies Workflow in Cisco ISE



Licenses for the Posture Service

Prerequisites:

Before you begin, you should have an understanding on how licenses restrict the usage of Cisco ISE posture service with both the base and advanced license packages.

For more information on Cisco ISE license packages, refer to the Performing Post Installation Tasks chapter in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

Cisco ISE allows you to configure the posture service to run on multiple Cisco ISE nodes in a distributed deployment. You can also configure the posture service on a single node in a standalone Cisco ISE deployment.

Cisco ISE deployment provides you with two main types of licenses, namely the base license and advanced license. You also have an evaluation license which, if further use is desired, needs to be upgraded to the appropriate base or advanced license once the evaluation license period is over.

In addition, if you do not have the advanced license installed on your primary administration node, then the SWISS server does not get initialized during run time. If the SWISS server does not initialize, then the posture requests will not be served in Cisco ISE. If the advanced license is not installed in Cisco ISE,

then the posture service menus on the Cisco ISE administration user interface will be removed except the default posture status configuration for unsupported operating system on the **Administration > System > Settings > Posture > General Settings** configuration page. The posture run-time services takes appropriate action when you add or remove any advanced license file to your Cisco ISE deployment. During run time, the SWISS server initializes when you add the advanced license, and it stops when you remove the advanced license, or when the advanced license expires.

Deploying the Posture Service

Prerequisites:

Before you begin, you should have an understanding of the centralized configuration and management of Cisco ISE nodes in the distributed deployment.

For information on Cisco ISE distributed deployment, Chapter 9, "Setting Up Cisco ISE in a Distributed Environment"

You can deploy Cisco ISE either in a standalone environment (on a single node), or in a distributed environment (on multiple nodes). Depending on the type of your deployment and the license you have installed, the posture service of Cisco ISE can run on a single node or on multiple nodes. You need to install either the base license to take advantage of the basic services or the advanced license to take advantage of all the services of Cisco ISE.

In a standalone Cisco ISE deployment, you can configure a single node for all the administration services, the monitoring and trouble shooting services, and the policy run-time services. You cannot configure a node as an node in a standalone deployment.

In a distributed Cisco ISE deployment, you can configure each node as a Cisco ISE node for administration services, monitoring and troubleshooting services, and policy run-time services, or as an inline posture node as needed. A node that runs the administration services is the primary node in that Cisco ISE deployment. The other nodes that run other services are the secondary nodes which can be configured for backup services for one another.

Configuring the Posture Service in Cisco ISE

From the Administration menu, you can choose Deployment to manage the ISE deployment on a single node or multiple nodes. You can use the Deployment Nodes page to configure the posture service for your Cisco ISE deployment.

To manage the Cisco ISE deployment, complete the following steps:

Step 1 Choose **Administration > System > Deployment**.

The Deployment menu window appears on the left pane of the user interface. You can use the Table view button or the List view button to display the nodes in your Cisco ISE deployment.

Step 2 Click the **Table** view button.

Step 3 Click the **Quick Picker** (right arrow) icon to view the nodes that are registered in your deployment.

The Table view displays all the nodes that are registered in a row format on the right pane of the user interface.

Note To view the nodes in your deployment in a tree, click the **List** view button. An arrow appears in front of the Deployment menu. Click the arrow in front of the Deployment menu to view the nodes that are registered in your deployment in a tree view. The List view displays all the nodes in the Deployment menu window in a tree.

From the Deployment menu, you can run the posture service on any Cisco ISE node that assumes the Policy Service persona in a distributed deployment.

To deploy the posture session service, complete the following steps:

Step 1 Choose **Administration > System > Deployment > Deployment** (menu window).

The Deployment menu window appears. You can use the Table view or the List view button to display the nodes on your deployment.

Step 2 Click the **Table** view button.

Step 3 Click the **Quick Picker** (right arrow) icon to view the nodes that are registered in your deployment.

The Table view displays all the nodes that are registered in a row format on the Deployment Nodes page of the user interface. The Deployment Nodes page displays the Cisco ISE nodes that you have registered, along with their names, personas, roles, and the replication status for the secondary nodes in your deployment.

Step 4 Choose a Cisco ISE node from the Deployment Nodes page.

Note If you have more than one node that are registered in a distributed deployment, all the nodes that you have registered appear in the Deployment Nodes page, apart from the primary node. You have the option to configure each node as a Cisco ISE node (administration, policy service, and monitoring personas) or an Inline Posture node.

Step 5 Click the **Edit** button.

The Edit Node page appears. This page contains the General settings tab that is used to configure the Cisco ISE deployment. This page also features the Profiling Configuration tab, which is used to configure the probes on each node. If you have the Policy Service persona disabled, or if enabled but the **Enable Profiler services** option is not selected, then the Cisco ISE administrator user interface does not display the Profiling Configuration tab. If you have the Policy Service disabled on any node, ISE displays only the General settings tab and does not display the Profiling Configuration tab that prevents you from configuring the probes on the node.

Step 6 From the General settings tab, check the **Policy Service** check box, if it is already active.

If you have the Policy Service check box unchecked, both the session services and the Profiler service check boxes are disabled.

Step 7 For the Policy Service persona to run the Network Access, Posture, Guest, and Client Provisioning session services, check the **Enable Session Services** check box, if it is not already active. To stop the session services, uncheck the **Enable Session Services** check box.

Note The posture service only runs on Cisco ISE nodes that assume the Policy Service persona and does not run on Cisco ISE nodes that assume the administration and monitoring personas in a distributed deployment.

Step 8 Click **Save** to save the node configuration.

Posture Compliance Dashlet

The Posture Compliance dashlet summarizes the posture compliance in percentage, and Mean Time To Remediate (MTTR) data for the last 24 hour period, as well as 60 minutes from the current system time. It refreshes data every minute and displays it on the dashlet. You can invoke the Posture Detail Assessment report from the tool tips that are displayed on the 24 hour and 60 minutes spark lines for a specific period. The stack bars display the posture noncompliance distribution of endpoints by operating systems and the reason for failures of the requirements.

The MAC address is used as a key to calculate MTTR.

The dashlet provides you the following distribution details for the last 24 hour period, as well as 60 minutes from the current system time.

Table 20-1 describes the details, which are shown in the Posture Compliance dashlet on Cisco ISE.

Table 20-1 Posture Compliance Dashlet

Name	Description
Passed in percentage	Displays the percentage (passed percentage) of posture compliance of endpoints by using posture compliance and noncompliance of endpoints.
Mean Time to Remediate (MTTR)	Displays the mean time difference between endpoints moving from the noncompliant state to the complaint state based on the unique MAC address.
Operating System	Displays the noncompliance distribution by operating system that is running on the client.
Reason	Displays the noncompliance distribution by failures of posture conditions.

Viewing Posture Reports

Cisco ISE provides you with various reports on posture, and troubleshooting tools that you can use to efficiently manage your network. You can generate reports for historical as well as current data. You may be able to drill down on a part of the report to look into more details. You can also schedule reports (specially for large reports) and download it in various formats.

For more information on how to generate reports and work with the interactive viewer, see Chapter 24, "Reporting."

For more information on posture reports see the "Standard Reports" section on page 20-9.

Standard Reports

For your convenience, the standard reports present a common set of predefined report definitions. You can click on the Report Name link to run the report for today. You can query the output by using various parameters, which are predefined in the system. You can enter specific values for these parameters.

You can use the Run button to run the report for a specific period, and as well as use the Query and Run option. The Query and Run option allows you to query the output by using various parameters. The Add to Favorite button allows you to add your reports that you use frequently to the Operations > Reports > Favorites location. The Reset Reports button allows you to reset your reports in this catalog to factory defaults.

You can run the reports on posture from the following location:

Operations > Reports > Catalog > Posture.

The following are the standard reports for posture:

- Posture Detail Assessment—a report to view the posture authentication summary information for a particular user for a selected time period
- Posture Trend—a report to view the count of passed/failed and status information for a particular policy along with the graphical representation for a selected time period

Posture Administration Settings in Cisco ISE

After you deploy Cisco ISE on your network, you can globally configure Cisco ISE to download updates automatically through web to the Cisco ISE server, or updates that can be done offline later.

For information on posture updates, see the "Posture Updates" section on page 20-22.

In addition, the NAC Agents and Web Agents, which are installed on the clients provide posture assessment, and remediation services to clients. The NAC Agents and Web Agents periodically update the compliance status of clients to Cisco ISE. After login and successful requirement assessment for posture, the NAC Agents and Web Agents on Windows display a dialog with a link that requires end users to comply with terms and conditions of network usage. You can use this link to define network usage information for your enterprise network that end users accept before they can gain access to your network.

For information on posture periodic assessment of clients for compliance that NAC Agents and Web Agents do, see the "Posture Reassessments" section on page 20-12.

For information on accepting network usage policies for your network, see the "Posture Acceptable Use Policy" section on page 20-24.

This section describes the configuration settings that you define for clients to remediate on Cisco ISE, periodic reassessments of clients for compliance that NAC and Web Agents check periodically and report to Cisco ISE. It describes the configuration settings that you define for Cisco ISE updates with Cisco rules, checks, antivirus and antispyware charts, and operating system support. It also provides information on the configuration settings that end users must comply with network usage policies for using your network resources.

This section provides procedures that describe the following topics:

- Posture General Settings, page 20-10
- Posture Reassessments, page 20-12
  - Configuring Client Posture Periodic Reassessments, page 20-15
  - Filtering Client Posture Periodic Reassessments, page 20-19

- Posture Updates, page 20-22
  - Dynamic Posture Updates, page 20-22
  - Offline Posture Updates, page 20-24
- Posture Acceptable Use Policy, page 20-24

Posture General Settings

The posture general settings for agents on Windows clients and Macintosh clients can be configured in client provisioning resources. Here, you can configure agent profiles in client provisioning by setting the timers used for remediation and transition of clients posture state on your network, and also setting the timer to close the login success screens automatically on agents without end users intervention.

You can configure all these timers for agents on Windows clients and Macintosh clients in client provisioning resources in the following location:

Policy > Policy Elements > Results > Client Provisioning > Resources > Add > New Profile.

For more information on creating agent profiles and setting agent profile parameters, see the "Agent Profile Parameters and Applicable Values" section on page 19-16.

Cisco recommends configuring agent profiles with remediation timers, network transition delay timers and the timer used to control the login success screen on client machines so that these settings are policy based. However, when there are no agent profiles configured match the client provisioning policies, you can use the settings in the **Administration > System > Settings > Posture > General Settings** configuration page to accomplish the same goal.

Remediation Timer

Here, you can configure the timer for clients to remediate themselves within the time specified in the timer after failing to meet all the requirements defined in the posture policies for compliance. When clients fail to satisfy configured posture policies during an initial assessment, the NAC Agents wait for the clients to remediate within the time configured in the remediation timer. If the client fails to remediate within this specified time, then the NAC Agents and Web Agents send a report to the posture run-time services after which the clients are moved to the noncompliance state. The remediation timer default value is four minutes.

Network Transition Delay Timer

Here, you can configure the timer for clients to transit from one state to the other state within a specified time as specified in the network transition delay timer, which is required for Change of Authorization (CoA) to complete for clients to move from one state to the other state. This timer is used for clients in both successful and failure of posture. It may require a longer delay time when clients need time to get a new VLAN IP address during successful and failure of posture. Upon successfully postured, Cisco ISE allows clients to transit from unknown to compliant mode within the time specified in the network transition delay timer. Upon failure of posture, Cisco ISE allows clients to transit from unknown to noncompliant mode within the time specified in the timer.

Default Posture Status

Here, you can configure the posture status of endpoints to compliant, or noncompliant for endpoints that run on Linux, iDevices like Ipad, Ipod (non-agent devices). The same settings also apply to endpoints that run on Windows and Macintosh operating systems when there is no client provisioning policy matching found during posture run-time.

iDevices and Android Smart Phones

When an Android device and Apple iDevices such as iPod, iPhone, and iPad connect to your Cisco ISE enabled network via WLC (that supports CoA), CoA Session Termination is issued.

If these devices connect to your Cisco ISE enabled network via VPN/iPEP, then CoA Re-Auth is issued and the posture status of those devices will take the Default Posture Status settings in Cisco ISE.

Successful Login Screen

After login and successful posture assessment, the NAC Agents and Web Agents display a temporary network access screen. Here, the agents display a network usage term and conditions link for end users to accept the network usage policies that you define for your network. If end users reject network usage policies from the temporary network access screen, then they are denied to access your network. If they accept the network usage policies, then the agents display the login success screen and permit network access.

This section describes the following posture general settings that you configure for clients in posture:

- Remediation Timer—specifies time in minutes required for any type of remediation within which clients need to remediate from the noncompliance state to the compliance state
- Network Transition Delay—specifies time in seconds for network transition for both successful and failure of posture of clients on your network
- Default Posture Status—specifies the posture status for clients that do not run supported operating systems in Cisco ISE
- Successful Login Screen—specifies the timeout in seconds that closes the login success screen without end users intervention.

You can use the posture General Settings page to configure the timers for remediation, network transition, and closing the login success screen on Windows clients.

Step 1 Choose **Administration > System > Settings** (menu window).

The Settings menu window appears.

Step 2 From the Settings menu window, choose **Posture**.

Step 3 Click the arrow to view the settings used for posture.

Step 4 Choose **General Settings**.

The Posture General Settings page appears.



Tip The information icon provides you details on the posture General Settings page with the following message: “These settings will be used if there is no profile under client provisioning policy.”

Step 5 Enter a time value in the **Remediation Timer** field in minutes.

The default value is 4 minutes. You can configure the remediation timer, which the information icon displays the valid range between 1-300 minutes.

Step 6 Enter a time value in the **Network Transition Delay** field in seconds.

The minimum default value is 3 seconds. You can configure the network transition delay timer, which the information icon displays the valid range between 2-30 seconds.

Step 7 From the **Default Posture Status** field, choose the option from the drop-down list.

Here, you can configure the posture status of endpoints to compliant, or noncompliant where the information icon displays with the following message: “Provides posture status for non-agent devices (i.e. Linux based operating systems), and endpoints for which no agent installation policy applies.”

The following are the options:

- Compliant (default)
- NonCompliant

Step 8 Click to check the **Automatically close login success screen after** check box.

Step 9 Enter a time value for the Automatically close login success screen after check box.

Once checked the check box, and configured the time in seconds, the NAC Agents and Web Agents display the login success screen till the time out occurs. This setting allows clients to login into your network failing which the login success screen is closed automatically. You can configure the timer to close the login screen automatically between 0-300 seconds. If the time is set to zero seconds, then the NAC Agents and Web Agents do not display the login success screen.

Tip The information icon provides you details on Automatically close login success screen after check box with the following message: “Setting the time to zero seconds will not display the login success screen. Valid range: 0-300 seconds.

Step 10 Click **Save** to save the current input data.

To reset the posture general settings, complete the following steps:

Step 1 Click the **Remediation Timer** field.

Enter a time value (current input data) in the Remediation Timer field in minutes.

or

Step 2 Click the **Network Transition Delay** field.

Enter a time value (current input data) in the Network Transition Delay field in seconds.

or

Step 3 From the **Default Posture Status** field, choose the option from the drop-down list.

The following options appear: Compliant (default), NonCompliant

or

Step 4 Check to enable, or uncheck to disable the **Automatically close login success screen after** check box.

Step 5 Click **Save** to save the current input data.

Posture Reassessments

This section describes the periodic reassessment (PRA) configurations for clients that are successfully postured already for compliance on your network. PRA cannot occur if clients are not compliant on your network.

For more information on initiating and requesting a PRA, see the Initiating and Requesting a PRA, page 20-13.

For more information on PRA failure action configuration, see the PRA Failure Actions, page 20-13.

For more information on PRA and a user identity group (role) assignment, see the User Identity Group (Role) Assignment, page 20-14.

For more information on PRA report tracking and enforcement, see the PRA Report Tracking and Enforcement, page 20-15

For more information on PRA enforcements when Cisco ISE distributed deployment failures, see the PRA Enforcement During Distributed System Failure, page 20-15

Initiating and Requesting a PRA

The NAC Agent sends a compliance report to the policy service node once the client is postured successfully compliant on your network. A PRA is valid and applicable only if endpoints are in compliant state. Then the policy service node checks the relevant policies, and compiles the requirements depending on the client role that is defined in the configuration to enforce a PRA. If PRA configuration match is found, the policy service node responds to the NAC Agent with the PRA attributes that are defined in the PRA configuration for the client before issuing a change of authorization request. The NAC Agent periodically sends the PRA requests based on the interval specified in the configuration. Here, the client remains in the compliant state, if the PRA succeeds, or the action configured in the PRA configuration is to continue. If the client fails to meet PRA, then the client is moved from the compliant state to the noncompliant state.

Note The PostureStatus attribute shows the current posture status as compliant in a PRA request instead of unknown even though it is a posture reassessment request. The same is updated in the Monitoring reports as well. The PostureStatus attribute of any client before reassessment of new requirements and posture policies retrieved from the server in a PRA request should represent the posture status as unknown in a PRA request assuming that the client is being postured after successful authentication.

PRA Failure Actions

If the client is not compliant, the policy service node activates a PRA failure action. The PRA failure action that will be taken either to continue so that the client continues to access your network, or to log off from your network, or to remediate itself.

If you associate an user to different roles and each associated role is configured with different PRA failure actions (logoff, remediate, and continue) then the *logoff* action is applied on the endpoint.

The following enforcement types apply to PRA failure actions:

- Continue
- Logoff
- Remediate

PRA Failure Action to Continue

In this scenario, the client is not compliant, and the configured PRA failure action is to continue. This failure action to continue does not allow the user to remediate the client and the NAC Agent does not show the user the need to remediate the client for compliance. Instead, the user continues to have the privileged access without any user intervention to remediate the client irrespective of the posture requirement, which is set to mandatory or optional.

PRA Failure Action to Logoff

In this scenario, the client is not compliant, and the configured PRA failure action is to force the client to log off from your network. The Agent sends a logoff request to the policy service node, and the client logs off. The client logs in again, and its compliance status is unknown for the current session.

PRA Failure Action to Remediate

In this scenario, the client is not compliant, and the configured PRA failure action is to remediate. The agent waits for a specified time for the remediation to occur. After the client has remediated, the agent sends the PRA report to the policy service node. If the remediation is ignored on the client, then the Agent sends a logoff request to the policy service node to force the client to log off from your network and log in again to remediate for compliance.

If the posture requirement is set to mandatory, then the RADIUS session will be cleared as a result of the PRA failure action and a new RADIUS session has to start for the client to be postured again.

If the posture requirement is set to optional, then the NAC Agent allows the user to click the continue option from the Agent. The user can continue to stay in the current network without any restriction.

User Identity Group (Role) Assignment

You can configure each PRA to a user identity group (a role) that is defined in the system. If you configure a PRA with a role *Any* then only the configuration with the role *Any* exists, and no other configurations can exist in the system.

The following section summarizes the PRA configuration to a user identity group:

1. Ensure that each PRA configuration has a unique group or a unique combination of user identity groups assigned to the configuration.

   Note You can assign a role_test_1 and a role_test_2, the two unique roles to a PRA configuration. You can combine these two roles with a logical operator and assign the PRA configuration as a unique combination of two roles. For example, role_test_1 or role_test_2.

2. Ensure that two PRA configurations cannot have a user identity group in common.
3. If a PRA configuration already exists with a user identity group "*Any*", you cannot create other PRA configurations unless you perform the following:
   a. You update the existing PRA configuration with a user identity group "*Any*" to reflect a user identity group (or user identity groups) other than *Any*.

      or

   b. You delete the existing PRA configuration with a user identity group "*Any*".

Note If you *must* create a PRA configuration with a user identity group *"Any"*, ensure that you delete all other PRA configurations from the Reassessment configurations.

PRA Report Tracking and Enforcement

You can keep track of the PRA reports from the NAC Agent and enforce PRA on the clients that are already successfully postured on your network.

Upon successful compliance for posture, the NAC Agent validates the client for compliance and sends the compliance reports to the policy service node. The NAC Agent periodically sends the PRA requests for reassessment based on the interval that is specified in the configuration.

If the policy service node does not receive the PRA report within the maximum wait interval period, then the policy service node assigns the client to the unknown status and the client needs to be checked again for posture compliance. The maximum wait interval is an interval between two consecutive compliance (PRA) reports from the NAC Agent sent to the policy service node before the execution of a PRA failure action for noncompliance and the end of the client session.

Note The maximum wait interval is the sum of the PRA interval and twice the grace time that is configured in the PRA configuration as maximum wait interval = PRA interval + (grace time * 2).

PRA Enforcement During Distributed System Failure

The PRA is not supported in cases where policy service nodes fail in the distributed environment.

You cannot enforce a PRA on your clients, and the clients stay connected on your network regardless of their compliance in case there is a failure in the distributed environment. The Agents stop sending the PRA requests to the policy service nodes.

Configuring Client Posture Periodic Reassessments

Upon successful compliance for posture, the NAC Agents validate the compliance of clients, and periodically send the compliance reports to the Cisco ISE policy service node. The Cisco ISE policy service nodes check the relevant policies and compiles requirements depending on the client roles that are defined in the configuration to enforce a periodic reassessment. The Cisco ISE policy service nodes then respond to the NAC Agents with PRA attributes defined in the PRA configurations. As you associate a user to more than one user identity group (user identity groups), the PRA configurations are applied according to the most restricted attributes on the relevant role's related configurations.

The following are the most restricted configuration definitions for the PRA attributes:

- Use reassessment enforcement—requires at least one configuration and has its reassessment required flag on the PRA configuration
- Interval—the least interval of all the relevant PRA configurations
- Grace time—the least interval of all the relevant PRA configurations
- Enforce type—the most restricted enforcement type is logoff; after log off, the client needs to remediate and then continue.

You can use the Reassessment configurations page to display and manage the periodic reassessments for a posture.

This section provides the procedures to configure the periodic reassessment configurations:

- Creating, Duplicating, Editing, and Deleting a Client Posture Periodic Reassessment, page 20-16
- Filtering Client Posture Periodic Reassessments, page 20-19

Creating, Duplicating, Editing, and Deleting a Client Posture Periodic Reassessment

This section describes the periodic reassessment configuration that you can create in Cisco ISE for your clients after they are successfully postured.

The Reassessment configurations page displays existing configurations that are configured to groups along with their names, description, and the action enforced on the clients in case the clients fail posture assessment. You can create, duplicate, edit, delete, or filter a PRA from the Reassessment configurations page. Once created and saved a PRA, you can see existing PRA configurations, and the groups to which the PRA configurations apply on the configurations list page.

To create a periodic reassessment, complete the following steps:

Step 1 Choose **Administration > System > Settings > Settings** (menu window).

Step 2 From the Settings menu window, choose **Posture**.

Step 3 Click the arrow to view the settings used for posture.

Step 4 Choose **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you have already created.

Step 5 Click **Add**.

Step 6 Modify the values on the New Reassessment Configuration page, as shown in Table 20-2 on page 20-18.

Here, you can create to add a new PRA on the Reassessment configurations page.

Step 7 Click **Submit** to create a PRA configuration.

Click **Cancel** to return to the Reassessment configurations page from the New Reassessment Configuration page when you do not want to add a new PRA on this page.

To duplicate a PRA, complete the following steps:

Step 1 From the Settings menu window, choose **Posture**.

Step 2 Click the arrow to view the settings used for posture.

Step 3 Choose **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you have already created. PRA configurations display the user identity groups to which existing PRAs are configured on the configurations list.

Step 4 Choose a PRA that you want to duplicate.

Step 5 From the Reassessment configurations page, choose **Duplicate**.

Here, you can create a copy of a PRA.

Step 6 Click **Submit** to create a copy of a PRA.

Click **Cancel** to return to the Reassessment configurations page from the edit page when you do not want to create a copy of a PRA on the edit page.

To edit a PRA, complete the following steps:

Step 1 From the Settings menu window, choose **Posture**.

Step 2 Click the arrow to view the settings used for posture.

Step 3 Choose **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you have already created.

Step 4 Choose the PRA that you want to edit.

Step 5 From the Reassessment configurations page, choose **Edit**.

Here, you can edit a PRA.

Step 6 Click **Save** to save the changes made to the PRA.

The PRA will appear on the Reassessment configurations page after editing on the edit page, as well as appear on the PRA configurations that displays the groups to which existing PRAs are configured on the configurations list.

Step 7 Click the **Reassessment Configurations List** link from the edit page to return to the Reassessment configurations page.

To delete a PRA, complete the following steps:

Step 1 From the Settings menu window, choose **Posture**.

Step 2 Click the arrow to view the settings used for posture.

Step 3 Choose **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you have already created.

Step 4 Choose the PRA that you want to delete.

Step 5 From the Reassessment configurations page, choose **Delete**.

A confirmation dialog appears with the following message: “Are you sure you want to delete?”.

Step 6 Click **OK** to delete a PRA.

Here, you can delete a PRA. Click **Cancel** to return to the Reassessment configurations page without deleting a PRA.

Table 20-2 describes the fields on the New Reassessment Configuration page that allow you to create a PRA, duplicate a PRA, and edit a PRA on its edit page:

Table 20-2 PRA Configurations

Field Name	Field Description
Configuration Name	From the Configuration Name field, enter the name of the PRA configuration that you want to create.
Configuration Description	From the Configuration Description field, enter the description of the PRA configuration.
Use Reassessment Enforcement?	When the Use Reassessment Enforcement check box is checked, the PRA configurations configured for the user identity groups are applied. If unchecked, the PRA configurations configured for the user identity groups are not applied.
Enforcement Type	If clients fail to meet the posture requirement, then one of the following actions is enforced on the client. Click the drop-down arrow to view the predefined settings: • Continue • Logoff • Remediate Choose one from the list.
Interval	From the Interval field, enter a time interval specified in minutes to initiate PRA on the clients thereafter first successful log in. The information icon next to the Interval field provides you the minimum and maximum interval that you can set for PRAs. The minimum interval can be 60 minutes (one hour), and the maximum interval can be 1440 minutes (24 hours) for PRAs. The default interval time is specified as 240 minutes (4 hours).
Grace time	From the Grace Time field, enter a time interval specified in minutes to allow the client to complete remediation. The grace time cannot be zero, and greater than the PRA interval. It can range between the default minimum interval (5 minutes) and the minimum PRA interval. The information icon next to the Grace time field provides you the minimum and maximum interval that you can set for PRAs. The minimum grace time can be 5 minutes and the maximum grace time can be 60 minutes. **Note** The grace time is enabled only when the enforcement type is set to remediate action after the client fails the posture reassessment.

Table 20-2 PRA Configurations (continued)

Field Name	Field Description
Select User Identity Groups	From the Select User Identity Groups field, choose a unique group, or a unique combination of groups for your PRA configuration. Note the following while creating a PRA configuration: • Each configuration must have a unique user identity group, or a unique combination of user identity groups. • No two configurations can have any user identity group in common. • If you want to create a PRA configuration with a user identity group "Any", delete all other PRA configurations first. • If you create a PRA configuration with a user identity group "Any", then you cannot create other PRA configurations with a unique user identity group, or user identity groups. To create a PRA configuration with a user identity group other than "Any", either delete an existing PRA configuration with an user identity group "Any" first, or update an existing PRA configuration with a user identity group "Any" with a unique user identity group, or user identity groups.
PRA configurations—configurations list	An area that lists existing PRA configurations and user identity groups associated to PRA configurations.

Filtering Client Posture Periodic Reassessments

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Reassessment configurations page. A quick filter is a simple and quick filter that can be used to filter periodic reassessments on the Reassessment configurations page. It filters periodic reassessments based on field description such as the name of the periodic reassessments, description, action enforced on the clients when clients fail posture assessment, user identity groups to which periodic reassessments are configured, and periodic reassessments that are enabled or disabled on the Reassessment configurations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Reassessment configurations page. It filters periodic reassessments based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the filtered results on the Reassessment configurations page. You can also edit preset filters and remove them from the preset filters list.

To filter periodic reassessments, complete the following steps:

Step 1 Choose **Administration > System > Settings** (menu window).

Step 2 From the Settings menu window, choose **Posture**.

Step 3 Click the arrow to view the settings used for posture.

Step 4 Choose **Reassessments**.

The Reassessment configurations page appears, which lists all the PRAs that you have already created.

Step 5 From the Reassessment configurations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-3.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-20 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-20.

Note To return to the Reassessment configurations page, choose **All** from the Show drop-down to display all the periodic reassessments without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters periodic reassessments based on each field description on the Reassessment configurations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Reassessment configurations page. If you clear the field, it displays the list of all the periodic reassessments on the Reassessment configurations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter periodic reassessments by using variables that are more complex. It contains one or more filters, which filter periodic reassessments based on the values that match the field description. A filter on a single row filters periodic reassessments based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter periodic reassessments by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add the filtered lists, or click the **Remove Row** button (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-3 describes the fields that allow you to filter the PRAs:

Table 20-3 Filtering Reassessment Configurations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter periodic reassessments by the name of the periodic reassessment.
	Description	This field enables you to filter periodic reassessments by the description of the periodic reassessment.
	Type	This field enables you to filter periodic reassessments by actions enforced on the client.
	User Identity Groups	This field enables you to filter periodic reassessments by user identity groups configured for periodic reassessments.
	Enable	This field enables you to filter periodic reassessments by those reassessments that are enabled.
Advanced Filter	Choose the field description from the following: • Name • Description • Type • User Identity Groups • Enable	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter periodic assessments.
	Value	From the Value field, choose the value for the field description that you selected against which to filter periodic assessments.

Posture Updates

Prerequisite

If the default Update Feed URL is not reachable, you must configure the proxy settings in the **Administration > System > Settings > Proxy**.

For more information on proxy settings, see Specifying Proxy Settings in Cisco ISE, page 8-17.

Updates for posture includes a set of predefined checks, rules, antivirus and antispyware support charts for both Windows and Macintosh operating systems, and operating systems information that are supported by Cisco. You can download posture updates from Cisco to your Cisco ISE deployment through the web dynamically, and as well as configure updates to occur automatically after allowing a time delay within a maximum of 24 hours in hh:mm:ss format. Thereafter, Cisco ISE checks and downloads updates at specified intervals from the initial updates automatically. You can also update Cisco ISE offline from a file on your local system, which contains the latest archives of updates.

When you deploy Cisco ISE on your network for the first time, you can download initially posture updates from the web that usually takes around 20 minutes of time. Thereafter, you can configure to check and download incremental updates to occur automatically on Cisco ISE without your intervention. Once updated, the Posture Updates page displays the current Cisco updates version information as a verification of an update under Update Information.

Note Cisco ISE creates default posture policies, requirements, and remediations only once during an initial posture updates. If you delete them, Cisco ISE does not create them again during subsequent updates that you perform either manually or using scheduled posture updates.

This section provides procedures that describe dynamic, and offline update configurations for posture:

- Dynamic Posture Updates, page 20-22
- Offline Posture Updates, page 20-24

Related Topics

Custom Conditions for Posture, page 20-42

Dynamic Posture Updates

You can use the Posture Update page to download updates dynamically from the web, and configure updates to occur automatically after allowing a time delay from the initial updates. Thereafter you can check and download updates at regular intervals without your intervention.

To download updates dynamically from the web, complete the following steps:

Step 1 Choose **Administration > System > Settings** (menu window).

Step 2 From the Settings menu window, choose **Posture**.

Step 3 Click the arrow to view the settings for posture.

Step 4 Choose **Updates**.

The Posture Updates page appears.

Step 5 From the Posture Updates page, choose the **Web** option to download updates dynamically.

Step 6 Click the **Set to Default** button to set the Cisco default value for the Update Feed URL field.

For example, the default Update Feed URL is https://www.cisco.com/web/secure/pmbu/posture-update.xml.

Note If this default Update Feed URL is not reachable, then you can configure the proxy settings alternatively on the Posture Updates page. For more information on proxy settings, see Specifying Proxy Settings in Cisco ISE, page 8-17.

Step 7 Modify the values on the Posture Updates page, as shown in Table 20-4.

Step 8 Click the **Update Now** button to download updates from Cisco.

Cisco ISE displays an information dialog with the following message:

"The update might take up to 20 minutes to finish. Navigating to other pages will not stop the updating and you can check the result on this page later."

Step 9 Click **OK** to continue with other tasks on Cisco ISE.

Once updated, the Posture Updates page displays the current Cisco updates version information as a verification of an update under Update Information.

Note Downloading updates dynamically from the web may take a few minutes for the first time to update the Cisco ISE server. When updates is in progress, you can leave the updates page to continue with other tasks on Cisco ISE. If an update is in progress, then you will see a waning dialog displayed on the updates page when you return to the Posture Updates page. When an update is in progress, Cisco ISE displays a warning dialog with the following warning message: "There is already an update running. Please try later."

After an initial update, you can configure to check for updates and download updates to your Cisco ISE deployment automatically on the Posture Updates page. Cisco ISE downloads updates at specified intervals from the web automatically after an allowed initial delay from the first time updates.

To continue to check for updates automatically and download at a specified interval from the initial updates, complete the following steps:

Step 1 Check the **Automatically check for updates starting from initial delay** check box.

Step 2 Enter the initial delay time in hh:mm:ss format.

Cisco ISE starts checking for updates after the initial delay time is over.

Step 3 Enter the time interval in hours.

Cisco ISE downloads updates to your deployment thereafter at specified intervals from the initial delay time.

Step 4 Click **Yes** to continue.

Step 5 Click **Save** to download updates at regular intervals from the initial time delay.

Note When you configure Cisco ISE to check for the updates automatically, the latest AV/AS Support charts get populated accordingly. Anyway, you need to download the latest Compliance Module and add it to the Client Provisioning policy manually. If the latest Support charts do not synchronize with the existing Compliance Module, ensure that you are downloading the latest Compliance Module and adding it to the Client Provisioning policy.

Table 20-4 describes the fields that allow you to download updates dynamically from the web, or offline.

Table 20-4 Update Configurations

Field	Field Description
Posture Updates options	The following options are available for Posture updates on Cisco ISE: Web, and Offline.
Update Feed URL	A valid URL to update from the web. For example: https://www.cisco.com/web/secure/pmbu/posture-update.xml
Set to Default	Click to set the Cisco default URL for Update Feed URL.
Proxy Address	The IP address of the configured proxy server.
Proxy Port	The port of the configured proxy server.
Automatically check for updates starting from initial delay check box	Allows Cisco ISE automatically to check for updates after the delay time is over, and thereafter download updates at regular intervals. Click to check the check box.
An initial delay time specified in hh:mm:ss format, after which Cisco ISE checks for updates	Cisco ISE starts checking for updates after an initial delay time is over. Here, click the drop-down arrow to choose the initial delay time in hh:mm:ss format after which Cisco ISE should start to check for updates.
An interval specified in hours, at which Cisco ISE downloads updates automatically from the initial delay time.	Here, enter the interval hours of time at which Cisco ISE should download updates automatically from the initial delay time.

Offline Posture Updates

For details on performing offline posture package updates in Cisco ISE, see the "Cisco ISE Offline Updates" section of the *Release Notes for the Cisco Identity Services Engine, Release 1.1*.

Posture Acceptable Use Policy

After login and successful posture assessment of clients, the NAC Agents and Web Agents display a temporary network access screen. Here, the agents display a link on the temporary network access screen for end users to click on the link. This link redirects end users to a page, where you can define your network usage terms and conditions that end users must read, and accept the network usage policies here.

Each AUP configuration must have a unique user identity group, or a unique combination of user identity groups. Even though a user can be associated to multiple user identity groups in Cisco ISE, and there are different AUP configurations for a unique user identity group, or a unique combination of user identity groups, Cisco ISE looks for the user identity groups and the associated AUP configuration for the user identity groups. Cisco ISE finds the AUP for the first matched user identity group, and then it communicates to the NAC Agent and Web Agent to display the AUP of the first matched user identity group. The user can click the link to accept the network usage policies here after which the user gets access privileges to your network.

Authorization Profile Configuration Guidance for Posture Clients Quarantine State

This section guides you through the configuration details when clients are moved into quarantine state due to end users deny to comply with your network usage policies, or when clients fail to meet the mandatory requirements.

Without accepting the network usage terms and conditions even though clients meet all the mandatory requirements that are defined in the posture assessment policies, they are denied network access to your network, and moved into a quarantine state forever. If clients are moved into the quarantine state, they will not be to reauthenticate again in order to be postured successfully for compliance again. If clients need to come out of the quarantine state in order to become compliant, then the network access devices must be configured to restart a new RADIUS session after the session times out so that clients can reauthenticate again depending on your configuration, and then agree to the network usage policies of your network.

You can choose an authorization profile and configure it using the **Policy > Policy Elements > Results > Authorization > Authorization Profiles** page.

For more information on authorization policies and profiles, see Chapter 17, “Managing Authorization Policies and Profiles.”

Here, you can choose the Access-Accept option from the Access Type field, and configure information for re-authentication under Common Tasks, or under Advanced Attributes Settings for an authorization profile.

For example, you can configure the value of RADIUS: Termination-Action attribute to Default, and the RADIUS: Session-Timeout attribute to a time value under Common Tasks > Re-authentication, or under Advanced Attributes Settings. If the value of RADIUS: Termination-Action attribute is set to RADIUS-Request, the NAS sends a new Access-Request to the RADIUS server, including the state attribute, if any upon termination of the specified service. This configuration allows you to set a timeout value for a quarantine state. After the time out, a new RADIUS session can be started and the client can reauthenticate again and check for posture.

- RADIUS: Termination-Action—An action, which should be taken by the NAS when the specified service is completed. It is only used in Access-Accept message.
- RADIUS: Session-Timeout—A timeout value specified in maximum number of seconds of service to be provided to the user before termination of the RADIUS session, where the client remains connected by the NAS. It is an attribute to be sent by the RADIUS server to the client in an Access-Accept, or Access-Challenge messages.

In addition to the above, you have to enter the following additional commands for your network device:

- authentication periodic—use this interface configuration command to enable, or disable re-authentication on a port. Enter the no form of this command to disable re-authentication.

  This CLI command shows how to enable periodic re-authentication on a port.

  ```
  Switch(config-if)# authentication periodic
  ```
- authentication timer reauthenticate server—use this interface configuration command to configure the time out and re-authentication parameters for an 802.1x-enabled port.

This CLI command shows how to set the re-authentication timer where reauthenticate specifies time in seconds after which an automatic re-authentication attempt should start, and server specifies an interval in seconds after which an attempt can be made to authenticate an unauthorized port.

authentication timer—interface configuration command

reauthenticate—specifies time in seconds after which an automatic re-authentication attempt starts. It is set to one hour.

server—specifies interval in seconds after which an attempt is made to authenticate an unauthorized port

```
Switch(config-if)# authentication timer reauthenticate server
```

Configuring Acceptable Use Policies

You can view, create, delete, or filter acceptable use policies (AUPs) on the Acceptable Use Policy Configurations page. It displays all the AUPs with their names, description, type, the name of the zipped file, or the URL that contains the network usage policies depending on the type of the AUPs, and the user identity groups to which they are configured.

This section covers the following procedures:

- Viewing, Adding, and Deleting an Acceptable Use Policy, page 20-26
- Filtering Acceptable Use Policies, page 20-29

Viewing, Adding, and Deleting an Acceptable Use Policy

You can use the Acceptable Use Policy Configurations page to view, create, or delete acceptable use policies, which allow network access to your network to clients on acceptance of the network usage policies.

To view an acceptable use policy, complete the following steps:

Step 1 Choose **Administration > System > Settings > Settings** (menu window).

Step 2 From the Settings menu window, choose **Posture**.

Step 3 Click the arrow to view the settings used for posture.

Step 4 Choose **Acceptable Use Policy**.

The Acceptable Use Policy Configurations page appears, which lists all the AUPs that you have already created.

Step 5 Choose an acceptable use policy from the list.

Step 6 Click **View**.

Here, you can view the acceptable use policy.

Step 7 Click the **Acceptable Use Policy Configuration list** link to return to the Acceptable Use Policy Configuration list page.

Click **Cancel** to return to the Acceptable use policy configuration list page. A confirmation dialog appears with the following message: “Are you sure you want to cancel?. You will lose all the changes you have made.” Click **Yes** to return to the Acceptable use policy configuration list page. If you click **No**, you are retained on the same view page.

To create an acceptable use policy, complete the following steps:

Step 1 Choose **Administration > System > Settings > Settings** (menu window).

Step 2 From the Settings menu window, choose **Posture**.

Step 3 Click the arrow to view the settings used for posture.

Step 4 Choose **Acceptable Use Policy**.

The Acceptable Use Policy Configurations page appears, which lists all the AUPs that you have already created.

Step 5 Click **Add**.

Step 6 Modify the values on the New Acceptable Use Policy Configuration page, as shown in Table 20-5.

Here, you can configure a new AUP for a user identity group on the Acceptable Use Policy Configurations page.

Step 7 Click **Submit** to create an AUP configuration.

Step 8 Click **Cancel** to return to the Acceptable Use Policy Configurations page from the Acceptable Use Policy Configuration page when you do not want to add a new AUP from this page.

To delete an acceptable use policy, complete the following steps:

Step 1 From the Settings menu window, choose **Posture**.

Step 2 Click the arrow to view the settings used for posture.

Step 3 Choose **Acceptable Use Policy**.

The Acceptable Use Policy Configurations page appears, which lists all the AUPs that you have already created.

Step 4 Choose an acceptable use policy that you want to delete.

Step 5 From the Acceptable Use Policy Configurations page, choose **Delete**.

A confirmation dialog appears with the following message: “Are you sure you want to delete?”.

Step 6 Click **OK** to delete an AUP.

Here, you can delete an AUP.

Step 7 Click **Cancel** to return to the Acceptable Use Policy Configurations page without deleting the AUP that you selected.

Table 20-5 describes the fields that allow to create an AUP configuration on the Acceptable use policy configurations page.

Table 20-5 AUP Configurations

Field	Field Description
Configuration Name	From the Configuration Name field, enter the name of the AUP configuration that you want to create.

Table 20-5 AUP Configurations (continued)

Field	Field Description
Configuration Description	From the Configuration Description field, enter the description of the AUP configuration that you want to create.
Show AUP to Agent users (for NAC Agent and Web Agent on Windows only)	If checked, the Show AUP to Agent users check box displays end users (for NAC Agents, and Web Agents on Windows only) the link to network usage terms and conditions for your network, and then click it to view the AUP upon successful authentication and posture assessment.
Use URL for AUP message radio button	When selected, you must enter the URL to the AUP message in the AUP URL field, which clients must access upon successful authentication and posture assessment.
Use file for AUP message radio button	When selected, you must browse to the location and upload a file in a zipped format in the AUP File field, which contains the index.html at the top level. The zip file can include other files and sub directories in addition to the index.html file. These files can reference each other using HTML tags.
AUP URL	From the AUP URL field, enter the URL to the AUP, which clients must access upon successful authentication and posture assessment.
AUP File	From the AUP File field, browse to the file and upload it to the Cisco ISE server. It should be a zipped file and the zipped file should contain the index.html at the top level.
Select User Identity Groups	From the Select User Identity Groups field, choose a unique user identity group, or a unique combination of user identity groups, for your AUP configuration. Note the following while creating an AUP configuration: • Posture AUP is not applicable for a guest flow • Each configuration must have a unique user identity group, or a unique combination of user identity groups • No two configurations have any user identity group in common • If you want to create a AUP configuration with a user identity group “Any”, then delete all other AUP configurations first • If you create a AUP configuration with a user identity group “Any”, then you cannot create other AUP configurations with a unique user identity group, or user identity groups. To create an AUP configuration with a user identity group other than Any, either delete an existing AUP configuration with a user identity group “Any” first, or update an existing AUP configuration with a user identity group “Any” with a unique user identity group, or user identity groups.

Table 20-5 AUP Configurations (continued)

Field	Field Description
Acceptable use policy configurations—Configurations list	An area that lists existing AUP configurations and end user identity groups associated to AUP configurations.

Filtering Acceptable Use Policies

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Acceptable Use Policy Configurations page. A quick filter is a simple and quick filter that can be used to filter acceptable use policies on the Acceptable Use Policy Configurations page. It filters acceptable use policies based on the field description such as the name of the acceptable use policies, description, URL of the acceptable use policy, user identity groups to which acceptable use policies are configured, acceptable use policies that are enabled, or disabled on the Acceptable Use Policy Configurations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Acceptable Use Policy Configurations page. It filters acceptable use policies based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the filtered results on the Acceptable Use Policy Configurations page. You can also edit preset filters and remove them from the preset filters list.

To filter acceptable use policies, complete the following steps:

Step 1 Choose **Administration > System > Settings > Settings** (menu window).

Step 2 From the Settings menu window, choose **Posture**.

Step 3 Click the arrow to view the settings used for posture.

Step 4 Choose **Acceptable Use Policy**.

The Acceptable Use Policy Configurations page appears, which lists all the AUPs that you have already created.

Step 5 From the Acceptable Use Policy Configurations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-6.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-30 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-30.

Note To return to the Acceptable Use Policy Configurations page, choose **All** from the Show drop-down to display all the acceptable use policies without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters acceptable use policies based on each field description on the Acceptable Use Policy Configurations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Acceptable Use Policy Configurations page. If you clear the field, it displays the list of all the acceptable use policies on the Acceptable Use Policy Configurations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter acceptable use policies by using variables that are more complex. It contains one or more filters, which filter acceptable use policies based on the values that match the field description. A filter on a single row filters acceptable use policies based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter acceptable use policies by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add the filtered lists, or click the **Remove Row** button (minus [-] sign) to remove the filtered lists.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

Step 8 The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-6 describes the fields that allow you to filter the AVPs:

Table 20-6 Filtering Acceptable Use Policy Configurations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter acceptable use policies by the name of the acceptable use policy.
	Description	This field enables you to filter acceptable use policies by the description of the acceptable use policy.
	Type	This field enables you to filter acceptable use policies by the type that a file is used, or the remote location of the acceptable use policy.
	File Name/URL	This field enables you to filter acceptable use policies by the file name that is used or the remote location of the acceptable use policy.
	User Identity Groups	This field enables you to filter acceptable use policies by the user identity groups configured for acceptable use policies.
	Enabled	This field enables you to filter acceptable use policies by AUPs that are configured to display, or not to Agent users (for NAC Agent and Web Agent on Windows only). • True—display AUP to Agent users • False—does not display AUP to Agent users
Advanced Filter	Choose the field description from the following: • Name • Description • Type • File Name/ URL • User Identity Groups • Enabled	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter acceptable use policies.
	Value	From the Value field, choose the value for the field description that you selected against which to filter acceptable use policies.

Client Posture Assessments in Cisco ISE

The posture service assists in determining the compliance of endpoints that are accessing your Cisco ISE-enabled network by using posture policies based on posture requirements, which are associated to posture policies. It evaluates the configured posture policies for all the endpoints that are connecting to your network, which are associated to one or more identity groups to which the users belong, and the operating systems that are installed on the clients. The NAC Agents that are installed on your clients interact with the Cisco ISE posture service, and evaluate the posture policies which are configured for your clients.

In addition, you should have an understanding on how Cisco ISE provides support for operating systems that are installed on the clients for posture.

Support for Hierarchical Operating Systems

Cisco ISE provides support to all the Windows and Macintosh operating systems, which are structured in a hierarchical group. You can also select an individual operating system from the hierarchy. A parent group includes the operating system versions for the group, and each version of the group includes the underlying operating system versions. When you select a parent group of an operating system from the hierarchy, you implicitly select all the underlying operating systems of the parent group. The posture conditions apply to all the underlying versions of the operating systems when you select the parent group or the group.

For example, when you choose Windows All from the Operating Systems field while creating a posture policy for posture in Cisco ISE, a condition that you define in the posture policy applies to all Microsoft Windows operating systems and their underlying operating systems, which includes Microsoft Windows 7 (All), Microsoft Windows Vista (All), Microsoft Windows XP (All), and their underlying operating systems for Windows All.

Filtering by Operating System

The selection of an operating system within the hierarchy implements the filtering of conditions, compound conditions and requirements that overrides a parent operating system Group associated to a simple condition. This implementation filters conditions, compound conditions and requirements by using the operating system that is associated with the compound condition. If you have a simple condition that is associated with a parent operating system group and a compound condition that is associated with the underlying version from the parent operating system group, then the filtering is based only on the underlying version of the operating system that is associated in the compound condition.

For example, you might have a simple condition that is associated with the Windows Vista parent operating system group. And you might also have a compound condition that is associated with the underlying version of Windows Vista from the operating system group. However, the filtering is done using only the underlying version of the operating system that is associated in the compound condition.

Dynamic Support for Operating System Version

You can configure the posture policies for an endpoint that is associated with the role to which you belong, as well as the operating system on the client. The posture configurations that you save apply only at the group level of an operating system that is not at the operating system level. This level of application allows you to map multiple versions of an operating system that is structured in the hierarchical groups.

For example, when you choose the Windows All option from the operating system group, you are choosing the hierarchical structure of all of the Windows 7, Windows Vista, and Windows XP groups that contain each of their underlying versions.

Cisco ISE dynamically supports new versions of client operating systems and Agents, including both the Windows and Macintosh NAC agents and NAC Web agent. Located on the ISE server, the osgroups.xml file is automatically updated by Cisco to reflect the latest version support information. If an Agent sends the Cisco ISE server an operating system version that is not listed in the osgroups.xml file, then you cannot continue to work with the posture service through the Agents.

Related Topics

- Client Posture Assessment Policies, page 20-33
- Client Posture Assessment Requirements, page 20-155

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

Client Posture Assessment Policies

A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. The Dictionary Attributes are optional conditions in conjunction with the identity groups, and the operating systems that allow you to define different policies for the clients.

Here, posture requirements are associated to the posture policies and also optional dictionary attributes where you can use dictionary simple and compound conditions from the library or create new dictionary simple and compound conditions.

Prerequisite:

You must have an understanding of acceptable use policy (AUP) and posture reassessments (PRA) as you create posture policies with respect to posture compliance.

For more information on AUP, see Posture Acceptable Use Policy, page 20-24 and on PRA, see Posture Reassessments, page 20-12.

In addition, see the following:

- Dictionary Simple Conditions, page 20-100
- Dictionary Compound Conditions, page 20-104
- Configuring Time and Date Conditions, page 17-23

You can use the Posture Policies page to insert (create) a new policy, or duplicate an existing policy, or delete an existing policy.

Table 20-7 describes the fields on the Posture Policies page that allow you to insert a new posture policy, or duplicate an existing policy. or delete an existing posture policy.

Table 20-7 Posture Policy

Field	Field Description
Status	From the Status field, click the drop-down arrow to choose an option. It can be used to enforce, or not to enforce a posture assessment policy for evaluation.
Rule Name	From the Rule Name field, enter the name of the posture policy that you want to create. Once created and saved, the name of the posture policy in not editable.

Table 20-7 Posture Policy (continued)

Field	Field Description
Identity Groups	From the Identity Groups field, choose an identity group. The selection of an identity group applies to the role of the user to which the user belongs in conjunction with the operating system that is installed on the client.
Operating Systems	From the Operating Systems field, choose an operating system. It allows you to select specific Windows, or Macintosh operating systems to which the posture requirement is applied.
Other Conditions	From the Other Conditions field, choose a dictionary simple condition, or a dictionary compound condition to which the posture requirement should apply. If more than one condition is selected, then all the conditions must be met to form a compound condition. The system uses "&" (a logical AND) as the AND operator.
Requirements	From the Requirements field, choose a posture requirement. The selection of a posture requirement that is associated to the matching posture policy determines the compliance of an endpoint during a posture policy evaluation.
Actions	It allows you to insert a new posture policy, duplicate an existing policy or delete an existing policy.

For information on how to manage posture policies, see the "Creating, Duplicating, and Deleting Client Posture Policies" section on page 20-35.

For more information on simplified posture policy configuration, see the "Simplified Posture Policy Configuration" section on page 20-34.

Simplified Posture Policy Configuration

This section describes the process to configure a posture policy in three steps on the Posture Policy page itself without navigating away to other configuration pages.

Once a posture policy is created on the Posture Policy page, posture conditions and remediation actions that you create on the Add Requirement widget are associated to the posture requirement, and posture requirements that you create on the Add Requirement widget are associated to the posture policy.

This section describes the process to configure a posture policy in three steps.

Simplified Posture Policy involves the following three steps:

Choose **Policy > Posture**. The Posture Policy page appears.

Step 1 From the Requirements field on the Posture Policy page, click the plus [+] sign to expand the Requirements anchored overlay. Click the minus [-] sign, or click outside the anchored overlay to close it.

Here, you can invoke the Requirements widget and create a new posture requirement from the Add Requirement widget. For more information, see the "Creating a New Posture Policy" section on page 20-35.

Step 2 From the Add Requirement widget, click the plus [+] sign to expand the Conditions anchored overlay. Click the minus [-] sign, or click outside the anchored overlay to close it.

Here, you can invoke the Conditions widget that lists user defined conditions and Cisco defined conditions separately.

You can create new conditions such as simple file, registry, application, service conditions, regular compound conditions, antivirus compound conditions, and antispyware compound conditions, and associate them to the requirement. You can also associate existing user defined simple and compound conditions that appear in the Conditions widget.

You can also choose Cisco defined conditions of file, registry, application, service conditions, regular compound conditions, antivirus compound conditions, and antispyware compound conditions, and associate them to the requirement.

For more information, see the "Creating a New Posture Requirement" section on page 20-157.

Step 3 From the Add Requirement widget, click the plus [+] sign to expand the Remediation Actions anchored overlay. Click the minus [-] sign, or click outside the anchored overlay to close it.

Here, you can invoke the Remediations widget that lists all the remediations that you have already created.

You can create new remediations such as file remediations, link remediations, launch program remediations, antivirus remediations, antispyware remediations, Windows Server Update Services remediations, and Windows Update remediations, and associate them to the requirement.

You can also choose existing remediations that appear on the Remediations widget.

For more information, see the "Creating a New Posture Requirement" section on page 20-157.

Once the posture conditions and posture remediations configuration is complete on the Add Requirement widget, the requirement is associated to the posture policy.

Creating, Duplicating, and Deleting Client Posture Policies

This section describes the following procedures on how to insert (create) a new policy, or duplicate an existing policy, or delete an existing policy on the Posture Policies page.

- Creating a New Posture Policy, page 20-35
- Duplicating a Posture Policy, page 20-40
- Deleting a Posture Policy, page 20-40

Creating a New Posture Policy

You can create a new posture policy on the Posture Policies page.

To create a new posture policy, complete the following steps:

Step 1 Choose **Policy > Posture**.

The Posture Policy page appears.

Step 2 Choose the **Status** type.

You can enforce a posture policy to be one of the following types:

- Enabled—this option allows you to enforce a posture policy for evaluation
- Disabled—this option allows you not to enforce a posture policy for evaluation

Step 3 From the Rule Name field, enter the policy name.

Step 4 From the Identity Groups field, choose **Select Role**.

The identity group anchored overlay appears.

To choose a role, complete the following steps:

a. From the Select Role field, click the plus [+] sign to expand the identity group anchored overlay.

The identity group anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the Select Role **Quick Picker** (down arrow) icon.

The Roles widget appears. The Table view button shows the roles that lists Any and the User Identity Groups in a row format in the right pane of the widget. The Tree view button shows Any and the User Identity Groups in a tree format.

c. From the Roles widget, choose the role.

d. Click the **Add** (plus [+] sign) button to associate more than one role to the policy.

e. Click the **Remove** (minus [-] sign) button to remove the role from the policy.

Step 5 From the Operating Systems field, choose **Select Operating Systems**.

The operating system anchored overlay appears.

To choose an operating system, complete the following steps:

a. From the Select Operating System field, click the plus [+] sign to expand the operating system anchored overlay.

The operating system anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the Select Operating System **Quick Picker** (down arrow) icon.

The Operating System Groups widget appears. The Table view button shows MAC OSX and Windows All operating system groups and their underlying versions in a row format in the right pane of the widget. The Tree view button shows MAC OSX and Windows All operating system groups and their underlying versions in a tree format.

Here, you cannot choose both the operating system types.

c. From the Operating System Groups widget, choose either **MAC OSX** or **Windows All**.

Here, click the **Quick Picker** (right arrow) icon to view the operating system groups.

Mac OS X (Macintosh) has three underlying versions.

- From the Mac OS X (Macintosh) group, choose the underlying Macintosh operating system.

Or

Windows has Windows 7 (All), Windows Vista (All), and Windows XP (All) groups and each group contains underlying versions.

- From the Windows All group, choose the underlying Windows group and the Windows version. Each Windows group contains its own underlying versions.

d. Click the **Add** (plus [+] sign) button to associate more than one operating system to the policy.

e. Click the **Remove** (minus [-] sign) button to remove the operating system from the policy.

Step 6 From the Other Conditions field, choose **(Optional) Dictionary Attributes**.

The conditions anchored overlay appears, which allows you an option to add new one or more dictionary attributes, and save them as simple, and compound conditions to a dictionary (a library). You can use an AND, or OR operator to form a dictionary compound condition, and then save them to the dictionaries. From the Other Conditions field, you can choose dictionary simple, and compound conditions from the library for validation during posture policies evaluation.

Note Dictionary simple conditions and dictionary compound conditions that you create on the Posture Policy page, Policy > Policy Elements > Conditions > Dictionary Simple Conditions page and Policy > Policy Elements > Conditions > Dictionary Compound Conditions page are not visible while configuring an authorization policy.

To choose a condition, complete the following steps:

a. From the (Optional) Dictionary Attributes field, click the plus [+] sign to expand the conditions anchored overlay. Click the minus [-] sign, or click outside the anchored overlay to close it.

   A widget displays Select Existing Condition from Library and Create New Condition (Advance Option).

   Select Existing Condition from Library—You can define an expression by selecting predefined conditions from the policy elements library. You can add ad-hoc attribute/value pairs to your expression in the subsequent steps.

   Create New Condition (Advance Option)—You can define an expression by selecting attributes from various system or user-defined dictionaries. You can add pre-defined conditions from the policy elements library in the subsequent steps.

b. Choose **Select Existing Condition from Library**.

c. Click the Select Conditions **Quick Picker** (down arrow) icon.

   The Dictionaries widget appears, which lists the dictionary simple conditions and dictionary compound conditions.

d. Choose the condition.

e. Choose an **AND** operator or an **OR** operator from the drop-down list.

f. Click the **Action Icon** button to add a new dictionary attribute and its value, add a condition from the library, or delete the existing conditions or dictionary attributes.

   Here, you can do the following:

   - Add Attribute/Value
   - Add Condition from Library
   - Delete

g. Click the **Save** icon to add all the conditions below to the library from the conditions overlay.

To choose a dictionary attribute (optional), complete the following steps:

a. From the (Optional) Dictionary Attributes field, click the plus [+] sign to expand the conditions anchored overlay. Click the minus [-] sign, or click outside the anchored overlay to close it.

   A widget displays Select Existing Condition from Library and Create New Condition (Advance Option)

b. Choose **Create New Condition (Advance Option)**.

   The conditions anchored overlay appears. It allows you to create a new dictionary simple condition or dictionary compound condition (an expression).

c. From the Expression field, click the Select Attribute **Quick Picker** (down arrow) icon.

   The Dictionaries widget appears that lists the following dictionaries:

   - AD1
   - DEVICE
   - Network Access
   - Radius
   - Session

d. From the Dictionaries widget, choose an existing dictionary.

e. Click the navigation arrow (right arrow) to view the dictionary attributes.

   The dictionary attributes appear for the dictionary.

f. Choose a dictionary attribute.

g. Choose an operator, and a value to create a dictionary simple condition.

h. Click the **Action Icon** button to add a dictionary simple condition to a library.

   Enter a name for that dictionary simple condition to be saved to the library.

i. Click the **Action Icon** button to add a new dictionary attribute and its value, add a condition from the library, duplicate a condition, add a condition to the library, or delete the existing conditions or dictionary attributes.

   Here, you can do the following:

   - Add Attribute/Value
   - Add Condition from Library
   - Duplicate
   - Add Condition to Library
   - Delete

j. Choose an **AND** operator or an **OR** operator from the drop-down list to create a dictionary compound condition.

k. Click the **Save** icon to add all the conditions from the conditions anchored overlay to the library.

   Here, you can define an expression by selecting attributes from various system, or user-defined dictionaries. You can create a new dictionary simple condition (an expression) by adding a new dictionary attribute and associating a value, which can be saved to the policy elements library. You can also add pre-defined conditions from the policy elements library in the subsequent steps.

   Session Agent-Request-Type

   The Session dictionary that you choose from the Dictionaries widget has the following attributes and values.

   - Agent-Request-Type—Initial and Periodic Reassessment are the values.
   - OS-Architecture—32-bit and 64-bit are the values.
   - URL-Redirected—Specify the value.

   By default, all the matching posture requirements are validated upon initial posture assessment and then periodically according to the periodic reassessments that are defined for posture assessment of clients. The Session attribute Agent-Request-Type can be used in the posture policy to selectively apply posture requirements either during initial posture assessment or during periodic reassessments of clients.

- To apply a matching posture requirement during initial posture assessment only, set the Session Agent-Request-Type attribute EQUAL to Initial.
- To apply a matching posture requirement during periodic reassessment only, set the Session Agent-Request-Type attribute EQUAL to Periodic Reassessment.
- To apply a matching posture requirement to both the initial posture assessment and periodic reassessments, then do not set the Session Agent-Request-Type attribute in the posture policy.

Step 7 From the Requirements field, choose **Select Requirement**.

To choose a requirement, complete the following steps:

a. From the Select Requirement field, click the plus [+] sign to expand the requirements anchored overlay.

The requirements anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

You can enforce a posture requirement to be one of the following items types:

Mandatory—This option enforces the client to meet the posture requirement. The user cannot proceed or have access to the network unless the client meets the posture requirement.

Optional—This option does not enforce the client to meet the posture requirement. The client can bypass the requirement, if required. The client does not require to meet the requirement for the user to proceed or have network access.

Audit—This option checks the client for the posture requirement without notifying the user. It does not affect user network access.

b. Click the Select Requirement **Quick Picker** (down arrow) icon.

The Requirements widget appears.

c. Choose a requirement.

d. Click the **Add** (plus [+] sign) button to associate more than one requirement to the posture policy.

e. Click the **Remove** (minus [-] sign) button to remove the requirement from the posture policy.

To create a requirement, complete the following steps:

a. From the Requirements field, choose **Select Requirement**.

b. From the Select Requirement field, click the plus [+] sign to expand the requirements anchored overlay.

The requirements anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

You can enforce a posture requirement to be one of the following items types:

Mandatory—This option enforces the client to meet the posture requirement. The user cannot proceed or have access to the network unless the client meets the posture requirement.

Optional—This option does not enforce the client to meet the posture requirement. The client can bypass the requirement, if required. The client does not require to meet the requirement for the user to proceed or have network access.

Audit—This option checks the client for the posture requirement without notifying the user. It does not affect user network access.

c. Click the Select Requirement **Quick Picker** (down arrow) icon.

The Requirements widget appears.

d. Click the **Quick Picker** (down arrow) on the **Action** button.

e. Choose **Create Requirement**.

The Add Requirement widget appears. Here, you can configure the posture requirement from the Posture Policy page where you can associate posture conditions and posture remediation actions for that requirement.

Step 8 Click **Save** to save the posture policy. Click **Cancel** to revert to the Posture Policy page without creating a new policy on the Posture Policy page.

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

Duplicating a Posture Policy

You can create a copy of the posture policy that you want to duplicate on the Posture Policies page.

To duplicate a policy, complete the following steps:

Step 1 Click the **Action Icon** button.

Step 2 Choose **Duplicate**.

Here, you can create a copy of the policy that you want to duplicate on the Posture Policies page.

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

Deleting a Posture Policy

You can also delete a posture policy from the Posture Policies page.

To delete a policy, complete the following steps:

Step 1 Click the **Action Icon** button.

Step 2 Choose **Delete**.

A confirmation dialog appears with the following message: “Are you sure you want to delete Policy(s)?”.

Step 3 Click **OK** to delete a policy.

Here, you can delete a posture policy from the Posture Policies page.

Step 4 Click **Cancel** to return to the Posture Policies page without deleting the posture policy.

Posture Assessment and Remediation Options in Cisco ISE

The NAC Agent and the Web Agent for Windows provide the posture assessment and remediation for Windows clients, and the NAC Agent for Macintosh provide the posture assessment and remediation for Macintosh clients. Before you begin to configure custom conditions and remediation actions in Cisco ISE, you must understand the posture assessment and remediation types that are supported by the NAC Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 20-8 provides the list of posture assessment (checks) and remediation options that are supported by the NAC Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 20-8 Posture Assessment and Remediation Options

	NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Posture Assessments			
Operating System/Service Packs/Hotfixes	*	*	Not Applicable
Process Check	*	*	Not Applicable
Registry Check	*	*	Not Applicable
File Check	*	*	Not Applicable
Application Check	*	*	Not Applicable
Antivirus Installation	*	*	*
Antivirus Version/ Antivirus Definition Date	*	*	*
Antispyware Installation	*	*	*
Antispyware Version/ Antispyware Definition Date	*	*	*
Windows Update Running	*	*	Not Applicable
Windows Update Configuration	*	*	Not Applicable
WSUS Compliance Settings	*	*	Not Applicable
Posture Remediations			
Message Text (Local Check)	*	*	*
URL Link (Link Distribution)	*	*	*
File Distribution	*	*	Not Applicable
Launch Program	*	Not Applicable	Not Applicable

Table 20-8 Posture Assessment and Remediation Options (continued)

	NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Antivirus Definition Update	*	Not Applicable	Antivirus Live Update
Antispyware Definition Update	*	Not Applicable	Antispyware Live Update
Windows Update	*	Not Applicable	Not Applicable
WSUS	*	Not Applicable	Not Applicable

Custom Conditions for Posture

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated to a posture requirement.

User Defined Conditions and Cisco Defined Conditions

Cisco ISE redefines posture conditions into either user defined conditions that you create on their respective conditions list pages or Cisco defined conditions.

After an initial posture update, Cisco ISE creates the following user defined AV compound conditions and AS compound conditions:

- ANY_av_mac_def—Any AV definition check on MAC
- ANY_av_mac_inst—Any AV installation check on MAC
- ANY_av_win_def—Any AV definition check on Windows
- ANY_av_mac_inst—Any AV installation check on Windows
- ANY_as_mac_def—Any AS definition check on MAC
- ANY_as_mac_inst—Any AS installation check on MAC
- ANY_as_win_def—Any AS definition check on Windows
- ANY_as_mac_inst—Any AS installation check on Windows

After an initial posture update, Cisco ISE also creates Cisco defined simple and compound conditions. Cisco defined simple file, registry, application, and service conditions have pc_ as their prefixes, and compound conditions have pr_ as their prefixes.

Note The conditions that appear in the **Policy > Policy Elements > Conditions > Posture > AV Compound Conditions** or **AS Compound Conditions** page may vary as follows:

- If you have performed a new installation of Cisco ISE, Release 1.1 and have not performed a compliance module update, this display will be empty.

- If you have performed a new installation of Cisco ISE, Release 1.1 and perform a compliance module update, Cisco ISE displays the appropriate antivirus or antispyware subset of the list above.
- If you have updated from an earlier release of Cisco ISE to release 1.1 and perform a compliance module update, Cisco ISE displays the appropriate antivirus or antispyware subset of the list above in addition to many other vendor specific conditions carried over from the earlier release database.

A user defined condition or a Cisco defined condition includes both simple conditions such as a file condition, a registry condition, an application condition, and a service condition, as well as compound conditions such as a regular compound condition, an antivirus compound condition, and an antispyware compound condition.

You can use the Posture menu to manage the following posture simple conditions:

- File Conditions—A simple condition that checks the existence of a file, the date of a file, and the versions of a file on the client
- Registry Conditions—A simple condition that checks for the existence of a registry key or the value of the registry key on the client
- Application Conditions—A simple condition that checks if an application (process) is running or not running on the client
- Service Conditions—A simple condition that checks if a service is running or not running on the client
- Dictionary Simple Conditions—A simple condition that checks an attribute associated to an operator and the operator to a value



Note A simple condition cannot be deleted due to Referential Integrity errors in Cisco ISE when it is associated to one or more compound conditions. As simple conditions can be associated to a compound condition, you cannot delete the following simple conditions: a file, a registry, an application, a service, and a dictionary simple condition. If you attempt to delete a simple condition, Cisco ISE throws an error message stating that the compound conditions need to be updated, or deleted first to which simple conditions are associated.



Note You cannot delete, or edit Cisco defined posture simple conditions.

You can use the Posture menu to manage the following posture compound conditions:

- Compound Conditions—contains one or more simple conditions, or compound conditions of the type File, Registry, Application, or Service condition
- Antivirus Compound Conditions—contains one or more AV conditions, or AV compound conditions
- Antispyware Compound Conditions—contains one or more AS conditions, or AS compound conditions
- Dictionary Compound Conditions—contains one or more dictionary simple conditions or dictionary compound conditions

Note A compound condition cannot be deleted due to Referential Integrity errors in Cisco ISE. As compound conditions can be associated to a posture requirement, you cannot delete the following compound conditions: a compound condition, an antivirus, an antispyware, and a dictionary compound condition. If you attempt to delete a compound condition, Cisco ISE throws an error message stating that the posture requirements need to be updated, or deleted first to which compound conditions are associated.

Note You cannot delete, or edit Cisco defined posture compound conditions.

File Conditions

A file condition is a simple (single) condition that checks for a file by its existence on the client, or its date when created, or modified on the client, or its version that exists on the client. You can create FileExistence, FileDate, and FileVersion types of file conditions to check the compliance of the file on the client. The FileExistence type checks the existence of a file on the client. The FileDate type checks the file based on its file-created date, or file-modified date on the client. The FileVersion type checks for the specific version of the file that you define in the file condition. When you create a file condition on the File condition list page, you can see the fields change to provide details according to your input.

The File Conditions page displays file conditions along with their names and description. It also displays the names of the files to be checked for each of the file condition type.

Note Cisco defined file conditions that are listed on the File Conditions page are not editable.

This section provides the procedures that you can use to configure file conditions.

- Configuring File Conditions, page 20-44

Configuring File Conditions

You can create any one of the following types of a file condition on the File Conditions page: FileExistence, FileDate, and FileVersion. You can also duplicate, edit, delete, or filter file conditions from the File Conditions page.

This section covers the following procedures:

- Viewing File Conditions, page 20-44
- Creating, Duplicating, Editing, and Deleting a File Condition of FileExistence Type, page 20-45
- Creating, Duplicating, Editing, and Deleting a File Condition of FileDate Type, page 20-47
- Creating, Duplicating, Editing, and Deleting a File Condition of FileVersion Type, page 20-50
- Filtering File Conditions, page 20-53

Viewing File Conditions

You can use the File Conditions page to view file conditions.

To view file conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Choose a file condition from the file conditions list.

Step 6 Click **View**.

Here, you can choose a file condition to view the details.

Creating, Duplicating, Editing, and Deleting a File Condition of FileExistence Type

You can use the File Conditions page to create, duplicate, edit, or delete a file condition of FileExistence type, which allows you to check that a file exists on the client, or does not exist on the client.

To create a file condition of FileExistence type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the file condition is not editable.**

Step 6 Modify the values on the New File Condition page, as shown in Table 20-9.

Here, you can create to add a file condition of FileExistence type, which appears on the File Conditions page.

Step 7 Click **Submit** to create a file condition of FileExistence type.

To duplicate a file condition of FileExistence type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to duplicate.

Step 3 From the File Conditions page, choose **Duplicate**.

Here, you can create a copy of the file condition of FileExistence type.

Step 4 Click **Submit** to create a copy of the file condition of FileExistence type.

To edit a file condition of FileExistence type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to edit.

Step 3 From the File Conditions page, choose **Edit**.

Here, you can edit a file condition of FileExistence type.

Step 4 Click **Save** to save the changes to the file condition of FileExistence type.

The file condition of FileExistence type will be available on the File Conditions page after editing on the edit page.

Step 5 Click the **File Conditions List** link from the edit page to return to the File Conditions page.

To delete a file condition of FileExistence type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to delete.

Step 3 From the File Conditions page, choose **Delete**.

Here, you can delete a file condition of FileExistence type.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-9 describes the fields on the New File Condition page that allow you to create, duplicate, or edit a file condition on its edit page of FileExistence type condition.

Table 20-9 File Condition of FileExistence Type

Field Name	Field Description
Name	From the Name field, enter the name of a file condition that you want to create.
Description	From the Description field, enter a description of the file condition that you want to create.
File Path	From the File Path field, this option allows you to check the existence of a file in the location you specify. Click the drop-down arrow to view the following predefined settings: • ABSOLUTE_PATH—checks the file in the fully qualified path of the file. For example, C:\<directory>\file name. For other settings, enter only the file name. • SYSTEM_32—checks the file in the C:\WINDOWS\system32 directory. Enter the file name. • SYSTEM_DRIVE—checks the file in the C:\ drive. Enter the file name. • SYSTEM_PROGRAMS—checks the file in the C:\Program Files. Enter the file name. • SYSTEM_ROOT—checks the file in the root path for Windows system. Enter the file name.
File Type	From the File Type field, selecting a File Type allows you to check a file for the existence of a file on the client, file-created or file-modified date of the file, and its version. Click the drop-down arrow to view the following predefined settings: • FileExistence—checks whether a file exists on the system. • FileDate—checks whether a file with a particular file-created or file-modified date exists on the system. • FileVersion—checks whether a particular version of a file exists on the system.
File Operator	From the File Operator field, selecting an operator allows you to check the existence of a file in the specified location. Click the drop-down arrow to view the following predefined settings. • Exists • DoesNotExist
Operating System	From the Operating System field, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Creating, Duplicating, Editing, and Deleting a File Condition of FileDate Type

You can use the File Conditions page to create, duplicate, edit, or delete a file condition of FileDate type by using file-created, or file-modified date.

To create a File Condition of FileDate type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the file condition is not editable.**

Step 6 Modify the values on the New File Condition page**,** as shown in Table 20-10.

Here, you can create a file condition of FileDate type with file-created date or file-modified date.

Step 7 Click **Submit** to create a file condition of FileDate type.

To duplicate a file condition of FileDate type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to duplicate.

Step 3 From the File Conditions page, choose **Duplicate**.

Here, you can create a copy of the file condition of FileDate type.

Step 4 Click **Submit** to create a copy of the file condition of FileDate type.

To edit a file condition of FileDate type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to edit.

Step 3 From the File Conditions page, choose **Edit**.

Here, you can edit a file condition of FileDate type.

Step 4 Click **Save** to save the changes to the file condition of FileDate type.

The file condition of FileDate type will be available on the File Conditions page after editing on the edit page.

Step 5 Click the **File Conditions List** link from the edit page to return to the File Conditions page.

To delete a file condition of FileDate type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to delete.

Step 3 From the File Conditions page, choose **Delete**.

Here, you can delete a file condition of FileDate type.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-10 describes the fields on the New File Condition page that allow you to create, duplicate, or edit a file condition on its edit page of FileDate type condition.

Table 20-10 File Condition of FileDate Type

Field Name	Field Description
Name	From the Name field, enter the name of a file condition that you want to create.
Description	From the Description field, enter the description of a file condition that you want to create
File Path	From the File Path field, this option allows you to check the existence of a file in the location you specify. Click the drop-down arrow to view the following predefined settings: • ABSOLUTE_PATH—checks the file in the fully qualified path of the file. For example, C:\<directory>\file name. For other settings, enter only the file name. • SYSTEM_32—checks the file in the C:\WINDOWS\system32 directory. Enter the file name. • SYSTEM_DRIVE—checks the file in the C:\ drive. Enter the file name. • SYSTEM_PROGRAMS—checks the file in the C:\Program Files. Enter the file name. • SYSTEM_ROOT—checks the file in the root path for Windows system. Enter the file name.

Table 20-10 File Condition of FileDate Type (continued)

Field Name	Field Description
File Type	From the File Type field, selecting a File Type allows you to check a file for the existence of the file on the client, file-created or file-modified date of the file, and its version. Click the drop-down arrow to view the following predefined settings: • FileExistence—checks whether a file exists on the system. • FileDate—checks whether a file with a particular file-created or file-modified date exists on the system. • FileVersion—checks whether a particular version of a file exists on the system.
File Date Type	From the File Date Type field, selecting the date type allows you to check the existence of a file with a particular file-created or file-modified date. Click the drop-down arrow to view the following predefined settings: • Creation Date • Modification Date
Operator	From the Operator field, selecting an operator allows you to check the existence of a file with a particular date or version. Click the drop-down arrow to view the following predefined settings: • EarlierThan • LaterThan • EqualTo
Date and Time	From the Date and Time fields, entering date and time of the client system, which is expressed in mm/dd/yyyy [hh:mm:ss] format allows you to check the existence of a file with date and time of the client system.
Operating System	From the Operating System field, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Creating, Duplicating, Editing, and Deleting a File Condition of FileVersion Type

You can use the File Conditions page to create, duplicate, edit, or delete a file condition of FileVersion type that has more than one version.

To create a file condition of FileVersion type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the file condition is not editable.**

Step 6 Modify the values on the New File Condition page**,** as shown in Table 20-11.

Here, you can create a file condition of FileVersion type, where the file has more than one version.

Step 7 Click **Submit** to create a file condition of FileVersion type.

To duplicate a file condition of FileVersion type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to duplicate.

Step 3 From the File Conditions page, choose **Duplicate**.

Here, you can create a copy of the file condition of FileVersion type.

Step 4 Click **Submit** to create a copy of the file condition of FileVersion type.

To edit a file condition of FileVersion type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to edit.

Step 3 From the File Conditions page, choose **Edit**.

Here, you can edit a file condition of FileVersion type.

Step 4 Click **Save** to save the changes to the file condition of FileVersion type.

A file condition of FileVersion type will be available on the File Conditions page after editing on the edit page.

Step 5 Click the **File Conditions List** link from the edit page to return to the File Conditions page.

To delete a file condition of FileVersion type, complete the following steps:

Step 1 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists predefined Cisco file conditions and all the file conditions that you have already created.

Step 2 Choose the file condition that you want to delete.

Step 3 From the File Conditions page, choose **Delete**.

Here, you can delete a file condition of FileVersion type.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-11 describes the fields on the New File Condition page that allow you to create, duplicate, or edit a file condition on its edit page of FileVersion type condition.

Table 20-11 File Condition of FileVersion Type

Field Name	Field Description
Name	From the Name field, enter the name of a file condition that you want to create.
Description	From the Description field, enter the description of a file condition that you want to create
File Path	From the File Path field, this option allows you to check the existence of a file in the location you specify. Click the drop-down arrow to view the following predefined settings: • ABSOLUTE_PATH—checks the file in the fully qualified path of the file. For example, C:\<directory>\file name. For other settings, enter only the file name. • SYSTEM_32—checks the file in the C:\WINDOWS\system32 directory. Enter the file name. • SYSTEM_DRIVE—checks the file in the C:\ drive. Enter the file name. • SYSTEM_PROGRAMS—checks the file in the C:\Program Files. Enter the file name. • SYSTEM_ROOT—checks the file in the root path for Windows system. Enter the file name.
File Type	From the File Type field, selecting a File Type allows you to check a file for the existence of the file on the client, file-created or file-modified date of the file, and its version. Click the drop-down arrow to view the following predefined settings: • FileExistence—checks whether a file exists on the system. • FileDate—checks whether a file with a particular file-created or file-modified date exists on the system. • FileVersion—checks whether a particular version of a file exists on the system.
Operator	From the Operator field, selecting an operator allows you to check the existence of a file with a particular date or version. Click the drop-down arrow to view the following predefined settings: • EarlierThan • LaterThan • EqualTo

Table 20-11 File Condition of FileVersion Type (continued)

Field Name	Field Description
File Version	From the File Version field, enter the version of the file that allows you to check the existence of a file with a particular version of the file.
Operating System	From the Operating System field, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Filtering File Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the File Conditions page. A quick filter is a simple and quick filter that can be used to filter file conditions on the File Conditions page. It filters file conditions based on the field description such as the name of the file conditions, description, and the file to be checked on the File Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the File Conditions page. It filters file conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the File Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter file conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **File Condition**.

The File Conditions page appears, which lists all the file conditions that you have already created.

Step 5 From the File Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-12.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-54 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-54.

Note To return to the File Conditions page, choose **All** from the Show drop-down to display all the file conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters file conditions based on each field description on the File Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the File Conditions page. If you clear the field, it displays the list of all the file conditions on the File Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter file conditions by using variables that are more complex. It contains one or more filters, which filter file conditions based on the values that match the field description. A filter on a single row filters file conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter file conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove a filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-12 describes the fields that allow you to filter file conditions on the File Conditions page.

Table 20-12 Filtering File Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter file conditions by the condition name.
	Description	This field enables you to filter file conditions by the condition description.
	Field Name	This field enables you to filter file conditions by the filename.
	Condition Type	This field enables you to filter file conditions by Cisco predefined and not Cisco predefined conditions.

Table 20-12 Filtering File Conditions (continued)

Filtering Method	Filtering Field	Filtering Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • File Name • Condition Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter file conditions.
	Value	From the Value field, choose the value for the field description that you selected against which to filter file conditions.

Registry Conditions

A registry condition is a simple (single) condition that checks a registry key or the value of the registry on the client. You can create RegistryKey, RegistryKeyValue, and RegistryValueDefault types of registry conditions to check the compliance of the client on a registry. The RegistryKey type checks the existence of a registry on the client, and the RegistryKeyValue type checks the data of the registry key on the client. The RegistryValueDefault is the same as the RegistryKeyValue except that the former checks for the default value. When you create a registry condition on the Registry Conditions page, you can see the fields change to provide details according to your input.

The Registry Conditions page displays registry conditions along with their names, description, and the type of registry conditions.

Note Cisco predefined registry conditions that are listed on the Registry Conditions page are not editable.

This section provides the procedure that you can use to configure registry conditions.

- Configuring Registry Conditions, page 20-55

Configuring Registry Conditions

You can create any one of the following types of a registry condition on the Registry Conditions page: RegistryKey, RegistryKeyValue, and RegistryValueDefault types. You can also duplicate, edit, delete, or filter the registry conditions from the Registry Conditions page.

This section covers the following procedures:

- Viewing Registry Conditions, page 20-56
- Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryKey Type, page 20-56

- Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValue Type, page 20-59
- Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValueDefault Type, page 20-63
- Filtering Registry Conditions, page 20-66

Viewing Registry Conditions

You can use the Registry Conditions page to view registry conditions.

To view registry conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Choose a registry condition from the registry conditions list.

Step 6 Click **View**.

Here, you can choose a registry condition to view the details.

Step 7 Click the **Registry Conditions List** link to return to the Registry Conditions page.

Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryKey Type

You can use the Registry Conditions page to create, duplicate, edit, or delete a registry condition of RegistryKey type, which allows you to check the existence of a registry on the client.

To create a registry condition of RegistryKey type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the registry condition is not editable.**

Step 6 Modify the values on the New Registry Condition page, as shown in Table 20-13.

Here, you can create to add a registry condition of RegistryKey type, which appears on the Registry Conditions page.

Step 7 Click **Submit** to create a registry condition of RegistryKey type.

To duplicate a registry condition of RegistryKey type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to duplicate.

Step 3 From the Registry Conditions page, choose **Duplicate**.

Here, you can create a copy of the registry condition of RegistryKey type.

Step 4 Click **Submit** to create a copy of the registry condition of RegistryKey type.

To edit a registry condition of RegistryKey type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to edit.

Step 3 From the Registry Conditions page, choose **Edit**.

Here, you can edit a registry condition of RegistryKey type.

Step 4 Click **Save** to save the changes to the registry condition of RegistryKey type.

A registry condition of RegistryKey type will appear on the Registry Conditions page after editing on the edit page.

Step 5 Click the **Registry Conditions List** link from the edit page to return to the Registry Conditions page.

To delete a registry condition of RegistryKey type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists predefined Cisco registry conditions and all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to delete.

Step 3 From the Registry Conditions page, choose **Delete**.

Here, you can delete a registry condition of RegistryKey type.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-13 describes the fields on the New Registry Condition page that allow you to create, duplicate, or edit a registry condition on its edit page of RegistryKey type condition.

Table 20-13 Registry Condition for RegistryKey

Field Name	Field Description
Name	From the Name field, enter the name of the registry condition that you want to create.
Description	From the Description field, enter the description of the registry condition that you want to create.
Registry Type	From the Registry Type field, selecting a Registry Type allows you to check the existence of the registry key in the client registry, or the value of the registry key. Click the drop-down arrow to view the following predefined settings: • RegistryKey—Checks whether a specific registry key exists in the registry. • RegistryValue—Checks whether a named registry key exists or has a particular value, version, or modification date. • RegistryValueDefault—Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
Registry Root Key	From the Registry Root Key field, selecting a Registry Root Key allows you to check the registry key, or the value of the registry key in the client registry from the root. Click the drop-down arrow to view the following Registry Root Key locations: • HKEY_LOCAL_MACHINE (HKLM) • HKEY_CURRENT_CONFIG (HKCC) • HKEY_CURRENT_USER (HKCU) • HKEY_USERS (HKU) • HKEY_CLASSES_ROOT (HKCR)
Sub Key	From the Sub Key field, selecting a sub key without the leading backslash (“\”) allows you to check the registry key and the registry key value in the path specified in the sub key. For example, SOFTWARE\Symantec\Norton AntiVirus\version from HKLM\SOFTWARE\Symantec\Norton AntiVirus\version

Table 20-13 Registry Condition for RegistryKey (continued)

Field Name	Field Description
Value Operator	From the Value Operator field, selecting an operator allows you to check the existence or nonexistence of the registry key and the registry key value. Click the drop-down arrow to view the following settings: • Exists • DoesNotExist
Operating System	From the Operating System field, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValue Type

You can use the Registry Conditions page to create, duplicate, edit, or delete a registry condition of RegistryValue type.

To create a registry condition of RegistryValue type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the registry condition is not editable.**

Step 6 Modify the values on the New Registry Condition page, as shown in Table 20-14.

Here, you can create to add a Registry Condition of RegistryValue type, which appears on the Registry Conditions page.

Step 7 Click **Submit** to create a registry condition of RegistryValue type

To duplicate a registry condition of RegistryValue type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to duplicate.

Step 3 From the Registry Conditions page, choose **Duplicate**.

Here, you can create a copy of the registry condition of RegistryValue type.

Step 4 Click **Submit** to create a copy of the registry condition of RegistryValue type.

To edit a registry condition of RegistryValue type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to edit.

Step 3 From the Registry Conditions page, choose **Edit**.

Here, you can edit a registry condition of RegistryValue type.

Step 4 Click **Save** to save the changes to the registry condition of RegistryValue type.

A registry condition of RegistryValue type appears on the Registry Conditions page after editing on the edit page.

Step 5 Click the **Registry Conditions List** link from the edit page to return to the Registry Conditions page.

To delete a registry condition of RegistryValue type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to delete.

Step 3 From the Registry Conditions page, choose **Delete**.

Here, you can delete a registry condition of RegistryValue type.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-14 describes the fields on the New Registry Condition page that allow you to create, duplicate, or edit a registry condition on its edit page of RegistryValue type condition.

Table 20-14 Registry Condition for RegistryValue

Field Name	Field Description
Name	From the Name field, enter the name of the registry condition that you want to create.
Description	From the Description field, enter the description of the registry condition that you want to create.

Table 20-14 Registry Condition for RegistryValue (continued)

Field Name	Field Description
Registry Type	From the Registry Type field, selecting a Registry Type allows you to check the existence of the registry key in the client registry, or the value of the registry key. Click the drop-down arrow to view the following predefined settings: • RegistryKey—Checks whether a specific registry key exists in the registry. • RegistryValue—Checks whether a named registry key exists or has a particular value, version, or modification date. • RegistryValueDefault—Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
Registry Root Key	From the Registry Root Key field, selecting a Registry Root Key allows you to check the registry key, or the value of the registry key in the client registry from the root. Click the drop-down arrow to view the following Registry Root Key locations: • HKEY_LOCAL_MACHINE (HKLM) • HKEY_CURRENT_CONFIG (HKCC) • HKEY_CURRENT_USER (HKCU) • HKEY_USERS (HKU) • HKEY_CLASSES_ROOT (HKCR)
Sub Key	From the Sub Key field, selecting a sub key without the leading backslash (“\”) allows you to check the registry key and the registry key value in the path specified in the sub key. For example, SOFTWARE\Symantec\Norton AntiVirus\version from HKLM\SOFTWARE\Symantec\Norton AntiVirus\version
Value Name	From the Value Name field, enter the name of the registry key value against which you want to check in the client registry.
Value Data Type	From the Value Data Type field, selecting the data type allows you to check the registry key value data type, and its value using an operator. Click the drop-down arrow to view the predefined settings: • Unspecified—choose one of the operators in the drop-down list to check the existence of the registry key value • Number—choose one of the operators in the drop-down list to check the registry key value using a number in the registry key value • String—choose one of the operators in the drop-down list to check the registry key value using a string in the registry key value • Version—choose one of the operators in the drop-down list to check the registry key value using its version

Table 20-14 Registry Condition for RegistryValue (continued)

Field Name	Field Description
Registry Type	From the Registry Type field, selecting a Registry Type allows you to check the existence of the registry key in the client registry, or the value of the registry key. Click the drop-down arrow to view the following predefined settings: • RegistryKey—Checks whether a specific registry key exists in the registry. • RegistryValue—Checks whether a named registry key exists or has a particular value, version, or modification date. • RegistryValueDefault—Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
Registry Root Key	From the Registry Root Key field, selecting a Registry Root Key allows you to check the registry key, or the value of the registry key in the client registry from the root. Click the drop-down arrow to view the following Registry Root Key locations: • HKEY_LOCAL_MACHINE (HKLM) • HKEY_CURRENT_CONFIG (HKCC) • HKEY_CURRENT_USER (HKCU) • HKEY_USERS (HKU) • HKEY_CLASSES_ROOT (HKCR)
Sub Key	From the Sub Key field, selecting a sub key without the leading backslash (“\”) allows you to check the registry key and the registry key value in the path specified in the sub key. For example, SOFTWARE\Symantec\Norton AntiVirus\version from HKLM\SOFTWARE\Symantec\Norton AntiVirus\version
Value Name	From the Value Name field, enter the name of the registry key value against which you want to check in the client registry.
Value Data Type	From the Value Data Type field, selecting the data type allows you to check the registry key value data type, and its value using an operator. Click the drop-down arrow to view the predefined settings: • Unspecified—choose one of the operators in the drop-down list to check the existence of the registry key value • Number—choose one of the operators in the drop-down list to check the registry key value using a number in the registry key value • String—choose one of the operators in the drop-down list to check the registry key value using a string in the registry key value • Version—choose one of the operators in the drop-down list to check the registry key value using its version

Table 20-14 Registry Condition for RegistryValue (continued)

Field Name	Field Description
Value Operator	From the Value Operator field, selecting an operator allows you to check the existence or nonexistence of data type of the registry key value using an operator. Click the drop-down arrow to view the following settings: • Exists • DoesNotExist
Value Data	From the Value Data field, enter the value of the registry key for the data type of the registry that you select.
Operating System	From the Operating System field, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Creating, Duplicating, Editing, and Deleting a Registry Condition of RegistryValueDefault Type

You can use the Registry Conditions page to create, duplicate, edit, or delete a registry condition of RegistryValueDefault type.

To create a registry condition of RegistryValueDefault type, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the registry condition is not editable.**

Step 6 Modify the values on the New Registry Condition page, as shown in Table 20-15.

Here, you can create to add a Registry Condition of RegistryValueDefault type, which appears on the Registry Conditions page.

Step 7 Click **Submit** to create a registry condition of RegistryValueDefault type.

To duplicate a registry condition of RegistryValueDefault type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to duplicate.

Step 3 From the Registry Conditions page, choose **Duplicate**.

Here, you can create a copy of the registry condition of RegistryValueDefault type.

Step 4 Click **Submit** to create a copy of the registry condition of RegistryValueDefault type.

To edit a registry condition of RegistryValueDefault type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to edit.

Step 3 From the Registry Conditions page, choose **Edit**.

Here, you can edit a registry condition of RegistryValueDefault type.

Step 4 Click **Save** to save the changes to the registry condition of RegistryValueDefault type.

A registry condition of RegistryValueDefault type appears on the Registry Conditions page after editing on the edit page.

Step 5 Click the **Registry Conditions List** link from the edit page to return to the Registry Conditions page.

To delete a registry condition of RegistryValueDefault type, complete the following steps:

Step 1 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you have already created.

Step 2 Choose the registry condition that you want to delete.

Step 3 From the Registry Conditions page, choose **Delete**.

Here, you can delete a registry condition of RegistryValueDefault type.



Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-15 describes the fields on the New Registry Condition page that allow you to create, or edit a registry condition on its edit page of RegistryValueDefault type condition.

Table 20-15 Registry Condition for RegistryValueDefault

Field Name	Field Description
Name	From the Name field, enter the name of the registry condition that you want to create.
Description	From the Description field, enter the description of the registry condition that you want to create.
Registry Type	From the Registry Type field, selecting a Registry Type allows you to check the existence of the registry key in the client registry, or the value of the registry key. Click the drop-down arrow to view the following predefined settings: • RegistryKey—Checks whether a specific registry key exists in the registry. • RegistryValue—Checks whether a named registry key exists or has a particular value, version, or modification date. • RegistryValueDefault—Checks whether an unnamed (default) registry key exists or has a particular value, version, or modification date.
Registry Root Key	From the Registry Root Key field, selecting a Registry Root Key allows you to check the registry key, or the value of the registry key in the client registry from the root. Click the drop-down arrow to view the following Registry Root Key locations: • HKEY_LOCAL_MACHINE (HKLM) • HKEY_CURRENT_CONFIG (HKCC) • HKEY_CURRENT_USER (HKCU) • HKEY_USERS (HKU) • HKEY_CLASSES_ROOT (HKCR)
Sub Key	From the Sub Key field, selecting a sub key without the leading backslash (“\”) allows you to check the registry key and the registry key value in the path specified in the sub key. For example, SOFTWARE\Symantec\Norton AntiVirus\version from HKLM\SOFTWARE\Symantec\Norton AntiVirus\version
Value Name	(Default)
Value Data Type	From the Value Data Type field, selecting the data type allows you to check the registry key value data type, and its value using an operator. Click the drop-down arrow to view the predefined settings: • Number—choose one of the operators in the drop-down list to check the registry key value using a number in the registry key value • String—choose one of the operators in the drop-down list to check the registry key value using a string in the registry key value • Version—choose one of the operators in the drop-down list to check the registry key value using its version

Table 20-15 Registry Condition for RegistryValueDefault (continued)

Field Name	Field Description
Value Operator	From the Value Operator field, selecting an operator allows you to check the existence or nonexistence of data type of the registry key value using an operator. Click the drop-down arrow to view the following settings: • Exists • DoesNotExist
Value Data	From the Value Data field, enter the value of the registry key for the data type of the registry that you select.
Operating System	From the Operating System field, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Filtering Registry Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Registry Conditions page. A quick filter is a simple and quick filter that can be used to filter registry conditions on the Registry Conditions page. It filters registry conditions based on the field description such as the name of the registry conditions, description, and the type of registry conditions on the Registry Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Registry Conditions page. It filters registry conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Registry Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter registry conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Conditions** (menu window).

Step 2 From the Conditions (menu window), choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Registry Condition**.

The Registry Conditions page appears, which lists all the registry conditions that you have created.

Step 5 From the Registry Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-16.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-67 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-67.

Note To return to the Registry Conditions page, choose **All** from the Show drop-down to display all the registry conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters registry conditions based on each field description on the Registry Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Registry Conditions page. If you clear the field, it displays the list of all the registry conditions on the Registry Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter registry conditions by using variables that are more complex. It contains one or more filters, which filter registry conditions based on the values that match the field description. A filter on a single row filters registry conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter registry conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-16 describes the fields that allow you to filter registry conditions on the Registry Conditions page.

Table 20-16 Filtering Registry Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter registry conditions by the condition name.
	Description	This field enables you to filter registry conditions by the condition description.
	Registry Type	This field enables you to filter registry conditions by the registry type.
	Condition Type	This field enables you to filter registry conditions by Cisco predefined and not Cisco predefined conditions
Advanced Filter	Choose the field description from the following: • Name • Description • Registry Type • Condition type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter registry conditions.
	Value	From the Value field, choose the value for the field description that you selected against which to filter registry conditions.

Application Conditions

An application condition is a simple (single) condition, which checks applications that are running, and are not running on the client. The application condition can check for various application processes that are typically viewable under Windows Task Manager.

The Application Conditions page displays application conditions along with their names, description, as well as applications that are running and are not running on the client. It also shows the status of applications whether they are running, or are not running on the client.

Note Cisco predefined application conditions that are listed on the Application Conditions page are not editable.

This section provides the procedure that you can use to configure application conditions.

Configuring Application Conditions, page 20-69

Configuring Application Conditions

You can create an application condition to check that an application is running, or not running on the client. You can also duplicate, edit, delete, or filter application conditions from the Application Conditions page.

This section covers the following procedures:

- Viewing Application Conditions, page 20-69
- Creating, Duplicating, Editing, and Deleting an Application Condition, page 20-69
- Filtering Application Conditions, page 20-71

Viewing Application Conditions

You can use the Application Conditions page to view application conditions.

To view application conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you create.

Step 5 Choose an application condition from the application conditions list.

Step 6 Click **View**.

Here, you can choose an application condition to view the details.

Step 7 Click the **Application Conditions List** link to return to the Application Conditions page.

Creating, Duplicating, Editing, and Deleting an Application Condition

You can use the Application Conditions page to create, duplicate, edit, or delete an application condition, which allows you to check various application processes that are running, or are not running on the client.

To create an application condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the application condition is not editable.**

Step 6 Modify the values on the New Application Condition page, as shown in Table 20-17.

Here, you can create to add an application condition, which appears on the Application Conditions page.

Step 7 Click **Submit** to create an application condition.

To duplicate an application condition, complete the following steps:

Step 1 From the Posture menu, choose **Application Condition**.

The Applications conditions list page appears, which lists predefined Cisco application conditions and all the application conditions that you have already created.

Step 2 Choose the application condition that you want to duplicate.

Step 3 From the Application Conditions page, choose **Duplicate**.

Here, you can create a copy of the application condition.

Step 4 Click **Submit** to create a copy of the application condition.

To edit an application condition, complete the following steps:

Step 1 From the Posture menu, choose **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you have already created.

Step 2 Choose the application condition that you want to edit.

Step 3 From the Application Conditions page, choose **Edit**.

Here, you can edit an application condition.

Step 4 Click **Save** to save the changes to the application condition.

The application condition will appear on the Application Conditions page after editing on the edit page.

Step 5 Click the **Application Conditions List** link from the edit page to return to the Application Conditions page.

To delete an application condition, complete the following steps:

Step 1 From the Posture menu, choose **Application Condition**.

The Application Conditions page appears, which lists predefined Cisco application conditions and all the application conditions that you have already created.

Step 2 Choose the application condition that you want to delete.

Step 3 From the Application Conditions page, choose **Delete**.

Here, you can delete an application condition.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-17 describes the fields on the New Application Condition list page that allow you to create, duplicate, or edit an application condition on its edit page.

Table 20-17 Application Condition

Field Name	Field Description
Name	From the Name field, enter the name of the application condition that you want to create.
Description	From the Description field, enter the description of the application condition that you want to create.
Process Name	From the Process Name field, enter the name of the application that you want to check whether it is running, or not running on the client.
Application Operator	From the Application Operator field, selecting the status of an application allows you to check whether that application is running, or not running on the client. Click the drop-down arrow to view the following predefined settings: • Running • NotRunning
Operating System	From the Operating System field, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Filtering Application Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Applications Conditions page. A quick filter is a simple and quick filter that can be used to filter application conditions on the Application Conditions page. It filters application conditions based on the field description such as the name of the application conditions, description, and that shows the status whether applications are running, or not running on the client on the Application Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Application Conditions page. It filters application conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Application Conditions page.You can also edit preset filters and remove them from the preset filters list.

To filter application conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Conditions** (menu window).

Step 2 From the Conditions (menu window), choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Application Condition**.

The Application Conditions page appears, which lists all the application conditions that you have created.

Step 5 From the Application Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-18.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-72 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-73.

Note To return to the Application Conditions page, choose **All** from the Show drop-down to display all the application conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters application conditions based on each field description on the Application Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Application Conditions page. If you clear the field, it displays the list of all the application conditions on the Application Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter application conditions by using variables that are more complex. It contains one or more filters, which filter application conditions based on the values that match the field description. A filter on a single row filters application conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter application conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-18 describes the fields that allow you to filter application conditions on the Application Conditions page.

Table 20-18 Filtering Application Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter application conditions by the condition name.
	Description	This field enables you to filter application conditions by the condition description.
	Status	This field enables you to filter application conditions by checking the status of applications whether they are running or not running.
	Condition Type	This field enables you to filter application conditions by Cisco defined and user defined conditions.

Table 20-18 Filtering Application Conditions (continued)

Filtering Method	Filtering Field	Filtering Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Status • Condition Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter application conditions.
	Value	From the Value field, choose the value for the field description that you selected against which to filter application conditions.

Service Conditions

A service condition is a simple (single) condition, which checks services that are running, and are not running on the client. The service condition can check for various services such as security, or application agents that are typically viewable from the Windows Services console.

The Service Conditions page displays service conditions along with their names and description of the service conditions. It also shows the status whether the services are, or are not running on the client.

Cisco Predefined Checks

The Service Conditions page displays predefined Cisco checks as well as service conditions that you create on the Service Condition page. The predefined Cisco checks are downloaded on your Cisco ISE deployment as a result of dynamic posture updates. The pc_AutoUpdateCheck is one of the predefined Cisco checks, which is downloaded to the service conditions list (simple conditions).

For information on downloading Posture updates through the web, see the "Dynamic Posture Updates" section on page 20-22.

pc_AutoUpdateCheck

The pc_AutoUpdateCheck is a single (simple) condition, which can be used in a compound condition. The pr_AutoUpdateCheck_Rule is a compound condition that uses the pc_AutoUpdateCheck simple condition.

For information on how the pr_AutoUpdateCheck_Rule is used in a Windows update remediation, see the "pr_AutoUpdateCheck_Rule" section on page 20-80.

Note Cisco predefined service conditions that are listed on the Service Conditions page are not editable.

This section provides the procedure that you can use to configure service conditions.

Configuring Service Conditions, page 20-75

Configuring Service Conditions

You can create a service condition to check that a service is running, or not running on the client. You can also duplicate, edit, delete, or filter service conditions from the Services conditions list page.

This section covers the following procedures:

- Viewing Service Conditions, page 20-75
- Creating, Duplicating, Editing, and Deleting a Service Condition, page 20-75
- Filtering Service Conditions, page 20-77

Viewing Service Conditions

You can use the Service Conditions page to view service conditions.

To view service conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Service Condition**.

The Service Conditions page appears, which lists predefined Cisco service conditions and all the service conditions that you create.

Step 5 Choose a service condition from the service conditions list.

Step 6 Click **View**.

Here, you can choose a service condition to view the details.

Step 7 Click the **Service Conditions List** link to return to the Service Conditions page.

Creating, Duplicating, Editing, and Deleting a Service Condition

You can use the Service Conditions page to create, duplicate, edit, or delete a service condition, which allows you to check various services that are running or not running on the client.

To create a service condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Service Condition**.

The Service Conditions page appears, which lists predefined Cisco service conditions and all the service conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the service condition is not editable.**

Step 6 Modify the values on the New Service Condition page, as shown in Table 20-19.

Here, you can create to add a service condition, which appears on the Service Conditions page.

Step 7 Click **Submit** to create a Service condition.

To duplicate a service condition, complete the following steps:

Step 1 From the Posture menu, choose **Service Condition**.

The Service Conditions page appears, which lists predefined Cisco service conditions and all the service conditions that you have already created.

Step 2 Choose the service condition that you want to duplicate.

Step 3 From the Service Conditions page, choose **Duplicate**.

Here, you can create a copy of the service condition.

Step 4 Click **Submit** to create a copy of the service condition.

To edit a service condition, complete the following steps:

Step 1 From the Posture menu, choose **Service Condition**.

The Service Conditions page appears, which lists predefined Cisco service conditions and all the service conditions that you have already created.

Step 2 Choose the service condition that you want to edit.

Step 3 From the Service Conditions page, choose **Edit**.

Here, you can edit a service condition.

Step 4 Click **Save** to save the changes to the service condition.

The service condition will appear on the Service Conditions page after editing on the edit page.

Step 5 Click the **Service Conditions List** link from the edit page to return to the Service Conditions page.

To delete a service condition, complete the following steps:

Step 1 From the Posture menu, choose **Service Condition**.

The Service Conditions page appears, which lists predefined Cisco service conditions and all the service conditions that you have already created.

Step 2 Choose the service condition that you want to delete.

Step 3 From the Service Conditions page, choose **Delete**.

Here, you can delete a service condition.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-19 describes the fields on the New Service Condition page that allow you to create, duplicate, or edit a service condition on its edit page.

Table 20-19 Service Condition

Field Name	Field Description
Name	From the Name field, enter the name of the service condition that you want to create.
Description	From the Description field, enter the description of the service condition that you want to create.
Service Name	From the Service Name field, enter the name of the service that you want to check whether it is running, or not running on the client.
Service Operator	From the Service Operator field, selecting the status of a service allows you to check whether that service is running, or not running on the client. Click the drop-down arrow to view the following predefined settings. • Running • NotRunning
Operating System	From the Operating System field, selecting an operating system allows you to specify a Windows operating system to which the condition is applied.

Filtering Service Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Service Conditions page. A quick filter is a simple and quick filter that can be used to filter service conditions on the Service Conditions page. It filters service conditions based on the field description such as the name of the service condition, description, and that checks for services that are running, or not running on the client on the Service Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Service Conditions page. It filters service conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Service Conditions page.You can also edit preset filters and remove them from the preset filters list.

To filter service conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Service Condition**.

The Service Conditions page appears, which lists all the service conditions that you have created.

Step 5 From the Service Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-20.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-78 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-78.

Step 6 From the Show drop-down, choose a preset filter.

The preset filter displays the filtered results on the Service Conditions page.

Note To return to the Service Conditions page, choose **All** from the Show drop-down to display all the service conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters service conditions based on each field description on the Service Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Service Conditions page. If you clear the field, it displays the list of all the service conditions on the Service Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter service conditions by using variables that are more complex. It contains one or more filters, which filter service conditions based on the values that match the field description. A filter on a single row filters service conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter service conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-20 describes the fields that allow you to filter service conditions on the Service Conditions page.

Table 20-20 Filtering Service Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter service conditions by the condition name.
	Description	This field enables you to filter service conditions by the condition description.
	Check for	This field enables you to filter service conditions by checking the status of applications whether it is running or not.
	Condition Type	This field enables you to filter service conditions by Cisco predefined and not Cisco predefined conditions.
Advanced Filter	Choose the field description from the following: • Name • Description • Check for • Condition Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter service conditions.
	Value	From the Value field, choose the value for the field description that you selected against which to filter service conditions.

Compound Conditions

A compound condition includes one or more simple conditions, or compound conditions of the type file, registry, application, service, or dictionary conditions. You can combine one or more conditions using an AND (ampersand [&]), an OR (horizontal bar [|]), or a NOT (exclamation point [!]) operator to create a compound condition.

Cisco Predefined Rules

The Compound Conditions page displays predefined Cisco rules, as well as compound conditions that you create on the Compound Conditions page. The predefined Cisco rules are downloaded on your Cisco ISE deployment as a result of dynamic posture updates through the web.

For information on downloading Posture updates through the web, see the "Dynamic Posture Updates" section on page 20-22.

pr_AutoUpdateCheck_Rule

The pr_AutoUpdateCheck_Rule is a predefined Cisco Rule, which is downloaded to the Compound Conditions page. It contains only the pc_AutoUpdateCheck, a single (simple) condition.

When used in a posture requirement, the pr_AutoUpdateCheck_Rule compound condition allows you to check whether Windows clients are enabled with the automatic updates feature. If the Windows clients fail to meet the requirement, then the NAC Agents enforce Windows clients to be enabled (remediate) with the automatic updates feature, and upon which the clients are postured compliant. The Windows update remediation that you associate in the posture requirement overrides the Windows administrator setting, if the automatic updates feature is not enabled on Windows clients.

The Compound Conditions page displays compound conditions along with their names and description according to their operating systems. The Compound Conditions page allows you to filter the conditions based on the operating systems, as every condition is associated with one or more operating systems. The filtering options allow you to quickly pick the right set of conditions for a specific operating system.

Note Cisco predefined compound conditions that are listed on the Compound Conditions page are not editable.

This section provides the procedure that you can use to configure compound conditions.

Configuring Compound Conditions

Configuring Compound Conditions

You can create, duplicate, edit, delete, or filter compound conditions from the Compound Conditions page.

This section covers the following procedures:

- Viewing Compound Conditions, page 20-81
- Creating, Duplicating, Editing, and Deleting a Compound Condition, page 20-81
- Filtering Compound Conditions, page 20-84

Viewing Compound Conditions

You can use the Compound Conditions page to view compound conditions.

To view compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and all the service conditions that you create.

Step 5 Choose a compound condition from the compound conditions list.

Step 6 Click **View**.

Here, you can choose a compound condition to view the details.

Step 7 Click the **Compound Conditions List** link to return to the Compound Conditions page.

Creating, Duplicating, Editing, and Deleting a Compound Condition

You can use the Compound Conditions page to create, duplicate, edit, or delete a compound condition.

To add a compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and compound conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the compound condition is not editable. The operating system is also not editable on the compound condition after you have associated the newly created compound condition to a requirement. In order to edit the operating system on the compound condition, you need to remove the compound condition association from the posture requirement.**

Step 6 Modify the values on the New Compound Condition page, as shown in Table 20-21.

Here, you can create an expression by using logical operators to form a compound condition by combining simple conditions. You can use the Simple Conditions (an object selector) widget to choose one or more simple conditions.

a. Choose **Select a condition to insert below** and click the down arrow.

   The Simple Conditions widget appears that displays simple file, registry, application and service conditions.

b. Choose a simple condition from any one of the file, registry, application, and service condition types from the conditions list or click the **Quick Picker** (down arrow) on the **Action** button to create a simple condition that allows you to save it to the existing list of respective simple conditions

c. Choose one of the following simple conditions:

   - Create File Condition

     Add File Condition widget appears. Here, you can create a file (simple) condition.

   - Create Registry Condition

     Add Registry Condition widget appears. Here, you can create a registry (simple) condition.

   - Create Application Condition

     Add Application Condition widget appears. Here, you can create an application (simple) condition.

   - Create Service Condition

     Add Service Condition widget appears. Here, you can create a service (simple) condition.

d. Choose an AND (ampersand [&]), an OR (horizontal bar [|]), or a NOT (exclamation point [!]) operator to combine simple conditions. Use the parentheses [( )], and the logical operators to create a compound condition.

e. Choose a simple condition from any one of file, registry, application, and service condition types from the conditions list to the previously chosen simple conditions to create a compound condition.

Step 7 Click the **Validate Expression** button to validate the compound condition.

Step 8 Click **Submit** to create a compound condition.

To duplicate a compound condition, complete the following steps:

Step 1 From the Posture menu, choose **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco ISE compound conditions and compound conditions that you have already created.

Step 2 Choose the compound condition that you want to duplicate.

Step 3 From the Compound Conditions page, choose **Duplicate**.

Here, you can create a copy of the compound condition.

Step 4 Click **Submit** to create a copy of the compound condition

---

To edit a compound condition, complete the following steps:

Step 1 From the Posture menu, choose **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and compound conditions that you have already created.

Step 2 Choose the compound condition that you want to edit.

Step 3 From the Compound Conditions page, choose **Edit**.

Here, you can edit a compound condition, which you have already created, and saved on the Compound Conditions page. The predefined Cisco rules are not editable.

Step 4 Click **Save** to save the changes to the compound condition.

The compound condition will appear on the Compound Conditions page after editing on the edit page.

Step 5 Click the **Compound Conditions List** link to return to the Compound Conditions page.

To delete a compound condition, complete the following steps:

Step 1 From the Posture menu, choose **Compound Condition**.

The Compound Conditions page appears, which lists predefined Cisco compound conditions and compound conditions that you have already created.

Step 2 Choose the compound condition that you want to delete.

Step 3 From the Compound Conditions page, choose **Delete**.

Here, you can delete a compound condition.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-21 describes the fields on the New Compound Condition page that allow you to create, duplicate, or edit a compound condition on its edit page.

Table 20-21 Compound Condition

Field Name	Field Description
Name	From the Name field, enter the name of the compound condition that you want to create.
Description	From the Description field, enter the description of the compound condition that you want to create.
Operating System	From the Operating System field, selecting one or more Windows operating systems allow you to associate Windows operating systems to which the condition is applied.
Select a condition to insert below	From the Select a condition to insert below button, click the down arrow to display the Simple Conditions widget.

Table 20-21 Compound Condition

Field Name	Field Description
Expression	An area in the New Compound Condition page where you can create compound conditions using logical operators.
Parentheses ( )	Within the parentheses, you can combine two simple conditions from the following simple condition types: file, registry, application, and service conditions.
(&)—AND operator (use "&" for an AND operator, without the quotes)	You can use the AND operator (ampersand [&]) in a compound condition. For example, enter **Condition1 & Condition2**.
(|)—OR operator (use "|" for an OR operator, without the quotes)	You can use the OR operator (horizontal bar [|]) in a compound condition. For example, enter **Condition1 | Condition2**.
(!)—NOT operator (use "!" for a NOT operator, without the quotes)	You can use the NOT operator (exclamation point [!]) in a compound conditions. For example, enter **Condition1 & (!Condition2)**.
Simple Conditions	The Simple Conditions widget provides you with the list of simple conditions of the following types: file, registry, application, and service. You can also create simple conditions of file, registry, application and service conditions from here. Click the **Quick Picker** (down arrow) on the **Action** button to create simple conditions of file, registry, application, and service conditions.

Filtering Compound Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Compound Conditions page. A quick filter is a simple and quick filter that can be used to filter compound conditions on the Compound Conditions page. It filters compound conditions based on the field description such as the name and description of the compound condition on the Compound Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Compound Conditions page. It filters compound conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Compound Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions (menu window), choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Compound Condition**.

The Compound Conditions page appears which lists all the compound conditions that you have created.

Step 5 From the Compound Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-22.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-85 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-85.

Note To return to the Compound Conditions page, choose **All** from the Show drop-down to display all the compound conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters compound conditions based on each field description on the Compound Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Compound Conditions page. If you clear the field, it displays the list of all the compound conditions on the Compound Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter compound conditions by using variables that are more complex. It contains one or more filters, which filter compound conditions based on the values that match the field description. A filter on a single row filters compound conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-22 describes the fields that allow you to filter compound conditions on the Compound Conditions page.

Table 20-22 Filtering Compound Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter compound conditions by the condition name.
	Description	This field enables you to filter compound conditions by the condition description.
	Condition Type	This filed enables you to filter compound conditions by Cisco defined and not Cisco defined conditions.
Advanced Filter	Choose the field description from the following: • Name • Description • Condition Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter compound conditions.
	Value	From the Value field, choose the value for the field description that you selected against which to filter compound conditions.

Antivirus and Antispyware Compound Conditions

Prerequisites:

Before you begin, you should read and understand the following antivirus and antispyware topics:

- Antivirus and Antispyware Support Charts, which explain antivirus and antispyware support.
- Antivirus and Antispyware Definition Updates, which explain updating antivirus and antispyware definition files.

An Antivirus Compound Condition

Cisco ISE loads preconfigured antivirus compound conditions on the AV Compound Conditions page, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These antivirus compound conditions can check for antivirus products for their existence on all the clients. You can also create new antivirus compound conditions on the New Anti-virus Compound Condition page.

The New Anti-virus Compound Condition page displays the Products for Selected Vendor table, which provides information on antivirus products for a selected vendor.

An Antispyware Compound Condition

Cisco ISE loads preconfigured antispyware compound conditions on the AS Compound Conditions page, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These antispyware compound conditions can check for antispyware products for their existence on all the clients. You can also create new antispyware compound conditions on the New Anti-spyware Compound Condition page.

The New Anti-spyware Compound Condition page displays the Products for Selected Vendor table, which provides information on antivirus products for a selected vendor.

Antivirus and Antispyware Support Charts

Cisco ISE uses an antivirus and antispyware support chart, which provides the latest version and date on the definition files for each vendor product. Users need to frequently poll antivirus and antispyware support charts for updates. The antivirus and antispyware vendors frequently update antivirus and antispyware definition files, and the antivirus and antispyware chart provides them the latest version and date on the definition files for each vendor product.

Each time the antivirus and antispyware support chart is updated to reflect support for new antivirus and antispyware vendors, products, and their releases, the NAC Agents receive a new antivirus and antispyware library. It helps NAC Agents to support newer additions. Once the NAC Agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the antivirus and antispyware library for a particular antivirus, or antispyware product, the appropriate requirements will be sent to the NAC Agents for validating their existence, and the status of particular antivirus and antispyware products on the clients during posture validation.

Antivirus and Antispyware Definition Updates

The New Anti-virus Compound Condition and New Anti-spyware Compound Condition configuration pages allow you to use the information from the av-chart archive files, which display the list of vendors, supported products, and their releases to configure client remediations on the AV Remediations and AS Remediations page.

On the New Anti-virus Compound Condition and New Anti-spyware Compound Condition configuration pages, you have an option to check for antivirus and antispyware definition file date, or version on all the clients for the following: a particular vendor product, or any product from a vendor, or for any vendor any product. In addition, you also have an option to specify that the definition files can be older than a specified certain number of days. It gives users a certain amount of time to enforce security policies with respect to how old the definition files can be on their system.

Antivirus and antispyware compound conditions allow you to verify that the virus definition files for a specified vendor are up-to-date on your clients. You can optionally configure antivirus and antispyware definition files of antivirus and antispyware compound conditions to be older by a number of days than the definition files, which are updated in the Cisco ISE servers. Even if the definition files have not been updated by the vendor, this option allows you to configure antivirus and antispyware compound conditions so that clients are validated for compliance with older versions by a few days.

For antivirus definition file updates, you can specify the number of days either from the latest antivirus definition file updates for a specified vendor, or from the current system date on Cisco ISE. For antispyware definition file updates, you must specify the number of days from the current system date. You do not have the option to specify the number of days from the latest antispyware definition file updates. The default number of days is zero (0), indicating that the antivirus and antispyware file definition date cannot predate the latest file or current system date.

You can also associate antivirus and antispyware compound conditions to the AV remediations and AS remediation actions. If your clients fail to meet antivirus and antispyware compound conditions, then the NAC Agents that are installed on your clients communicate directly with the installed antivirus and antispyware software on the clients. The NAC Agents display a dialog with an update, or remediate button on it for end users to use them to remediate clients automatically with the latest antivirus and antispyware definition files.

Related Topics

Antivirus Compound Conditions, page 20-88

Antispyware Compound Conditions, page 20-94

Antivirus Compound Conditions

An antivirus compound condition contains one or more antivirus conditions (simple conditions), or antivirus compound conditions. An antivirus compound condition checks an antivirus installation, or checks for an antivirus signature definition version/date on a client. You can create an antivirus compound condition to check for an antivirus installation, or definition updates on the client for any vendor.

This section provides the procedure that you can use to configure antivirus compound conditions.

Configuring Antivirus Compound Conditions, page 20-88

Configuring Antivirus Compound Conditions

The AV Compound Conditions page displays antivirus compound conditions along with their names and description.

You can create an antivirus compound condition to check that an antivirus installation exists on your clients, or check that the latest antivirus signature definition version/date on the client for a selected vendor. You can duplicate, edit, delete, or filter antivirus compound conditions from the AV Compound Conditions page.

This section covers the following procedures:

- Creating, Duplicating, Editing, and Deleting an Antivirus Compound Condition, page 20-88
- Filtering Antivirus Compound Conditions, page 20-92

Creating, Duplicating, Editing, and Deleting an Antivirus Compound Condition

You can use the AV Compound Conditions page to create, duplicate, edit, or delete an antivirus compound condition.

To create an antivirus compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the Cisco predefined rules, and also antivirus compound conditions that you create on the New Anti-virus Compound Condition page.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the antivirus compound condition is not editable.**

Step 6 Modify the values on the New Anti-virus Compound Conditions page, as shown in Table 20-23.

Here, you can create an antivirus compound condition to check the installation of an antivirus program, or check that an antivirus definition file is up-to-date.

Note Choose a product from the Products for Selected Vendor table.

Step 7 Click **Submit** to create an antivirus compound condition.

To duplicate an antivirus compound condition, complete the following steps:

Step 1 From the Posture menu, choose **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the Cisco predefined rules, and also antivirus compound conditions that you have already created.

Step 2 Choose the antivirus compound condition that you want to duplicate.

Step 3 From the AV Compound Conditions page, choose **Duplicate**.

Here, you can create a copy of the antivirus compound condition.

Step 4 Click **Submit** to create a copy of the antivirus compound condition.

To edit an antivirus compound condition, complete the following steps:

Step 1 From the Posture menu, choose **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the Cisco predefined rules, and also antivirus compound conditions that you have already created.

Step 2 Choose an antivirus compound condition that you want to edit.

Step 3 From the AV Compound Conditions page, choose **Edit**.

Here, you can edit an antivirus compound condition, which you have already created and saved on the AV Compound Conditions page. The predefined Cisco rules are not editable.

Step 4 Click **Save** to save the changes to an antivirus compound condition.

The antivirus compound condition will appear on the AV Compound Conditions page after editing on the edit page.

Step 5 Click the **Anti-virus Compound Conditions List** link to return to the AV Compound Conditions page.

To delete an antivirus compound condition, complete the following steps:

Step 1 From the Posture menu, choose **AV Compound Condition**.

The AV Compound Conditions page appears, which lists all the Cisco predefined rules, and also AV compound conditions that you have already created.

Step 2 Choose an antivirus compound condition that you want to delete.

Step 3 From the AV Compound Conditions page, choose **Delete**.

Here, you can delete an antivirus compound condition.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-23 describes the fields on the AV Compound Conditions page that allow you to create, duplicate, or edit an antivirus compound condition.

Table 20-23 AV Compound Condition

Field Name	Field Description
Name	The name of the antivirus compound condition that you want to create.
Description	The description of the antivirus compound condition that you want to create.
Operating System	The field selection of Operating System allows you to check the installation of an antivirus programs on your client, or check the latest antivirus definition file updates to which the condition is applied.
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antivirus products and versions, which are displayed in a table (Products for Selected Vendor) on the New Anti-virus Compound Condition page.
Check Type	The field selection of Check Type allows you to choose whether to check an installation or check the latest definition file update on the client.
Installation radio button	The field selection of Installation radio button allows you to check only the installation of an antivirus program on the client.

Table 20-23 AV Compound Condition (continued)

Field Name	Field Description
Definition radio button	The field selection of Definition radio button allows you to check only the latest definition file update of an antivirus product on the client. When enabled, Cisco ISE provides you the following two options to check clients against latest antivirus definition file version or latest antivirus definition file date: • Check against latest AV definition file version if available. Otherwise check against latest definition file date • Allow virus definition file to be a specific number of days days older than latest file date or current system date
Check against latest AV definition file version, if available. (Otherwise check against latest definition file date).	The field selection allows you to check the antivirus definition file version on the client against the latest antivirus definition file version, if available as a result of posture updates in Cisco ISE. Otherwise, it allows you to check the definition file date on the client against the latest definition file date in Cisco ISE.
Allow virus definition file to be check box (Enabled)	The Allow virus definition file to be check box is enabled only when you choose creating antivirus definition check types, and disabled when creating antivirus installation check types. If checked, the selection allows you to check the antivirus definition file version and the latest antivirus definition file date on the client. The latest definition file date cannot be older than that you define in the next field (days older than field) from the latest antivirus definition file date of the product or the current system date. If unchecked, Cisco ISE allows you to check only the version of the antivirus definition file using the Check against latest AV definition file version, if available option.
days older than	The field defines the number of days that the latest antivirus definition file date on the client can be older from the latest antivirus definition file date of the product or the current system date. The default value is zero (0).
The latest file date radio button	When selected, the latest file date option checks that the antivirus definition file date on the client, which can be older by the number of days that you define in the next field (days older than field). If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the latest antivirus definition file date of the product.
The current system date radio button	When selected, the current system date option checks that the antivirus definition file date on the client, which can be older by the number of days that you define in the next field (days older than field). If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the current system date.

Table 20-23 AV Compound Condition (continued)

Field Name	Field Description
Products for Selected Vendor table	Choose an antivirus product from the table. Based on the vendor that you select in the New Anti-virus Compound Condition page, the table retrieves information on their antivirus products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antivirus program, or check for the latest antivirus definition file date, and its latest version.

Filtering Antivirus Compound Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the AV Compound Conditions page. A quick filter is a simple and quick filter that can be used to filter antivirus compound conditions on the AV Compound Conditions page. It filters antivirus compound conditions based on the field description such as the name and description of the antivirus compound condition on the AV Compound Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the AV Compound Conditions page. It filters antivirus compound conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the AV Compound Conditions page.You can also edit preset filters and remove them from the preset filters list.

To filter antivirus compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions (menu window), choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **AV Compound Condition**.

The AV Compound Conditions page appears which lists all the antivirus compound conditions.

Step 5 From the AV Compound Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-24.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-93 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-93.

Note To return to the AV Compound Conditions page, choose **All** from the Show drop-down to display all the antivirus compound conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters antivirus compound conditions based on each field description on the AV Compound Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the AV Compound Conditions page. If you clear the field, it displays the list of all the antivirus compound conditions on the AV Compound Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter antivirus compound conditions by using variables that are more complex. It contains one or more filters, which filter antivirus compound conditions based on the values that match the field description. A filter on a single row filters antivirus compound conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter antivirus compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-24 describes the fields that allow you to filter antivirus compound conditions on the AV Compound Conditions page.

Table 20-24 Filtering Antivirus Compound Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter antivirus compound conditions by the condition name.
	Description	This field enables you to filter antivirus compound conditions by the condition description.
Advanced Filter	Choose the field description from the following: • Name • Description	Click the drop-down arrow to choose the field description.
	Operator	Click the drop-down arrow to choose a value that can be used to filter in the Operator field.
	Value	Enter the value for the field description that you selected against to filter the conditions.

Antispyware Compound Conditions

An antispyware compound condition contains one or more antispyware conditions (simple conditions), or antispyware compound conditions. An antispyware compound condition checks an antispyware installation, or checks for an antispyware signature definition version/date on a client against the current system date. You can create an antispyware compound condition to check for an antivirus installation, or definition updates on the client for any vendor.

When you create an antispyware definition file update condition, the antispyware definition file date can be older than the current system date by the number of days that you specify for checking the definition file date on the client. The default value is zero (0) days.

Here, you must enable (check) the Allow virus definition file to be check box to check that the latest antispyware definition file date on the client. It can be older than the current system date by the number of days, which you define in the days older than field.

This section provides the procedure that you can use to configure antispyware compound conditions.

Configuring Antispyware Compound Conditions, page 20-94

Configuring Antispyware Compound Conditions

The AS Compound Conditions page displays antispyware compound conditions along with their names and description.

You can create an antispyware compound condition to check that an antispyware installation exists on your clients, or check that the latest antispyware signature definition version/date on the client for a selected vendor. You can duplicate, edit, delete, or filter antispyware compound conditions from the AS Compound Conditions page.

This section covers the following procedures:

- Creating, Duplicating, Editing, and Deleting an Antispyware Compound Condition, page 20-95

- Filtering Antispyware Compound Conditions, page 20-98

Creating, Duplicating, Editing, and Deleting an Antispyware Compound Condition

You can use the AS Compound Conditions page to create, duplicate, edit, or delete an antispyware compound condition.

To create an antispyware compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the Cisco predefined rules, and also antispyware compound conditions that you create on the New Anti-spyware Compound Condition page.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the antispyware compound condition is not editable.**

Step 6 Modify the values on the New Anti-spyware Compound Condition page, as shown in Table 20-25.

Here, you can create an antispyware compound condition to check the installation of an antispyware program, or check that an antispyware definition file is up-to-date.

Note Choose a product from the Products for Selected Vendor table.

Step 7 Click **Submit** to create an antispyware compound condition.

To duplicate an antispyware compound condition, complete the following steps:

Step 1 From the Posture menu, choose **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the Cisco predefined rules, and also antispyware compound conditions that you have already created.

Step 2 Choose the antispyware compound condition that you want to duplicate.

Step 3 From the AS Compound Conditions page, choose **Duplicate**.

Here, you can create a copy of the antispyware compound condition.

Step 4 Click **Submit** to create a copy of the antispyware compound condition.

To edit an antispyware compound condition, complete the following steps:

Step 1 From the Posture menu, choose **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the Cisco predefined rules, and also antispyware compound conditions that you have already created.

Step 2 Choose an antispyware compound condition that you want to edit.

Step 3 From the AS Compound Conditions page, choose **Edit**.

Here, you can edit an antispyware compound condition, which you have already created and saved on the AS Compound Conditions page. The predefined Cisco rules are not editable.

Step 4 Click **Save** to save the changes to an antispyware compound condition.

The antispyware compound condition will appear on the AS Compound Conditions page after editing on the edit page.

Step 5 Click the **AS Compound Conditions List** link to return to the AS Compound Conditions page.

To delete an antispyware compound condition, complete the following steps:

Step 1 From the Posture menu, choose **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the Cisco predefined rules, and also AS compound conditions that you have already created.

Step 2 Choose an antispyware compound condition that you want to delete.

Step 3 From the AS Compound Conditions page, choose **Delete**.

Here, you can delete an antispyware compound condition.

Warning **Cisco predefined conditions cannot be deleted. Please select conditions that are not defined by Cisco to delete.**

Table 20-25 describes the fields on the AS Compound Conditions page that allow you to create, duplicate, or edit an antispyware compound condition.

Table 20-25 Antispyware Compound Condition

Field Name	Field Description
Name	The name of the antispyware compound condition that you want to create.
Description	The description of the antispyware compound condition that you want to create.
Operating System	The field selection of Operating System allows you to check the installation of an antispyware programs on your client, or check the latest antispyware definition file updates to which the condition is applied.

Table 20-25 Antispyware Compound Condition (continued)

Field Name	Field Description
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antispyware products and versions, which are displayed in a table (Products for Selected Vendor) on the New Anti-spyware Compound Condition page.
Check Type	The field selection of Check Type allows you to choose a type whether to check an installation, or check the latest definition file update on the client.
Installation radio button	The field selection of Installation radio button allows you to check only the installation of an antispyware program on the client.
Definition radio button	The field selection of Definition radio button allows you to check only the latest definition file update of an antispyware product on the client.
Allow virus definition file to be check box (Enabled)	The Allow virus definition file to be check box is enabled only when creating antispyware definition check types, and disabled when creating antispyware installation check types. If checked, the selection allows you to check antispyware definition file version and the latest antispyware definition file date on the client. The latest definition file date cannot be older than that you define in the next field (days older than field) from the current system date. If unchecked, the selection allows you to check only the version of the antispyware definition file as the Allow virus definition file to be check box is not checked.
days older than	The field defines the number of days that the latest antispyware definition file date on the client can be older from the current system date. The default value is zero (0).
The current system date radio button	When selected, the current system date option checks that the antispyware definition file date on the client, which can be older by the number of days that you define in the next field (days older than field). If you set the number of days to the default value (0), then the antispyware definition file date on the client should not be older than the current system date.
Products for Selected Vendor table	Choose an antispyware product from the table. Based on the vendor that you select in the New Anti-spyware Compound Condition page, the table retrieves information on their antispyware products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antispyware program, or check for the latest antispyware definition file date, and its latest version.

Filtering Antispyware Compound Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the AS Compound Conditions page. A quick filter is a simple and quick filter that can be used to filter antispyware compound conditions on the AS Compound Conditions page. It filters antispyware compound conditions based on the field description such as the name and description of the antispyware compound condition on the AS Compound Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the AS Compound Conditions page. It filters antispyware compound conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the AS Compound Conditions page.You can also edit preset filters and remove them from the preset filters list.

To filter antispyware compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions (menu window), choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **AS Compound Condition**.

The AS Compound Conditions page appears, which lists all the antispyware compound conditions.

Step 5 From the AS Compound Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-26.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-98 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-99.

Note To return to the AS Compound Conditions page, choose **All** from the Show drop-down to display all the antispyware compound conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters antispyware compound conditions based on each field description on the AS Compound Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Compound conditions list page. If you clear the field, it displays the list of all the antispyware compound conditions on the AS Compound Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter antispyware compound conditions by using variables that are more complex. It contains one or more filters, which filter antispyware compound conditions based on the values that match the field description. A filter on a single row filters antispyware compound conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter antispyware compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-26 describes the fields that allow you to filter antispyware compound conditions on the AS Compound Conditions page.

Table 20-26 Filtering Antispyware Compound Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter conditions by the condition name.
	Description	This field enables you to filter conditions by the condition description.
Advanced Filter	Choose the field description from the following: • Name • Description	Click the drop-down arrow to choose the field description.
	Operator	Click the drop-down arrow to choose a value that can be used to filter in the Operator field.
	Value	Enter the value for the field description that you selected against to filter the conditions.

Dictionary Simple Conditions

A dictionary simple condition is a simple (single) condition, where you can associate a value to a dictionary attribute. Once created and saved, the dictionary simple conditions are added to a library. You can use these dictionary simple conditions to form a dictionary compound condition on the Dictionary Compound Conditions page.

This section provides the procedure that you can use to configure dictionary simple conditions.

Configuring Dictionary Simple Conditions, page 20-100

Configuring Dictionary Simple Conditions

You can create a dictionary simple condition to check the value of an attribute that you associate to the dictionary attribute in the dictionary simple condition. You can also duplicate, edit, delete, or filter dictionary simple conditions from the Dictionary Simple Conditions page.

The Dictionary Simple Conditions page displays dictionary simple conditions along with their names and description, as well as the conditions in detail that you define in the dictionary simple conditions.

This section covers the following procedures:

- Creating, Duplicating, Editing, and Deleting a Dictionary Simple Condition, page 20-100
- Filtering Dictionary Simple Conditions, page 20-102

Creating, Duplicating, Editing, and Deleting a Dictionary Simple Condition

You can use the Dictionary Simple Conditions page to create, duplicate, edit, or delete a dictionary simple condition.

To create a dictionary simple condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Dictionary Simple Condition.**

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the dictionary simple condition is not editable.**

Step 6 Modify the values on the New Dictionary Condition page, as shown in Table 20-27.

Here, you can create a dictionary simple condition where you can associate a value to a dictionary attribute.

Step 7 Click **Submit** to create a dictionary simple condition.

To duplicate a dictionary simple condition, complete the following steps:

Step 1 From the Posture menu, choose **Dictionary Simple Condition.**

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you have already created.

Step 2 Choose a dictionary simple condition that you want to duplicate.

Step 3 From the Dictionary Simple Conditions page, choose **Duplicate**.

Here, you can create a copy of a dictionary simple condition.

Step 4 Click **Submit** to create a copy of a dictionary simple condition.

To edit a dictionary simple condition, complete the following steps:

Step 1 From the Posture menu, choose **Dictionary Simple Condition.**

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you have already created.

Step 2 Choose a dictionary simple condition that you want to edit.

Step 3 From the Dictionary Simple Conditions page, choose **Edit**.

Here, you can edit a dictionary simple condition.

Step 4 Click **Save** to save the changes to a dictionary simple condition.

The dictionary simple condition will appear on the Dictionary Simple Conditions page after editing on the edit page.

Step 5 Click the **Dictionary Conditions List** link to return to the Dictionary Simple Conditions page.

You cannot delete a dictionary simple condition, which is associated to a dictionary compound condition. To delete, you must first remove the association from the dictionary compound condition, and then delete it.

To delete a dictionary simple condition, complete the following steps:

Step 1 From the Posture menu, choose **Dictionary Simple Condition**.

The Dictionary Simple Conditions page appears, which lists all the dictionary simple conditions that you have already created.

Step 2 Choose a dictionary simple condition that you want to delete.

Step 3 From the Dictionary Simple Conditions page, choose **Delete**.

Here, you can delete a dictionary simple condition.

Table 20-27 describes the fields on the Dictionary Simple Conditions page that allow you to create, duplicate a dictionary simple condition, or edit a dictionary simple condition on its edit page.

Table 20-27 Dictionary Simple Condition

Field Name	Field Description
Name	From the Name field, enter the name of the dictionary simple condition that you want to create.
Description	From the Description field, enter the description of the dictionary simple condition that you want to create.
Attribute	From the Attribute field, you can choose an attribute from a dictionary in the dictionaries widget.
Operator	From the Operator field, you can choose an operator to associate a value to an attribute that you have selected. Click the drop-down arrow to choose an operator from the predefined settings for each of the dictionary attribute that you have selected.
Value	From the Value field, enter a value that you want to associate to the dictionary attribute, or choose a predefined value from the drop-down list.

Filtering Dictionary Simple Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Dictionary Simple Conditions page. A quick filter is a simple and quick filter that can be used to filter dictionary simple conditions on the Dictionary Simple Conditions page. It filters dictionary simple conditions based on the field description such as the name of the dictionary simple condition, condition that you define in the dictionary simple condition, and description on the Dictionary Simple Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Dictionary Simple Conditions page. It filters dictionary simple conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Dictionary Simple Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter dictionary simple conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions (menu window), choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Dictionary Simple Condition**.

The Dictionary Simple Conditions page appears which displays all the dictionary simple conditions that you create.

Step 5 From the Dictionary Simple Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-28.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-103 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-103.

Note To return to the Dictionary Simple Conditions page, choose **All** from the Show drop-down to display all the dictionary simple conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters dictionary simple conditions based on each field description on the Dictionary Simple Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Dictionary Simple Conditions page. If you clear the field, it displays the list of all the dictionary simple conditions on the Dictionary Simple Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter dictionary simple conditions by using variables that are more complex. It contains one or more filters, which filter dictionary simple conditions based on the values that match the field description. A filter on a single row filters dictionary simple conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-28 describes the fields on the Dictionary Simple Conditions page that allow you to filter dictionary simple conditions.

Table 20-28 Filtering Dictionary Simple Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter dictionary simple conditions by the condition name.
	Condition	This field enables you to filter dictionary simple conditions by the condition that you define in the dictionary simple condition.
	Description	This field enables you to filter dictionary simple conditions by the condition description.
Advanced Filter	Choose the field description from the following: • Name • Condition • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter dictionary simple conditions.
	Value	From the Value field, choose the value for the field description that you selected against which to filter dictionary simple conditions.

Dictionary Compound Conditions

A dictionary compound condition is a logical combination of more than one dictionary simple condition (a dictionary attribute that is associated with a value). It is a set of dictionary simple conditions (dictionary attributes that are associated with values) that are logically combined with an AND, or an OR operator. You can save a dictionary compound condition, only when you define more than one dictionary simple condition, and then combine them on the Dictionary Compound Conditions page. One or more dictionary simple conditions that you create on the Dictionary Compound Conditions page must be saved to a library first, which can be added later from the library to form a dictionary compound condition.

This section provides the procedure that you can use to configure dictionary compound conditions.

Configuring Dictionary Compound Conditions, page 20-104

Configuring Dictionary Compound Conditions

The Dictionary Compound Conditions page displays the list of dictionary compound conditions along with their names and description, as well as dictionary simple conditions that are logically combined.

This section covers the following procedure:

- Creating, Duplicating, Editing, and Deleting a Dictionary Compound Condition, page 20-105

- Filtering Dictionary Compound Conditions, page 20-108

Creating, Duplicating, Editing, and Deleting a Dictionary Compound Condition

You can create, duplicate, edit, or delete a dictionary compound condition from the Dictionary Compound Conditions page.

To create a dictionary compound condition, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions menu window, choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Dictionary Compound Condition**.

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you create.

Step 5 Click **Add**.

Warning **Once created and saved, the name of the dictionary compound condition is not editable.**

Step 6 Modify the values on the New Dictionary Compound Condition page, as shown in Table 20-29.

Here, you can create a dictionary compound condition where you can logically combine more than one dictionary simple conditions.

Step 7 Click **Submit** to create a dictionary compound condition.

To duplicate a dictionary compound condition, complete the following steps:

Step 1 From the Posture menu, choose **Dictionary Compound Condition.**

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you have already created.

Step 2 Choose a dictionary compound condition that you want to duplicate.

Step 3 From the Dictionary Compound Conditions page, choose **Duplicate**.

Here, you can create a copy of a dictionary compound condition.

Step 4 Click **Submit** to create a copy of a dictionary compound condition.

To edit a dictionary compound condition, complete the following steps:

Step 1 From the Posture menu, choose **Dictionary Compound Condition.**

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you have already created.

Step 2 Choose the dictionary compound condition that you want to edit.

Step 3 From the Dictionary Compound Conditions page, choose **Edit**.

Here, you can edit a dictionary compound condition.

Step 4 Click **Save** to save the changes to a dictionary compound condition.

The dictionary compound condition will appear on the Dictionary Compound Conditions page after editing on the edit page.

Step 5 Click the **Dictionary Compound Conditions List** link to return to the Dictionary Compound Conditions page.

To delete a dictionary compound condition, complete the following steps:

Step 1 From the Posture menu, choose **Dictionary Compound Condition**.

The Dictionary Compound Conditions page appears, which lists all the dictionary compound conditions that you have already created.

Step 2 Choose the dictionary compound condition that you want to delete.

Step 3 From the Dictionary Compound Conditions page, choose **Delete**.

Here, you can delete a dictionary compound condition.

Table 20-29 describes the fields on the Dictionary Compound Conditions page that allow you to create, duplicate a dictionary compound condition, or edit a dictionary compound condition on its edit page.

Table 20-29 Dictionary Compound Condition

Field Name	Field Description
Name	From the Name field, enter the name of the dictionary compound condition that you want to create.
Description	From the Description field, enter the description of the dictionary compound condition that you want to create.
Select Existing Condition from Library	You can define an expression by selecting pre-defined conditions from the policy elements library. Click the **Action Icon** button to do the following: • Add Attribute/Value • Add Condition from Library • Delete You can add ad-hoc attribute/value pairs to your expression in the subsequent steps. Click the **Action Icon** button to do the following: • Add Attribute/Value—allows you to create a dictionary simple condition • Add Condition from Library—allows you to choose a dictionary simple, or dictionary compound condition from the library that are already created and saved • Duplicate—allows to duplicate a condition that you create or choose on this page. • Add Condition to Library—allows you to save new dictionary simple, and dictionary compound conditions that you create here to the library for use later • Delete—allows to remove the association of a dictionary simple or dictionary compound condition from the dictionary compound condition.
Condition Name	From the Condition Name field, you can choose dictionary simple conditions that you have already created from the policy elements library.
Expression	The Expression field is updated based on your selection from the Condition Name field.
AND or OR operator	Either an AND operator, or an OR operator allows you to logically combine dictionary simple conditions, which can be added from the library. Click the **Action Icon** button to do the following: • Add Attribute/Value • Add Condition from Library • Delete

Table 20-29 Dictionary Compound Condition (continued)

Field Name	Field Description
Create New Condition (Advance Option)	You can define an expression by selecting attributes from various system or user-defined dictionaries. Click the **Action Icon** button to do the following: • Add Attribute/Value • Add Condition from Library • Duplicate • Add Condition to Library • Delete You can add pre-defined conditions from the policy elements library in the subsequent steps.
Condition Name	From the Condition Name field, you can create a new dictionary simple condition and then save it to the library, or choose dictionary simple conditions that you have already created from the library.
Expression	From the Expression field, you can create a dictionary simple condition by choosing an attribute from a dictionary in the dictionaries widget to which you can associate a value.
Operator	From the Operator field, you can choose an operator to associate a value to an attribute. Click the drop-down arrow to choose an operator from the predefined settings for each of the dictionary attribute that you select.
Value	From the Value field, enter a value that you want to associate to the dictionary attribute, or choose a value from the drop-down list.
AND or OR operator	Either an AND operator, or an OR operator allows you to logically combine dictionary simple conditions, which can be added from the library.

Filtering Dictionary Compound Conditions

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Dictionary Compound Conditions page. A quick filter is a simple and quick filter that can be used to filter dictionary compound conditions on the Dictionary Compound Conditions page. It filters dictionary compound conditions based on the field description such as the name of the dictionary compound condition, conditions that you define in the dictionary compound condition, and description on the Dictionary Compound Conditions page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Dictionary Compound Conditions page. It filters dictionary compound conditions based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Dictionary Compound Conditions page. You can also edit preset filters and remove them from the preset filters list.

To filter compound conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions** (menu window).

Step 2 From the Conditions (menu window), choose **Posture**.

Step 3 Click the **Quick Picker** (right arrow) icon to navigate to the list of posture conditions.

The Posture menu appears, which lists all the posture condition types.

Step 4 From the Posture menu, choose **Dictionary Compound Condition**.

The Dictionary Compound Conditions page appears which lists all the dictionary compound conditions that you create.

Step 5 From the Dictionary Compound Conditions page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-30.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-109 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-109.

Note To return to the Dictionary Compound Conditions page, choose **All** from the Show drop-down to display all the dictionary compound conditions without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters dictionary compound conditions based on each field description on the Dictionary Compound Conditions page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Dictionary Compound Conditions page. If you clear the field, it displays the list of all the compound conditions on the Dictionary Compound Conditions page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter dictionary compound conditions by using variables that are more complex. It contains one or more filters, which filter dictionary compound conditions based on the values that match the field description. A filter on a single row filters dictionary compound conditions based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter compound conditions by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-30 describes the fields on the Dictionary Compound Conditions page that allow you to filter dictionary compound conditions.

Table 20-30 Filtering Dictionary Compound Conditions

Filtering Method	Filtering Field	Filtering Field Description
Quick Filter	Name	This field enables you to filter compound conditions by the condition name.
	Condition	This field enables you to filter dictionary compound conditions by the condition that you define in the dictionary compound condition.
	Description	This field enables you to filter compound conditions by the condition description.
Advanced Filter	Choose the field description from the following: • Name • Condition • Description	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter dictionary compound conditions.
	Value	From the Value field, choose the value for the field description that you selected against which to filter dictionary compound conditions.

Posture Results

Posture results are associated mandatory requirements to posture policies that all clients must meet their requirements during posture evaluation, and associated remediation actions to requirements that are required by clients to remediate themselves to meet failed requirements in order to become compliant on your network.

Posture results in posture requirements which all clients must meet for compliance with your organization security policies during policy evaluation of endpoints The posture requirements can be set to mandatory, optional, or audit types in posture policies during posture evaluation of endpoints.

Mandatory Requirements

If clients fail to meet mandatory requirements as defined in posture policies, then they are provided with remediation options in order for clients to meet them during policy evaluation. When clients fail to meet mandatory requirements during policy evaluation, it results in remediation actions that are associated to requirements, and end users are given remediation time within minutes specified in the remediation timer settings to remediate failed requirements.

If a client machine is unable to remediate a mandatory requirement, the session posture status changes to “non-compliant” and the agent session is quarantined. The only way to get the client machine past this “non-compliant” state is by initiating a new RADIUS or posture session where the agent starts posture assessment on the client machine again.

You can restart posture assessment on the client machine by doing one of the following:

- For wired and wireless CoA in an 802.1X environment—You can configure the Reauthentication Timer for the specific authorization policy in the **Policy > Policy Elements > Results > Authorization > Authorization Profiles** page. When you have the authorization policy page open, enable the **Reauthentication** function under **Common Tasks** and set the Maintain Connectivity During Reauthentication option to “Default.” The result is that the timer expires and a brand new session launches, thus restarting posture assessment. For more details, see Modifying an Existing Authorization Profile, page 17-31. (This method is not supported in Inline Posture deployments.)

  Alternatively, wired users can get out of the quarantine state once they disconnect and reconnect to the network. In a wireless environment, the user must disconnect from the WLC and wait until the user idle timeout period has expired before attempting to reconnect to the network.

- In a VPN environment—The only option is to disconnect and reconnect the VPN tunnel.

Optional Requirements

If client machines fail to meet optional requirements during policy evaluation, then the agents prompt end users with an option to continue further so that end users can skip optional requirements even though they fail during policy evaluation.

Audit Requirements

Audit requirements are not shown to end users even though they pass, or fail during policy evaluation.

Related Topics

- Custom Posture Remediation Actions, page 20-112
- Configuring Custom Posture Remediation Actions, page 20-113
- Client Posture Assessment Requirements, page 20-155

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

Custom Posture Remediation Actions

A custom posture remediation action can take the form of a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) types.

Here, you also have a text box for all the remediation types that can be used to communicate to the Agent users. In addition to remediation actions, you can also communicate to Agent users of non compliance of clients only with messages. Here, the NAC Agent does not trigger any remediation action.

Message Text Only

The Message Text Only option informs Agent users about noncompliance of clients. It also provides optional instructions to the user to contact the Help desk for more information, or to remediate the client manually.

When you create a posture requirement on the Requirements page, you can associate any one of a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) types to the requirement.

You can use the Posture Remediation Actions menu to manage the following remediations for a posture in Cisco ISE:

- A file remediation—downloads the required file version on your client for compliance
- A link remediation—provides a URL link for the client to click for access to a remediation page or resource
- An antivirus remediation—updates antivirus signature definitions on the client for compliance
- An antispyware remediation—updates antispyware signature definitions on the client for compliance
- Launch programs remediation—launches one or more programs on the client for compliance
- Windows update remediation—changes the Windows Automatic Update configuration (System Properties) on the client per customer security policy, and helps to ensure Windows Update remediates the client for compliance
- Windows Server Update Services (WSUS) remediation—remediates the Windows client from a locally managed WSUS server, or Microsoft-managed WSUS server with the latest WSUS updates for compliance

To manage the posture remediation actions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to view the posture results.

The following results appear:

- Remediation Actions—associated to requirements, which are required by clients to remediate themselves to meet failed requirements during policy evaluation
- Requirements—associated to posture policies that all clients must meet during policy evaluation

Step 4 Choose **Remediation Actions**.

The following remediation types appear:

- File Remediation
- Link Remediation
- Antivirus Remediation
- Antispyware Remediation
- Launch Program Remediation
- Windows Update Remediation
- Windows Server Update Services Remediation

Step 5 Choose a remediation type to view the remediations list.

Configuring Custom Posture Remediation Actions

This section describes the custom remediation types that you can define in Cisco ISE.

Table 20-31 shows remediation types that are supported by NAC web agent, NAC agents for Windows and Macintosh clients.

Table 20-31 Remediation Types Supported by Agents

Remediation Action Type	Web Agent	NAC Agent for Windows	NAC Agent for Macintosh
File Remediation	Supported	Supported	Not applicable
Link remediation (manual)	Supported	Supported	Supported
Link remediation (automatic)	Not supported	Supported	Not supported
Antivirus remediation (manual)	Not supported	Supported	Supported
Antivirus remediation (automatic)	Not supported	Supported	Not supported
Antispyware remediation (manual)	Not supported	Supported	Not supported
Antispyware remediation (automatic)	Not supported	Supported	Not supported
Launch Program remediation (manual)	Not supported	Supported	Not applicable
Launch Program remediation (automatic)	Not supported	Supported	Not applicable
Windows Update remediation (manual)	Not supported	Supported	Not applicable
Windows Update remediation (automatic)	Not supported	Supported	Not applicable

Table 20-31 Remediation Types Supported by Agents (continued)

Remediation Action Type	Web Agent	NAC Agent for Windows	NAC Agent for Macintosh
Windows Server Update Services remediation (manual)	Not supported	Supported	Not applicable
Windows Server Update Services remediation (automatic)	Not supported	Supported	Not applicable

This section covers the following procedures for managing remediation actions for a posture:

- Viewing, Adding, and Deleting a File Remediation, page 20-115
  - Filtering File Remediations, page 20-116
- Adding, Duplicating, Editing, and Deleting a Link Remediation, page 20-119
  - Filtering Link Remediations, page 20-122
- Adding, Duplicating, Editing, and Deleting an Antivirus Remediation, page 20-125
  - Filtering Antivirus Remediations, page 20-127
- Adding, Duplicating, Editing, and Deleting an Antispyware Remediation, page 20-130
  - Filtering Antispyware Remediations, page 20-133
- Adding, Duplicating, Editing, and Deleting a Launch Program Remediation, page 20-135
  - Filtering Launch Program Remediations, page 20-139
- Adding, Duplicating, Editing, and Deleting a Windows Update Remediation, page 20-142
  - Filtering Windows Update Remediations, page 20-146
- Adding, Duplicating, Editing, and Deleting a Windows Server Update Services Remediation, page 20-149
  - Filtering Windows Server Update Services Remediations, page 20-153

Troubleshooting Topics

- Agent Fails to Initiate Posture Assessment, page D-27

File Remediation

A file remediation allows clients to download the required file version for compliance. You are only allowed to create a file remediation, where the NAC Agent and Web Agent can remediate an endpoint with a file that is required by the client for compliance.

You can filter, view, or delete file remediations on the File Remediations page, but you cannot edit file remediations as you are allowed to edit other remediation types. The File Remediations page displays all the file remediations along with their names, description, and the files that are required for remediation.

This section describes the following procedures to configure and filter file remediations.

- Viewing, Adding, and Deleting a File Remediation, page 20-115
- Filtering File Remediations, page 20-116

Viewing, Adding, and Deleting a File Remediation

This section describes the procedures to view, add, or delete file remediations from the File Remediations page.

To view a file remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **File Remediation**.

The File Remediations page appears, which lists all the file remediations on the File Remediations page.

Step 7 Click the check box to choose a file remediation from the File Remediations page.

Step 8 From the File Remediations page, choose **View**.

Here, you can view a file remediation.

Step 9 Click the **File Remediations List** link to return back to the File Remediations page.

To add a file remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **File Remediation**.

The File Remediations page appears, which lists all the file remediations on the File Remediations page.

Step 7 From the File Remediations page, choose **Add**.

The New File Remediation page appears. Here, you can create to add a new file remediation.

Warning **Once created and saved, the name of the file remediation is not editable.**

Step 8 Modify the values on the New File Remediation page, as shown in Table 20-32.

Step 9 Click **Submit** to save the file remediation.

The new file remediation appears on the File Remediations page.

To delete a file remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **File Remediation**.

The File Remediations page appears, which lists all the file remediations on the File Remediations page.

Step 7 Click the check box to choose a file remediation from the File Remediations page.

Step 8 From the File Remediations page, choose **Delete**.

Here, you can delete a file remediation from the File Remediations page.

Table 20-32 describes the fields that allow you to create a file remediation on the New File Remediation page.

Table 20-32 File Remediation

Field Name	**Field Description**
File Remediation Name	From the File Remediation Name field, enter the name of the file remediation that you want to create.
File Remediation Description	from the File Remediation Description field, enter the description of the file remediation.
Version	From the Version field, add the version of the file.
File to upload	From the File to upload field, browse to the name of the file to be uploaded to the Cisco ISE server. This is in turn the file that is downloaded to the client, if file remediation action is triggered.

Filtering File Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the File Remediations page. A quick filter is a simple and quick filter that can be used to filter file remediations on the File Remediations page. It filters file remediations based on the field description such as the name of the file remediations, description, and the file to be uploaded that is required for remediation on the File Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the File Remediations page. It filters file remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the File Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter file remediations, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **File Remediation**.

Step 7 From the File Remediations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-32.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-117 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-118.

Note To return to the File Remediations page, choose **All** from the Show drop-down to display all the file remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters file remediations based on each field description on the File Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the File Remediations page. If you clear the field, it displays the list of all the file remediations on the File Remediations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter file remediations by using variables that are more complex. It contains one or more filters, which filter file remediations based on the values that match the field description. A filter on a single row filters file remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter file remediations by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-33 describes the fields that allow you to filter file remediations.

Table 20-33 Filtering File Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter file remediations by the name of the file remediation.
	Description	This field enables you to filter file remediations by the description of the file remediation.
	File Name	This field enables you to filter file remediations by the file name.
Advanced Filter	Choose the field description from the following: • Name • Description • File Name	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter file remediations.
	Value	From the Value field, choose the value for the field description that you selected against which to filter file remediations.

Link Remediation

A link remediation allows clients to click a URL link for access to a remediation page, or resource. You can create a link remediation, where the NAC Agents and Web Agents open a browser with a link for clients to access a remediation page or resource, and remediate themselves for compliance.

You can filter, duplicate, edit, or delete link remediations on the Link Remediations page. The Link Remediations page displays all the link remediations along with their names, description, and their modes of remediation.

This section describes the procedures to configure and filter link remediations.

- Adding, Duplicating, Editing, and Deleting a Link Remediation
- Filtering Link Remediations

Adding, Duplicating, Editing, and Deleting a Link Remediation

This section describes the procedures to add, duplicate, edit, or delete link remediations from the Link Remediations page.

To add a link remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Link Remediation**.

The Link Remediations page appears, which lists all the link remediations on the Link Remediations page.

Step 7 From the Link Remediations page, choose **Add**.

The New Link Remediation page appears. Here, you can create to add a new link remediation.

Warning **Once created and saved, the name of the link remediation is not editable.**

Step 8 Modify the values on the New Link Remediation page, as shown in Table 20-34.

Step 9 Click **Submit** to save the link remediation.

The new link remediation appears on the Link Remediations page.

To duplicate a link remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Link Remediation**.

The Link Remediations page appears, which lists all the link remediations on the Link Remediations page.

Step 7 Click the check box to choose a link remediation from the Link Remediations page.

Step 8 From the Link Remediations page, choose **Duplicate**.

Here, you can duplicate a link remediation on the Link Remediations page. You cannot duplicate a link remediation with the same name.

Step 9 Click **Submit** to duplicate a link remediation.

A copy of a link remediation appears on the Link Remediations page.

To edit a link remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Link Remediation**.

The Link Remediations page appears, which lists all the link remediations on the Link Remediations page.

Step 7 Click the check box to choose a link remediation from the Link Remediations page.

Step 8 From the Link Remediations page, choose **Edit**.

Here, you can edit a link remediation on the edit page.

Step 9 Click **Save** to save the link remediation.

The link remediation will be available on the Link Remediations after editing on the edit page.

Step 10 Click the **Link Remediations List** link from the edit page to return to the Link Remediations page.

To delete a link remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Link Remediation**.

The Link Remediations page appears, which lists all the link remediations on the Link Remediations page.

Step 7 Click the check box to choose a link remediation from the Link Remediations page.

Step 8 From the Link Remediations page, choose **Delete**.

Here, you can delete a link remediation from the Link Remediations page.

Table 20-34 describes the fields that allow you to create a link remediation on the New Link Remediation page.

Table 20-34 Link Remediation

Field Name	Field Description
Link Remediation Name	From the Link Remediation Name field, enter the name of the link remediation that you want to create.
Link Remediation Description	From the Link Remediation Description field, enter the description of the link remediation that you want to create.
Remediation Type	From the Remediation Type field, choose the mode that are predefined for a link remediation: • Automatic • Manual—when selected, Retry Count and Interval fields are not editable
Retry Count	From the Retry Count field, enter the number of attempts that clients can try to remediate from the link.
Interval (in seconds)	From the Interval field, enter the time interval in seconds that clients can try to remediate from the link after previous attempts.
URL	A valid URL that clients can access a remediation page or resource to remediate.

Filtering Link Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Link remediations page. A quick filter is a simple and quick filter that can be used to filter link remediations on the Link Remediations page. It filters link remediations based on the field description such as the name of the link remediation, description, and the mode of remediation on the Link Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Link Remediations page. It filters link remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Link Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter link remediations, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Link Remediation**.

Step 7 From the Link Remediations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-35.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-122 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-123.

Note To return to the Link Remediations page, choose **All** from the Show drop-down to display all the link remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters link remediations based on each field description on the Link Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Link Remediations page. If you clear the field, it displays the list of all the link remediations on the Link Remediations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter link remediations by using variables that are more complex. It contains one or more filters, which filter link remediations based on the values that match the field description. A filter on a single row filters link remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter link remediations by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-35 describes the fields that allow you to filter link remediations.

Table 20-35 Filtering Link Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter link remediations by the name of the link remediation.
	Description	This field enables you to filter link remediations by the description of the link remediation.
	Type	This field enables you to filter link remediations by the mode of remediation.

Table 20-35 Filtering Link Remediations (continued)

Filtering Method	Filtering Field	Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter link remediations.
	Value	From the Value field, choose the value for the field description that you selected against which to filter link remediations.

Antivirus Remediation

An antivirus remediation updates clients with antivirus signature definitions for compliance. You can create an antivirus remediation, which updates clients with up-to-date file definitions for compliance after remediation.

You can filter, duplicate, edit, or delete antivirus remediations on the AV Remediations page. The AV Remediations page displays all the antivirus remediations along with their names, description, and their modes of remediation.

This section describes the following procedures to configure and filter antivirus remediations.

- Adding, Duplicating, Editing, and Deleting an Antivirus Remediation
- Filtering Antivirus Remediations

Adding, Duplicating, Editing, and Deleting an Antivirus Remediation

This section describes the procedures to add, duplicate, edit, or delete antivirus remediations from the AV Remediations page.

To add an antivirus remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations on the AV Remediations page.

Step 7 From the AV Remediations page, choose **Add**.

The New AV Remediation page appears. Here, you can create to add a new antivirus remediation.

Warning **Once created and saved, the name of the antivirus remediation is not editable.**

Step 8 Modify the values on the New AV Remediation page, as shown in Table 20-36.

Step 9 Click **Submit** to save an antivirus remediation.

The new antivirus remediation appears on the AV Remediations page.

To duplicate an antivirus remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations on the AV Remediations page.

Step 7 Click the check box to choose an antivirus remediation from the AV Remediations page.

Step 8 From the AV Remediations page, choose **Duplicate**.

Here, you can duplicate an antivirus remediation on the AV Remediations page. You cannot duplicate an antivirus remediation with the same name.

Step 9 Click **Submit** to duplicate an antivirus remediation.

A copy of an antivirus remediation appears on the AV Remediations page.

To edit an antivirus or antispyware remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations on the AV Remediations page.

Step 7 Click the check box to choose an antivirus remediation from the AV Remediations page.

Step 8 From the AV Remediations page, choose **Edit**.

Here, you can edit an antivirus remediation on the edit page.

Step 9 Click **Save** to save the antivirus remediation.

The antivirus remediation will be available on the AV Remediations after editing on the edit page.

Step 10 Click the **AV Remediations List** link from the edit page to return to the AV Remediations page.

To delete an antivirus or antispyware remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AV Remediation**.

The AV Remediations page appears, which lists all the antivirus remediations on the AV Remediations page.

Step 7 Click the check box to choose an antivirus remediation from the AV Remediations page.

Step 8 From the AV Remediations page, choose **Delete**.

Here, you can delete an antivirus remediation from the AV Remediations page.

Table 20-36 describes the fields that allow you to create an antivirus remediation.

Table 20-36 Antivirus Remediation

Field Name	Field Description
Name	From the Name field, enter the name of an antivirus remediation that you want to create.
Description	From the Description field, enter the description of an antivirus remediation.
Remediation Type	From the Remediation Type field, choose the mode that are predefined for an antivirus remediation: • Automatic • Manual—when selected, Interval and Retry Count fields are not editable
Interval (in seconds)	From the Interval field, enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	From the Retry Count field, enter the number of attempts that clients can try to update an antivirus definition.
Operating System	From the Operating System field, choose one of the following options: • Windows • Macintosh—when selected, Remediation Type, Interval, and Retry Count fields are not editable This option specifies the operating system to which AV remediations apply.
AV Vendor Name	Click the drop-down arrow to view the predefined values for antivirus vendors.

Filtering Antivirus Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the AV Remediations page. A quick filter is a simple and quick filter that can be used to filter antivirus remediations on the AV Remediations page. It filters antivirus remediations based on the field description such as the name of the antivirus remediation, description, and as well as the mode of remediation on the AV Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the AV Remediations page. It filters antivirus remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to

manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the AV Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter antivirus remediations, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AV Remediation**.

Step 7 From the AV Remediations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-37.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-128 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-128.

Step 8 From the Show drop-down, choose a preset filter.

The preset filter displays the filtered results on the AV Remediations page.

Note To return to the AV Remediations page, choose **All** from the Show drop-down to display all the antivirus remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters antivirus remediations based on each field description on the AV Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the AV Remediations page. If you clear the field, it displays the list of all the antivirus remediations on the AV Remediations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter antivirus remediations by using variables that are more complex. It contains one or more filters, which filter antivirus remediations based on the values that match the field description. A filter on a single row filters antivirus remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter antivirus remediations by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-37 describes the fields that allow you to filter antivirus remediations.

Table 20-37 Filtering AV Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter antivirus remediations by the name of an antivirus remediation.
	Description	This field enables you to filter antivirus remediations by the description of an antivirus remediation.
	Type	This field enables you to filter antivirus remediations by the mode of remediation.
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter antivirus remediations.
	Value	From the Value field, choose the value for the field description that you selected against which to filter antivirus remediations.

Antispyware Remediation

An antispyware remediation updates clients with antispyware signature definitions for compliance. You can create an antispyware remediation, which updates clients with up-to-date file definitions for compliance after remediation.

You can filter, duplicate, edit, or delete antispyware remediations on the AS Remediations page. The AS Remediations page displays all the antivirus remediations along with their names, description, and their modes of remediation.

This section describes the following procedures to configure and filter antispyware remediations.

- Adding, Duplicating, Editing, and Deleting an Antispyware Remediation
- Filtering Antispyware Remediations

Adding, Duplicating, Editing, and Deleting an Antispyware Remediation

This section describes the procedures to add, duplicate, edit, or delete antispyware remediations from the AS Remediations page.

To add an antispyware remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations on the AS Remediations page.

Step 7 From the AS Remediations page, choose **Add**.

The New AS Remediation page appears. Here, you can create to add a new antispyware remediation.

Warning **Once created and saved, the name of the antispyware remediation is not editable.**

Step 8 Modify the values on the New AS Remediations page, as shown in Table 20-38.

Step 9 Click **Submit** to save an antispyware remediation.

The new antispyware remediation appears on the AS Remediations page.

To duplicate an antispyware remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations on the AS Remediations page.

Step 7 Click the check box to choose an antispyware remediation from the AS Remediations page.

Step 8 From the AS Remediations page, choose **Duplicate**.

Here, you can duplicate an antispyware remediation on the AS Remediations page. You cannot duplicate an antispyware remediation with the same name.

Step 9 Click **Submit** to duplicate an antispyware remediation.

A copy of an antispyware remediation appears on the AS Remediations page.

To edit an antispyware remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations on the AS Remediations page.

Step 7 Click the check box to choose an antispyware remediation from the AS Remediations page.

Step 8 From the AS Remediations page, choose **Edit**.

Here, you can edit an antispyware remediation on the edit page.

Step 9 Click **Save** to save the antispyware remediation.

The antispyware remediation will be available on the AS Remediations after editing on the edit page.

Step 10 Click the **AS Remediations List** link from the edit page to return to the AS Remediations page.

To delete an antispyware remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AS Remediation**.

The AS Remediations page appears, which lists all the antispyware remediations on the AS Remediations page.

Step 7 Click the check box to choose an antispyware remediation from the AS Remediations page.

Step 8 From the AS Remediations page, choose **Delete**.

Here, you can delete an antispyware remediation from the AS Remediations page.

Table 20-38 describes the fields that allow you to create an antispyware remediation:

Table 20-38 Antispyware Remediation

Field Name	Field Description
Name	From the Name field, enter the name of an antispyware remediation that you want to create.
Description	From the Description field, enter the description of an antispyware remediation.
Remediation Type	From the Remediation Type field, choose the mode that are predefined for an antispyware remediation: • Automatic • Manual—when selected, Interval and Retry Count fields are not editable
Interval (in seconds)	From the Interval field, enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	From the Retry Count field, enter the number of attempts that clients can try to update an antispyware definition.
Operating System	From the Operating System field, choose one of the following options: • Windows • Macintosh—when selected, Remediation Type, Interval, and Retry Count fields are not editable This option specifies the operating system to which AS remediations apply.
AS Vendor Name	Click the drop-down arrow to view the predefined values for antispyware vendors.

Filtering Antispyware Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the AS remediations page. A quick filter is a simple and quick filter that can be used to filter antispyware remediations on the AS Remediations page. It filters antispyware remediations based on the field description such as the name of the antispyware remediation, description, and as well as the mode of remediation on the AS Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the AS Remediations page. It filters antispyware remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the AS Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter antispyware remediations, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **AS Remediation**.

Step 7 From the AS Remediations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-39.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-133 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-134.

Note To return to the AS Remediations page, choose **All** from the Show drop-down to display all the antispyware remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters antispyware remediations based on each field description on the AS Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the AS Remediations page. If you clear the field, it displays the list of all the antispyware remediations on the AS Remediations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter antispyware remediations by using variables that are more complex. It contains one or more filters, which filter antispyware remediations based on the values that match the field description. A filter on a single row filters antispyware remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter antispyware remediations by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-39 describes the fields that allow you to filter antispyware remediations.

Table 20-39 Filtering AS Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter antispyware remediations by the name of an antispyware remediation.
	Description	This field enables you to filter antispyware remediations by the description of an antispyware remediation.
	Type	This field enables you to filter antispyware remediations by the mode of remediation.

Table 20-39 Filtering AS Remediations (continued)

Filtering Method	Filtering Field	Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter antispyware remediations.
	Value	From the Value field, choose the value for the field description that you selected against which to filter antispyware remediations.

Launch Program Remediation

A launch program remediation launches one, or more programs on clients for compliance. You can create a launch program remediation, where the NAC Agents and Web Agents remediate clients by launching one, or more applications on clients for compliance.

You can filter, duplicate, edit, or delete launch program remediations on the Launch Program Remediations page. The Launch Program Remediations page displays all the launch program remediations along with their names, description, and their modes of remediation.

This section describes the following procedures to configure and filter launch program remediations.

- Adding, Duplicating, Editing, and Deleting a Launch Program Remediation
- Filtering Launch Program Remediations

Adding, Duplicating, Editing, and Deleting a Launch Program Remediation

This section describes the procedures to add, duplicate, edit, delete launch program remediations from the Launch Program Remediations page.

To add a launch program remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Launch Program Remediation**.

The Launch Program Remediations page appears, which lists all the launch program remediations on the Launch Program Remediations page.

Step 7 From the Launch Program Remediations page, choose **Add**.

The New Launch Program Remediation page appears. Here, you can create to add a new launch program remediation.

Warning **Once created and saved, the name of the launch program remediation is not editable.**

Step 8 Modify the values on the New Launch Program Remediation page, as shown in Table 20-40.

Step 9 Click **Submit** to save the launch program remediation.

The new launch program remediation appears on the Launch Program Remediations page.

To duplicate a launch program remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Launch Program Remediation**.

The Launch Program Remediations page appears, which lists all the launch program remediations on the Launch Program Remediations page.

Step 7 Click the check box to choose a launch program remediation from the Launch Program Remediations page.

Step 8 From the Launch Program Remediations page, choose **Duplicate**.

Here, you can duplicate a launch program remediation on the Launch Program Remediations page. You cannot duplicate a launch program remediation with the same name.

Step 9 Click **Submit** to duplicate a launch program remediation.

A copy of a launch program remediation appears on the Launch Program Remediations page.

To edit a launch program remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Launch Program Remediation**.

The Launch Program Remediations page appears, which lists all the launch program remediations on the Launch Program Remediations page.

Step 7 Click the check box to choose a launch program remediation from the Launch Program Remediations page.

Step 8 From the Launch Program Remediations page, choose **Edit**.

Here, you can edit a launch program remediation on the edit page.

Step 9 Click **Save** to save the launch program remediation.

The launch program remediation will be available on the Launch Program Remediations after editing on the edit page.

Step 10 Click the **Launch Program Remediations List** link from the edit page to return to the Launch Program Remediations page.

To delete a launch program remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Launch Program Remediation**.

The Launch Program Remediations page appears, which lists all the launch program remediations on the Launch Program Remediations page.

Step 7 Click the check box to choose a launch program remediation from the Launch Program Remediations page.

Step 8 From the Launch Program Remediations page, choose **Delete**.

Here, you can delete a launch program remediation from the Launch Program Remediations page.

Table 20-40 describes the fields that allow you to create a launch program remediation.

Table 20-40 Launch Program Remediation

Field Name	Field Description
Name	From the Name field, enter the name of the launch program remediation that you want to create.
Description	From the Description field, enter the description of the launch program remediation that you want to create.
Remediation Type	From the Remediation Type field, choose the mode that are predefined to launch programs: • Automatic • Manual
Interval (in seconds)	From the Interval field, enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	From the Retry Count field, enter the number of attempts that clients can try to launch required programs.
Program Installation Path	From the Program Installation Path field, choose the path in which a remediation program has to be installed. Click the drop-down arrow to view the following predefined paths to installing programs: • ABSOLUTE_PATH—remediation program is installed in the fully qualified path of the file. For example, C:\<directory>\ • SYSTEM_32—remediation program is installed in the C:\WINDOWS\system32 directory • SYSTEM_DRIVE—remediation program is installed in the C:\ drive • SYSTEM_PROGRAMS—remediation program is installed in the C:\Program Files • SYSTEM_ROOT—remediation program is installed in the root path for Windows system
Program Executable	From the Program Executable field, enter the name of the remediation program executable, or an installation file.
Program Parameters	From the Program Parameters field, enter (optional) required parameters for the remediation programs.
Existing Programs	An area to display the installation paths of existing remediation programs, the name of the remediation programs installed, and parameters if any. Add—to add remediation programs to the list after entering program executable, or an installation file. Delete—to delete remediation programs from the list.

Filtering Launch Program Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Launch Program Remediations page. A quick filter is a simple and quick filter that can be used to filter launch program remediations on the Launch Program Remediations page. It filters launch program remediations based on the field description such as the name of the launch program remediations, description, and as well as the mode of remediation on the Launch Program Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Launch Program Remediations page. It filters launch program remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Launch Program Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter launch program remediations, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Launch Program Remediation**.

Step 7 From the Launch Programs Remediations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-41.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-139 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-140.

Note To return to the Launch Program Remediations page, choose **All** from the Show drop-down to display all the launch program remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters launch program remediations based on each field description on the Launch Program Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Launch Program Remediations page. If you clear the field, it displays the list of all the launch program remediations on the Launch Program Remediations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter launch program remediations by using variables that are more complex. It contains one or more filters, which filter launch program remediations based on the values that match the field description. A filter on a single row filters launch program remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter launch program remediations by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-41 describes the fields that allow you to filter launch program remediations.

Table 20-41 Filtering Launch Program Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter launch program remediations by the name of the program remediation.
	Description	This field enables you to filter launch program remediations by the description of the program remediation.
	Type	This field enables you to filter launch program remediations by type.

Table 20-41 Filtering Launch Program Remediations (continued)

Filtering Method	Filtering Field	Field Description
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter launch program remediations.
	Value	From the Value field, choose the value for the field description that you selected against which to filter launch program remediations.

Windows Update Remediation

A Windows update remediation ensures that Automatic Updates configuration is turned on Windows clients per your security policy, and helps you to ensure that Automatic Updates remediates Windows clients to result in successful posture assessments for compliance.

You can filter, duplicate, edit, or delete Windows update remediations from the Windows Update Remediations page. The Windows Update Remediations page displays all the Windows update remediations along with their names, description, and as well as their modes of remediation.

This section describes the following procedures to configure and filter Windows update remediations.

- Adding, Duplicating, Editing, and Deleting a Windows Update Remediation
- Filtering Windows Update Remediations

Windows Automatic Updates

The Windows administrators have an option to turn on or turn off Automatic Updates on Windows clients. The Microsoft Windows uses this feature to regularly check for important updates and install them on your clients. If the Automatic Updates feature is turned on, then the Windows automatically updates Windows-recommended updates before any other updates.

Windows XP provides the following settings for configuring Automatic Updates:

- Automatic (recommended)—Windows allows clients automatically download recommended Windows updates for their computers and install them
- Download updates for me, but let me choose when to install them—Windows downloads updates for clients, and allows clients to choose when to install them
- Notify me but don't automatically download or install them—Windows only notifies clients, but does not automatically download, or install them
- Turn off Automatic Updates—Windows allows clients to turn off Windows Automatic Updates feature. Here, clients are vulnerable unless clients install updates regularly. They can install updates from the Windows Update Web site link.

Note The Windows Automatic Updates setting will differ for different Windows operating systems.

You can create a Windows update remediation to check for the Windows updates service (wuaserv) whether the service is started or stopped in any Windows client by using the **pr_AutoUpdateCheck_Rule**. It is a predefined Cisco rule, which can be used to create a posture requirement. If the posture requirement fails, the remediation action (Windows update remediation) that you associate to the requirement enforces the Windows client to remediate by using one of the automatic updates options.

Override User's Windows Update Setting With Administrator's Option in Windows Update Remediations

You can enable the "Override User's Windows Update setting with administrator's" option to override the user's with remediation settings, or else you can disable the option.

Note The users setting are not restored back here to their original setting even after they exit from NAC Agents, or when they reboot their Windows clients, or when they restart the Windows Automatic Updates service on their Windows clients.

If "Override User's Windows update setting with administrator's" option is disabled, Windows update remediations will not be enforced except for "Turn Off Automatic Updates" settings on Windows clients.

Windows update remediations will fail when you want to change the Windows Automatic Updates setting:

- From Automatic (recommended) to Download updates for me, but let me choose when to install them and vice versa.
- From Automatic (recommended) to Notify me but don't automatically download or install them and vice versa.
- From Notify me but don't automatically download or install them to Download updates for me, but let me choose when to install them and vice versa.

Adding, Duplicating, Editing, and Deleting a Windows Update Remediation

This section describes the procedures to add, duplicate, edit, or delete Windows update remediations from the Windows Update Remediations page.

To add a Windows update remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations on the Windows Update Remediations page.

Step 7 From the Windows Update Remediations page, choose **Add**.

The New Windows Update Remediation page appears. Here, you can create to add a new Windows update remediation.

Warning **Once created and saved, the name of the Windows update remediation is not editable.**

Step 8 Modify the values on the New Windows Update Remediation page, as shown in Table 20-42.

Step 9 Click **Submit** to save the Windows update remediation.

The new Windows update remediation appears on the Windows update remediations page.

To duplicate a Windows update remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations on the Windows Update Remediations page.

Step 7 Click the check box to choose a Windows update remediation from the Windows Update Remediations page.

Step 8 From the Windows Update Remediations page, choose **Duplicate**.

Here, you can duplicate a Windows update remediation on the Windows Update Remediations page. You cannot duplicate a Windows update remediation with the same name.

Step 9 Click **Submit** to duplicate a Windows update remediation.

A copy of a Windows update remediation appears on the Windows Update Remediations page.

To edit a Windows update remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations on the Windows Update Remediations page.

Step 7 Click the check box to choose a Windows update remediation from the Windows Update Remediations page.

Step 8 From the Windows Update Remediations page, choose **Edit**.

Here, you can edit a Windows update remediation on the edit page.

Step 9 Click **Save** to save the Windows update remediation.

The Windows update remediation will be available on the Windows Update Remediations after editing on the edit page.

Step 10 Click the **Windows Update Remediations List** link from the edit page to return to the Windows Update Remediations page.

To delete a Windows update remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Windows Update Remediation**.

The Windows Update Remediations page appears, which lists all the Windows update remediations on the Windows Update Remediations page.

Step 7 Click the check box to choose a Windows update remediation from the Windows Update Remediations page.

Step 8 From the Windows Update Remediations page, choose **Delete**.

Here, you can delete a Windows update remediation from the Windows Update Remediations page.

Table 20-42 describes the fields that allow you to create a Windows update remediation:

Table 20-42 Windows Update Remediation

Field Name	Field Description
Name	From the Name field, enter the name of the Windows update remediation that you want to create.
Description	From the Description field, enter the description of the Windows update remediation.
Remediation Type	From the Remediation Type field, choose the mode that are predefined for Windows updates: • Automatic • Manual—when selected, Interval and Retry Count fields are not editable
Interval (in seconds)	From the Interval field, enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	From the Retry Count field, enter the number of attempts that Windows clients can try for Windows updates.
Windows Update Setting	Cisco ISE provides the following four options for Windows update remediations: **a.** Do not change setting—If selected, the Windows Automatic Updates client configuration does not change during, or after Windows update remediation. **b.** Notify to download and install—Windows only notifies clients, but does not automatically download, or install them. If selected, Windows only notifies clients to download, or install Windows updates. **c.** Automatically download and notify to install—Windows downloads updates for clients, and allows them to choose when to install them. If selected, Windows automatically downloads, and notifies clients to install Windows updates. **d.** Automatically download and install—Windows allows clients automatically download recommended Windows updates for their computers and install them. If selected, Windows automatically downloads, and installs Windows updates. This is the highly recommended setting from Windows for Windows clients. Click the drop-down arrow to choose an option for Automatic Updates setting on Windows clients.

Table 20-42 Windows Update Remediation (continued)

Field Name	Field Description
Override User's Windows Update setting with administrator's check box.	A check box, which allows Cisco ISE administrators to override Automatic Updates configuration of Windows clients. If checked, the setting enforces the Cisco ISE administrator-specified setting for Windows Automatic Updates on all the client machines during, and after Windows update remediation. If unchecked, the setting enforces the following: • The Cisco ISE administrator-specified setting only when Automatic Updates are disabled on Windows clients. • The Windows clients-specified setting only when Windows Automatic Updates are enabled on the client.

Filtering Windows Update Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Windows Update Remediations page. A quick filter is a simple and quick filter that can be used to filter Windows update remediations on the Windows Update Remediations page. It filters Windows update remediations based on the field description such as the name of the Windows update remediations, description, and as well as the mode of remediation on the Windows Update Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Windows Update Remediations page. It filters Windows update remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Windows Update Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter Windows update remediations, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Step 6 Choose **Windows Update Remediation**.

Step 7 From the Windows Update Remediations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-43.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-147 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-147.

Note To return to the Windows Update Remediations page, choose **All** from the Show drop-down to display all the Windows update remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters Windows update remediations based on each field description on the Windows Update Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Windows Update Remediations page. If you clear the field, it displays the list of all the Windows update remediations on the Windows Update Remediations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter Windows update remediations by using variables that are more complex. It contains one or more filters, which filter Windows update remediations based on the values that match the field description. A filter on a single row filters Windows update remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter Windows update remediations by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-43 describes the fields that allow you to filter Windows update remediations:

Table 20-43 Filtering Windows Update Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter Windows update remediations by the name of the Windows update remediation.
	Description	This field enables you to filter Windows update remediations by the description of the Windows update remediation.
	Type	This field enables you to filter Windows update remediations by type.
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter Windows update remediations.
	Value	From the Value field, choose the value for the field description that you selected against which to filter Windows update remediations.

Windows Server Update Services Remediation

A Windows Server Update Services (WSUS) remediation remediates Windows clients from a locally managed WSUS server, or a Microsoft-managed WSUS server with the latest Windows service packs, hotfixes, and patches (WSUS updates) for compliance.

You can create a WSUS remediation where a NAC Agent integrates with the local WSUS Agent to check whether the endpoint is up-to-date for WSUS updates. You can filter, duplicate, edit or delete WSUS remediations from the remediations list. You can configure Windows clients to receive the latest WSUS updates from a Microsoft-managed WSUS server, or locally administered WSUS server for compliance.The Windows Server Update Services (WSUS) Remediations page displays all the WSUS remediations along with their names, description, and as well as their modes of remediation.

Note When you associate a WSUS remediation action to a posture requirement to validate Windows updates by using the severity level option, you must choose the pr_WSUSRule (a dummy compound condition) compound condition in the posture requirement. When the posture requirement fails, the NAC Agent enforces the remediation action (Windows updates) based on the severity level that you define in the WSUS remediation.

This section describes the following procedures to configure and filter WSUS remediations.

- Adding, Duplicating, Editing, and Deleting a Windows Server Update Services Remediation

- Filtering Windows Server Update Services Remediations

Adding, Duplicating, Editing, and Deleting a Windows Server Update Services Remediation

This section describes the procedures to add, duplicate, edit, or delete WSUS remediations from the Windows Server Update Services Remediations page.

To add a Windows server update services remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Windows Server Update Services Remediation**.

The Windows Server Update Services Remediations page appears, which lists all the WSUS remediations on the Windows Server Update Services Remediations page.

Step 7 From the Windows Server Update Services Remediations page, choose **Add**.

The New Windows Server Update Services Remediation page appears. Here, you can create to add a new WSUS remediation.

Warning **Once created and saved, the name of the Windows server update services remediation is not editable.**

Step 8 Modify the values on the New Windows Server Update Services Remediation page, as shown in Table 20-44.

Step 9 Click **Submit** to save the WSUS remediation.

The new WSUS remediation appears on the Windows Server Update Services Remediations page.

To duplicate a Windows server update services remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Windows Server Update Services Remediation**.

The Windows Server Update Services Remediations page appears, which lists all the WSUS remediations on the Windows Server Update Services Remediations page.

Step 7 Click the check box to choose a WSUS remediation from the Windows Server Update Services Remediations page.

Step 8 From the Windows Server Update Services Remediations page, choose **Duplicate**.

Here, you can duplicate a WSUS remediation on the Windows Server Update Services Remediations page. You cannot duplicate a WSUS remediation with the same name.

Step 9 Click **Submit** to duplicate a WSUS remediation.

A copy of a WSUS remediation appears on the Windows Server Update Services Remediations page.

To edit a Windows server update services remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Windows Server Update Services Remediation**.

The Windows Server Update Services Remediations page appears, which lists all the WSUS remediations on the Windows Server Update Services Remediations page.

Step 7 Click the check box to choose a WSUS remediation from the Windows Server Update Services Remediations page.

Step 8 From the Windows Server Update Services Remediations page, choose **Edit**.

Here, you can edit a WSUS remediation on the edit page.

Step 9 Click **Save** to save the WSUS remediation.

The WSUS remediation will be available on the Windows Server Update Services Remediations after editing on the edit page.

Step 10 Click the **Windows Server Update Services Remediations List** link to return back to the WSUS remediation list page.

To delete a Windows server update services remediation, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Remediation Actions menu window displays the choices for remediation actions.

Step 6 Choose **Windows Server Update Services Remediation**.

The Windows Server Update Services Remediations page appears, which lists all the WSUS remediations on the Windows Server Update Services Remediations page.

Step 7 Click the check box to choose a WSUS remediation from the Windows Server Update Services Remediations page.

Step 8 From the Windows Server Update Services Remediations page, choose **Delete**.

Here, you can delete a WSUS remediation from the Windows Server Update Services Remediations page.

Table 20-44 describes the fields that allow you to create a WSUS remediation.

Table 20-44 WSUS Remediation

Field Name	Field Description
Name	From the Name field, enter the name of the WSUS remediation that you want to create.
Description	From the Description field, enter the description of the WSUS remediation that you want to create.
Remediation Type	From the Remediation Type field, choose the mode that are predefined for WSUS remediations. The following options are available: • Automatic—The NAC Agents automatically updates Windows clients with the latest WSUS updates. • Manual—When it is selected, Interval and Retry Count fields are nor editable. The user manually updates the Windows client with the latest WSUS updates from a Microsoft-managed WSUS server, or from the locally administered WSUS server for compliance.
Interval (in seconds)	From the Interval field, you can specify the interval in seconds (the default interval is 0) to delay WSUS updates before the NAC Agents and Web Agents attempt to retry after the previous attempt.
Retry Count	From the Retry Count field, you can set a limit on the number of attempts that the NAC Agents and web Agents retry to update Windows clients with WSUS updates.

Table 20-44 WSUS Remediation (continued)

Field Name	Field Description
Validate Windows updates using	The validation method that you use to check the Windows operating system that is installed on the client for Windows updates. The available options are: • Cisco Rules • Severity Level
Cisco Rules radio button	The validation method that you will use to check the client Windows operating system to meet minimum security standards as a result of dynamic posture updates downloaded to the Cisco ISE server. Click the Cisco Rules radio button to validate WSUS updates using Cisco Rules. If selected, custom or pre-configured rules must be selected as conditions in the posture requirement.
Severity Level radio button	The validation method that you will use to check the client Windows operating system to meet minimum security standards by using a Microsoft-managed WSUS server, or locally administered WSUS server. Click the Security Level radio button to validate WSUS updates based on the Security Level set on the WSUS server. If selected, custom or pre-configured rules can be selected as conditions in the posture requirement, but they are not used. For this purpose, the pr_WSUSRule can be used as a placeholder condition (a dummy condition) in the posture requirement that specifies a WSUS remediation.
Windows Updates Severity Level	The severity level of Windows updates that you select to install on Windows clients. The following are the severity levels of WSUS updates that you can install on Windows clients: • Critical—Installs only critical Windows updates • Express—Installs important and critical Windows updates • Medium—Installs all critical, important and moderate Windows updates • All—Installs all critical, important, moderate and low Windows updates
Update to latest OS Service Pack check box	If checked, then the WSUS remediation installs the latest service pack available for the client's operating system automatically. **Note** The operating system service packs are updated automatically irrespective of the Medium and All severity level options selected in WSUS remediation.

Table 20-44 WSUS Remediation (continued)

Field Name	Field Description
Windows Updates Installation Source	This selection specifies the source from where you install WSUS updates on Windows clients: • Microsoft server—Microsoft-managed WSUS server • Managed server—Locally administered WSUS server
Installation Wizard Interface Setting	An option to display the installation wizard on the client during WSUS updates: • Show UI—an option to display the Windows Update Installation Wizard progress on Windows clients. (Users must have Administrator privileges on client machines in order to see the installation wizard user interface during WSUS updates.) • No UI—an option to hide the Windows Update Installation Wizard progress on Windows clients.

Filtering Windows Server Update Services Remediations

You can use the Show drop-down list, or click the filter icon to invoke a quick filter and close it as well on the Windows Server Update Services Remediations page. A quick filter is a simple and quick filter that can be used to filter WSUS remediations on the Windows Server Update Services Remediations page. It filters WSUS remediations based on the field description such as the name of the WSUS remediations, description, and the mode of remediation on the Windows Server Update Services Remediations page.

You can use the Show drop-down list to invoke an advanced filter. An advanced filter is a complex filter that can also be preset for use later and retrieved, along with the results on the Windows Server Update Services Remediations page. It filters WSUS remediations based on a specific value associated with the field description. You can add or remove filters, as well as combine a set of filters into a single advanced filter.

You can use the Manage Preset Filters option which lists all the preset filters. This option allows you to manage preset filters. Once created and saved a preset filter, you can choose a preset filter from the list which displays the results on the Windows Server Update Services Remediations page. You can also edit preset filters and remove them from the preset filters list.

To filter WSUS remediations, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results menu window, choose **Posture**.

Step 3 Click the **Quick Picker** icon to navigate to posture result types.

Remediation Actions and Requirements appear for posture result types.

Step 4 Choose **Remediation Actions**.

Step 5 Click the **Quick Picker** icon to navigate to Remediation Actions types.

Step 6 Choose **WSUS Server Update Services Remediation**.

Step 7 From the Windows Server Update Services Remediations page, click the drop-down arrow of Show to list the filter options.

Here, you can choose a Quick Filter, an Advanced Filter for filtering, or Manage Preset Filters option which allows you to manage preset filters for filtering. See Table 20-45.

For more information, see the "To filter by using the Quick Filter option, complete the following steps:" section on page 20-154 and "To filter by using the Advanced Filter option, complete the following steps:" section on page 20-154.

Note To return to the Windows Server Update Services Remediations page, choose **All** from the Show drop-down to display all the WSUS remediations without filtering.

To filter by using the Quick Filter option, complete the following steps:

A quick filter filters WSUS remediations based on each field description on the Windows Server Update Services Remediations page. When you click inside in any field, and as you enter the search criteria in the field, it refreshes the page with the results on the Windows Server Update Services Remediations page. If you clear the field, it displays the list of all the WSUS remediations on the Windows Server Update Services Remediations page.

Step 1 To filter, click the **Go** button within each field.

Step 2 To clear the field, click the **Clear** button within each field.

To filter by using the Advanced Filter option, complete the following steps:

An advanced filter enables you to filter WSUS remediations by using variables that are more complex. It contains one or more filters, which filter WSUS remediations based on the values that match the field description. A filter on a single row filters WSUS remediations based on each field description and the value that you define in the filter. Multiple filters can be used to match the value(s) and filter WSUS remediations by using any one or all the filters within a single advanced filter.

Step 1 To view and choose the field description, click the drop-down arrow.

Step 2 To view and choose the operator, click the drop-down arrow.

Step 3 Enter the value for the field description that you selected.

Step 4 Click the **Add Row** (plus [+] sign) button to add a filter, or click the **Remove Row** (minus [-] sign) button to remove the filter.

Step 5 Choose **All** to match the value in each filter, or **Any** to match the value in any one of the filters.

Step 6 Click **Go** to start filtering.

Step 7 Click the **Save** icon to save the filter.

The Save a Preset Filter dialog appears. Enter a file name to save the filter and click **Save**, or **Cancel** to clear the filter.

Table 20-45 describes the fields that allow you to filter WSUS remediations.

Table 20-45 Filtering Windows Server Update Services Remediations

Filtering Method	Filtering Field	Field Description
Quick Filter	Name	This field enables you to filter WSUS remediations by the name of the WSUS remediation.
	Description	This field enables you to filter WSUS remediations by the description of the WSUS remediation.
	Type	This field enables you to filter WSUS remediations by type.
Advanced Filter	Choose the field description from the following: • Name • Description • Type	Click the drop-down arrow to choose the field description.
	Operator	From the Operator field, click the drop-down arrow to choose an operator that can be used to filter WSUS remediations.
	Value	From the Value field, choose the value for the field description that you selected against which to filter WSUS remediations.

Client Posture Assessment Requirements

Prerequisite

You must have an understanding of Acceptable Use Policy (AUP) for a posture as you create posture requirements. Refer to the following location on AUP with respect to posture compliance:

Administration > System > Settings > Posture > Acceptable Use policy.

For more information on AUP, see Posture Acceptable Use Policy, page 20-24.

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role in conjunction with an operating system. All the clients that are connecting to your network must meet mandatory requirements during posture policies evaluation, which are associated to posture policies in order to become compliant on your network. If requirements are optional and clients fail these requirements, then the clients have an option to continue further so that end users can skip optional requirements even though they fail during policy evaluation.

If clients fail to meet mandatory requirements during posture policies evaluation, then they are denied network access to your network, and they are moved into a quarantine state forever. If clients are moved into the quarantine state, they will not be to reauthenticate again in order to be postured successfully for compliance again. If clients need to come out of the quarantine state in order to become compliant, then the network access devices must be configured to restart a new RADIUS session after the session times out so that clients can reauthenticate again in order to meet mandatory requirements for compliance.

For information on configuration guidance of posture clients quarantine state, see "Authorization Profile Configuration Guidance for Posture Clients Quarantine State" section on page 20-25.

pr_WSUSRule

The pr_WSUSRule is a dummy compound condition, which is used in a posture requirement with a Windows Server Update Services (WSUS) remediation associated to it. The associated WSUS remediation action must be configured to validate Windows updates by using the severity level option. When this requirement fails, the NAC Agent that is installed on the Windows client enforces the WSUS remediation action based on the severity level that you define in the WSUS remediation.

Note The pr_WSUSRule cannot be viewed in the Compound conditions list page. You can only select the pr_WSUSRule from the Conditions widget.

You can use the Posture Requirements page to insert (create) a new requirement, or duplicate an existing requirement, or delete an existing requirement.

Creating User Defined Conditions and Remediation Actions

Cisco ISE allows you to create and associate user defined conditions, associate Cisco defined conditions, and create and associate remediation actions on the Requirements page itself that simplifies requirement configuration without navigating to their respective pages. Once created and saved on the Requirements page, these user defined conditions and remediation actions can be viewed from their respective lists.

Table 20-46 describes the fields on the Posture Requirements page that allow you to insert a new posture requirement, or duplicate an existing requirement or delete an existing posture requirement.

Table 20-46 Posture Requirement

Field	Field Description
Name	From the Name field, enter the name of the requirement that you want to create.
Operating Systems	From the Operating Systems field, choose an operating system. It allows you to select all, or specific Windows, or Macintosh operating systems to which the posture requirement is applied.
Conditions	From the Conditions field, choose one or more dictionary simple conditions, and dictionary compound conditions to which the posture requirement should apply. If more than one condition is selected, then all the conditions must be met (a logical AND operation) to form a compound condition. The system uses "&" as the AND operator. The conditions are defined in the following location: **Policy > Policy Elements > Conditions > Posture.** For more information on the posture conditions, see the Custom Conditions for Posture, page 20-42.

Table 20-46 Posture Requirement (continued)

Field	Field Description
Remediation Actions	The remediation action defines the action to be taken when the posture requirement fails on the client. The remediation actions are defined in the following location: **Policy > Policy Elements > Results > Posture > Remediation Actions**. For information on the posture remediation actions, see the Custom Posture Remediation Actions, page 20-112.

For more information on how to manage posture requirements, see the "Creating, Duplicating, and Deleting Client Posture Requirements" section on page 20-157

Related Topics

Client Posture Assessment Policies, page 20-33

Custom Posture Remediation Actions, page 20-112

Creating, Duplicating, and Deleting Client Posture Requirements

This section describes the following procedures on how to insert (create) a new requirement, or duplicate an existing requirement, or delete an existing requirement on the Posture Requirements page.

- Creating a New Posture Requirement, page 20-157
- Duplicating a Posture Requirement, page 20-161
- Deleting a Posture Requirement, page 20-161

Creating a New Posture Requirement

You can create a new posture requirement on the Requirements page.

To insert a new requirement, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Posture > Requirements**.

Step 2 Choose **Requirements**.

The Posture Requirements page appears.

Step 3 Enter the requirement name.

Warning **The operating system is also not editable on the posture requirement after you have associated the newly created requirement to a posture policy. In order to edit the operating system on the requirement, you need to remove the posture requirement association from the posture policy.**

Step 4 From the Operating Systems field, choose **Select Operating Systems**.

To choose an operating system, complete the following steps:

a. From the Select Operating System field, click the plus [+] sign to expand the operating system anchored overlay.

   The operating system anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the Select Operating System **Quick Picker** (down arrow) icon.

   The Operating System Groups widget appears.

c. From the Operating System Groups widget, choose **All**.

   Here, click the **Quick Picker** (right arrow) icon to view the operating system groups.

d. From the All widget, choose the operating system group.

   The parent groups for the operating system appears.

e. Choose the parent operating system group.

   - For Mac OS X (Macintosh), the group has three underlying versions.
   - For Windows All, the group has the Windows 7 (All), Windows Vista (All), and Windows XP (All) groups that contain underlying versions for each of the groups.

f. From the Mac OS X (Macintosh) group, choose the underlying Macintosh operating system.

g. From the Windows All group, choose the underlying Windows group and the Windows version.

   Each Windows group contains its own underlying versions.

h. Click the **Add** (plus [+] sign) button to associate more than one operating system to the policy.

i. Click the **Remove** (minus [-] sign) button to remove the operating system from the policy.

Step 5 From the Conditions field, choose **Select Conditions**.

To choose a condition, complete the following steps:

a. From the Conditions field, click the plus [+] sign to expand the conditions anchored overlay.

   The conditions anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the Select Conditions **Quick Picker** (down arrow) icon.

   The Conditions widget appears. The Conditions widget lists User Defined Conditions and Cisco Defined Conditions. Here, you can create a user defined condition that can be saved to the respective user defined conditions list.

c. From the Conditions widget, choose **User Defined Conditions**.

   The Table view button shows the list of user defined conditions in a row format in the right pane of the widget. The Tree view button shows the list of user defined conditions in a tree format under the user defined conditions.

To choose a user defined condition, complete the following steps:

d. Click the **Quick Picker** (right arrow) to view the list of user defined conditions.

   Here, you can choose one of the following user defined conditions:

   - File Conditions
   - Registry Conditions
   - Service Conditions
   - Application Conditions

- Regular Compound Condition
- AV Compound Condition
- AS Compound Condition

e. Click the **Quick Picker** (right arrow) to view the list of each user defined condition.

Here, you can choose a user defined condition from the list.

To create a user defined condition from the Conditions widget, complete the following steps:

You cannot edit the associated parent operating system while creating user defined conditions on the Requirements page.

a. Click the Select Conditions **Quick Picker** (down arrow) icon.

The Conditions widget appears. The Condition widget lists User Defined Conditions and Cisco Defined Conditions.

b. Click the **Quick Picker** (down arrow) on the **Action** button.

Here, you can create any user defined condition that allows you to save it to the existing list of respective user defined conditions, as well as associate it from the Requirements page.

c. Choose one of the user defined conditions from the following conditions:

- Create File Condition

  The Add File Condition widget appears. Here, you can create a file (simple) condition.

- Create Registry Condition

  The Add Registry Condition widget appears. Here, you can create a registry (simple) condition.

- Create Application Condition

  The Add Application Condition widget appears. Here, you can create an application (simple) condition.

- Create Service Condition

  The Add Service Condition widget appears. Here, you can create a service (simple) condition.

- Create Compound Condition

  The Add Compound Condition widget appears. Here, you can create a regular compound condition where you can add simple file conditions, registry conditions, application conditions and service conditions and form a compound condition by using AND. OR, NOT logical operators.

- Create AV Compound Condition

  The Add AV Compound Condition widget appears. Here, you can create an AV compound condition.

- Create AS Compound Condition

  The Add AS Compound Condition widget appears. Here, you can create an AS compound condition.

d. Click **Save and Select**.

Once created, the user defined condition can be saved to the existing list of respective user defined conditions, as well as associated to the requirements from the Requirements page.

To choose a Cisco defined condition, complete the following steps:

a. From the Conditions widget, choose **Cisco Defined Conditions**.

The Table view button shows the list of Cisco defined conditions in a row format in the right pane of the widget. The Tree view button shows the list of Cisco defined conditions in a tree format under the compound conditions.

b. Click the **Quick Picker** (right arrow) to view to view the list of each Cisco defined conditions.

Here, you can choose one of the following Cisco defined conditions:

- File Conditions
- Registry Conditions
- Service Conditions
- Application Conditions
- Regular Compound Condition

  pr_WSUSRule is a dummy compound condition. For more information, see the pr_WSUSRule, page 20-156.
- AV Compound Condition
- AS Compound Condition

c. Choose a Cisco defined condition.

To associate one or more conditions to the requirement, complete the following steps:

a. Click the **Add** (plus [+] sign) button to associate more than one condition to the requirement.

b. Click the **Remove** (minus [-] sign) button to remove the condition from the requirement.

To validate associated conditions in a requirement, complete the following step:

a. Choose one of the following options:

- All selected conditions succeed
- Any selected condition succeeds
- No selected condition succeeds

Step 6 From the Remediations Actions field, choose **Select Remediations**.

To choose a remediation action, complete the following steps:

a. From the Remediation Actions field, click the plus [+] sign to expand the remediation anchored overlay.

The Remediations anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

b. Click the Select Remediations **Quick Picker** (down arrow) icon.

The Remediations widget appears.

c. Choose the remediation action.

For Message Text only action, enter appropriate information in text so that the NAC Agent displays it on the client. For more information, see the Message Text Only, page 20-112.

To create a remediation action, complete the following steps:

a. Click the Select Remediation **Quick Picker** (down arrow) icon.

The Remediation widget appears, which lists all the remediation actions.

b. Click the **Quick Picker** (down arrow) on the **Action** button.

Here, you can create a remediation action that allows you to save it to the existing list of respective remediation actions, as well as associate it from the Requirements page.

c. Choose one of the remediation actions from the following:

- Create AV Remediation

  The Add AV Remediation widget appears. Here, you can create an AV remediation.

- Create AS Remediation

  The Add AS Remediation widget appears. Here, you can create an AS remediation.

- Create File Remediation

  The Add File Remediation widget appears. Here, you can create a file remediation.

- Create Launch Program Remediation

  The Add Launch Program Remediation widget appears. Here, you can create a launch program remediation.

- Create Link Remediation

  The Add Link Remediation widget appears. Here, you can create a link remediation.

- Create Windows Server Update Services Remediation

  The Add Windows Server Update Services Remediation widget appears. Here, you can create a WSUS remediation.

- Create Windows Update Remediation

  The Add Windows Update Remediation widget appears. Here, you can create a Windows update remediation.

d. Click **Save and Select**.

Once created, the remediation actions can be saved to the existing list of respective remediation actions list, as well as associated to the requirements from the Requirements page.

Step 7 Click **Save** to save the posture requirement.

Duplicating a Posture Requirement

You can create a copy of a posture requirement that you want to duplicate on the Requirements page.

To duplicate a requirement, complete the following steps:

Step 1 Click the **Action Icon** button.

Step 2 Choose **Duplicate**.

Here, you can create a copy of the requirement that you want to duplicate on the Requirements page.

Deleting a Posture Requirement

You can also delete a posture requirement from the Requirements page.

To delete a requirement, complete the following steps:

Step 1 Click the **Action Icon** button.

Step 2 Choose **Delete**.

Here, you can delete a requirement from the Requirements page.

Custom Authorization Policies for Posture

This section describes the standard authorization policies that you define for posture in the Cisco ISE appliance.

You can define two types of authorization policies on the Authorization Policy page, the standard authorization policies and the exceptions authorization policies. The standard authorization policies that are specific to posture on the Authorization Policy page are used to make policy decisions (enforce policies) based on the compliance status of endpoints such as unknown, compliant, and noncompliant. The standard authorization profiles (permissions) that you define on the Authorization Profiles page set access privileges based on the matching compliance status.

You can create posture-specific authorization policies for all wired, wireless, and guest deployments by specifying the Session:PostureStatus attribute in the authorization policies. This attribute has three values, unknown, compliant, and noncompliant, which you can use n the authorization policies.

First Matched Rule Applies

With this option selected, one or more authorization profiles (permissions) that are defined in the authorization policy set the access privileges (authorization) for an end user based on the first matching authorization policy during evaluation.

The selection of First Matched Rule Applies option allows you to configure authorization profiles for an end user by applying the first matching authorization policy from the standard authorization policies that are enabled on the Authorization Policy page. Cisco ISE evaluates the standard authorization policies that are enabled on the Authorization Policy page and then determines the authorization profile, or authorization profiles that are associated in the standard authorization policies. Once the first matching authorization policy is found, Cisco ISE stops evaluating the rest of the standard authorization policies on the Authorization Policy page.

Multiple Matched Rule Applies

With this option selected, one or more authorization profiles that are defined in the authorization policies determine the access privileges for an end user based on multiple matching authorization policies during evaluation.

The selection of Multiple Matched Rule Applies option allows you to configure authorization profiles for an end user by applying multiple matching authorization policies from the standard authorization policies that are enabled on the Authorization Policy page. Cisco ISE evaluates all the standard authorization policies that are enabled on the Authorization Policy page and finds all the matching authorization policies on the Authorization Policy page. When multiple matching authorization policies are found, Cisco ISE determines the authorization profile or profiles for the end user.

Prerequisites:

Before you begin, you should have an understanding of authorization policies in Cisco ISE.

For information on the authorization policies, see Chapter 17, “Managing Authorization Policies and Profiles.”

This section covers the following procedures:

- Standard Authorization Policies for a Posture, page 20-163
- Creating, Duplicating, and Deleting a Standard Authorization Policy for a Posture, page 20-164

Standard Authorization Policies for a Posture

This section describes the basic operations that allow you to manage the standard authorization policies that are specific to posture service.

The Authorization Policy page displays the list of exceptions authorization policies and the standard authorization policies. The Authorization Policy page allows you to configure the standard authorization policies that can be applied to the first matching rule (authorization policy) or multiple matching rules (authorization policies) on the Authorization Policy page.

When they are created and saved, you can also prioritize the standard authorization policies by moving the standard authorization policy widgets up and down on the Authorization Policy page. If the policies are set to be enabled within the standard authorization policy widget, then the standard authorization policies enforce policies based on the compliance status of the endpoints. If they are set to be disabled, then the standard authorization policies do not enforce policies on the endpoints. You can also configure the standard authorization policies that can be set to monitor policies based on the compliance status.

To create a standard authorization policy, complete the following steps:

Step 1 Choose **Policy > Authorization**.

The Authorization Policy page appears. This page displays the list of authorization policies for standard and exceptions types.

Step 2 Click the drop-down arrow to view the matching rule option.

Step 3 Choose the **First Matched Rule Applies** option, or choose the **Multiple Matched Rule Applies** option.

The first matched rule applies option sets access privileges (standard authorization profiles) with a single authorization policy that is first matched during evaluation from the list of standard authorization policies.

The multiple matched rule applies option sets access privileges (standard authorization profiles) with multiple authorization policies that are matched during evaluation from the list of all the standard authorization policies.

Step 4 Click the **Action Icon** button to insert a new authorization policy, duplicate an existing authorization policy, or delete an existing authorization policy.

Here, you can do the following:

- Insert New Rule Above
- Insert New Rule Below
- Duplicate Above
- Duplicate Below
- Delete

Step 5 Click **Save** to create a new standard authorization policy.

The standard authorization policy appears on the Authorization Policy page.

Step 6 Click **Reset** without saving the current input data.

A confirmation dialog appears with the following message:

"Are you sure you want to reset? You will lose all the changes you have made."

Step 7 Click **Yes** to discard the current input data, or click **No** to continue.

Creating, Duplicating, and Deleting a Standard Authorization Policy for a Posture

You can create a new authorization policy, duplicate an existing authorization policy, or delete an existing authorization policy on the Authorization Policy page. Exceptions and Standard items on the Authorization Policy page display the authorization policy widgets.

To create (insert) a standard authorization policy for posture, complete the following steps:

Step 1 Choose **Policy > Authorization**.

Here, you can find the list of authorization policies displayed for standard and exceptions types on the Authorization Policy page. The Exceptions page displays the list of exceptions authorization policies, and the Standard page displays the list of standard authorization policies.

Step 2 From the Authorization Policy page, click **Standard** to display the Standard page.

The standard authorization policy widget appears on the Authorization Policy page. Click **Standard** to close the Standard page.

Step 3 From the standard authorization policy widget, click the drop-down arrow to view the predefined settings to enforce policies.

Here, you can choose one of the following options to enforce the policies based on the compliance status. The following are the options available:

- Enabled—The standard authorization policies enforce policies based on the compliance status of the endpoints
- Disabled—The standard authorization policies do not enforce policies
- Monitor—The standard authorization policies monitor enforced policies on endpoints

Step 4 Choose **Enabled**, or **Disabled**, or **Monitor**.

Step 5 Enter the rule (standard authorization policy) name.

To choose an identity group, complete the following steps:

Step 6 From the Identity Groups field, click the plus [+] sign to expand the anchored overlay.

The identity groups anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

a. From the identity groups anchored overlay, click the **Quick Picker** (down arrow) icon.

   The Identity Groups widget appears.

b. From the Identity Groups widget, choose an identity group.

c. Click the plus [+] sign to associate more than one identity group.

To choose a condition, complete the following steps:

Step 7 From the Conditions field, click the plus [+] sign to expand the anchored overlay.

The conditions anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

a. Click the Select Conditions **Quick Picker** (down arrow) icon.

The Dictionaries widget appears that lists the time and date conditions, dictionary simple conditions, and dictionary compound conditions.

b. Choose the condition.

c. Choose an AND operator or an OR operator from the drop-down list.

d. Click the **Action Icon** button to add a dictionary attribute and its value, add a condition from the library, or delete the existing conditions or dictionary attributes.

Here, you can do the following:

- Add Attribute/Value
- Add Condition from Library
- Delete

To choose an attribute, complete the following steps:

Step 8 From the Conditions field, click the plus [+] sign to expand the conditions anchored overlay.

The conditions anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

Step 9 Choose **Select Existing Condition from Library** or **Create new Condition (Advance Option)**.

For information on selecting an existing condition, see the "To select an existing condition from the library, choose Select Existing Condition from Library:" section on page 20-166.

For information on creating a new condition, see the "To create a new condition, choose Create New Condition (Advance Option)." section on page 20-166.

To choose a permission (standard authorization profile), complete the following steps:

Step 10 From the Permissions field, click the plus [+] sign to expand the authzprofile(s) anchored overlay.

The authzprofile(s) anchored overlay appears. Click the minus [-] sign, or click outside the anchored overlay to close it.

a. From the authzprofile(s) field, click the **Quick Picker** (down arrow) icon.

The Profiles widget appears. From the Profiles widget, click the navigation arrow to view the authorization profiles in each category. The Profiles widget displays the following authorization profile categories:

- Inline Posture Node
- Security Group
- Standard

b. Choose **Standard**.

c. Click the navigation arrow to view the authorization profiles in the standard authorization profile category.

d. Choose an authorization profile from the standard category.

e. Click the plus [+] sign to associate more than one authorization profile from the standard category

Step 11 Click **Save** to create a new standard authorization policy.

The standard authorization policy appears on the Authorization Policy page.

To select an existing condition from the library, choose Select Existing Condition from Library:

Here, you can choose a condition from the library that is already saved.

Step 1 From the Conditions field, click the Select Condition **Quick Picker** (down arrow) icon.

The Dictionaries widget appears that lists the available dictionaries.

Step 2 From the Dictionaries widget, click the navigation arrow to view the available dictionary conditions.

The following options appear:

- Simple Conditions
- Compound Conditions
- Time and Date Conditions

Step 3 Choose a condition.

Step 4 Choose an **AND** operator, or an **OR** operator from the drop-down list.

Step 5 Click the **Action Icon** button to add a dictionary attribute and its value, add a condition from the library, or delete existing conditions or dictionary attributes.

To create a new condition, choose Create New Condition (Advance Option).

Here, you can create new conditions. You can use the **Save** icon to add all the new conditions to the library.

Step 1 From the Attribute field, click the Select Attribute **Quick Picker** (down arrow) icon.

The Dictionaries widget appears that lists the available dictionaries.

Step 2 From the Dictionaries widget, click the navigation arrow to view the available dictionary attributes.

The dictionary attributes appear for the dictionary.

Step 3 Choose the dictionary attribute, an operator and a value for the attribute.

For the posture status, you can use the Session:PostureStatus attribute, an operator, and the values such as Unknown, Compliant, and Noncompliant.

Step 4 Choose an **AND** operator, or an **OR** operator from the drop-down list.

Step 5 Click the **Action Icon** button to add a dictionary attribute and its value, add a condition from the library, duplicate a condition, add a condition to the library, or delete existing conditions or dictionary attributes.

Here, you can do the following:

- Add Attribute/Value
- Add Condition from Library
- Duplicate
- Add Condition to Library

Here, you can save new conditions that you create. You can choose a condition that is already saved by using the Add Condition from Library option.

- Delete

You can create a copy of a standard authorization policy on the Authorization Policy page above or below the current policy selection.

To duplicate a standard authorization policy, complete the following steps:

Step 1 Click the **Action Icon** button to create a copy (duplicate) of a standard authorization policy.

Step 2 Choose **Duplicate Above** to duplicate a standard authorization policy above the current policy, or choose **Duplicate Below** to duplicate a standard authorization policy below the current policy.

Step 3 Click **Save** to create a copy of the standard authorization policy.

You can also delete a standard authorization policy on the Authorization Policy page.

To delete a standard authorization policy, complete the following steps:

Step 1 Click the **Action Icon** button to delete a standard authorization policy.

Step 2 Choose **Delete**.

Custom Permissions for Posture

A custom permission is an authorization profile (standard authorization profile) that you define in the Cisco ISE appliance. The standard authorization profiles set access privileges based on the matching compliance status of the endpoints. The posture service broadly classifies the posture into unknown, compliant, and noncompliant profiles. The posture policies and the posture requirements determine the compliance status of the endpoint.

You must create three different authorization profiles for an unknown, compliant, and noncompliant posture status of endpoints that can have different set of VLANs, DACLs and other attribute value pairs and then associate them to three different authorization policies. To differentiate these authorization policies, you can use the Session:PostureStatus attribute along with other conditions.

This section describes the standard authorization profiles that you can define in the Cisco ISE appliance.

Prerequisites:

Before you begin, you should have an understanding of the states for a posture.

Review the following states:

- Unknown Profile
- Compliant Profile
- Noncompliant Profile

Unknown Profile

If no matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint may be set to unknown. A posture compliance status of unknown can also apply to an endpoint where a matching posture policy is enabled, but posture assessment has not yet occurred for that endpoint, and therefore no compliance report has been provided to Cisco ISE by a NAC Agent. For an endpoint to have privileged network access on your network, the compliant status of the endpoint should be compliant.

Compliant Profile

If a matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint is set to compliant. When the posture assessment occurs, the endpoint meets all the mandatory requirements that are defined in the matching posture policy. For an endpoint that is postured compliant, it can be granted privileged network access on your network.

Noncompliant Profile

The posture compliance status of an endpoint is set to noncompliant when a matching posture policy is defined for that endpoint, but the endpoint fails to meet all the mandatory requirements that are defined in the matching posture policy during posture assessment. An endpoint that is postured noncompliant matches a posture requirement with a remediation action and it should be granted limited network access to remediation resources in order to remediate itself to be compliant.



CHAPTER 21

User Access Management

This chapter provides information on managing network user access, sponsor accounts, and how to create the necessary policies for these network users.

This chapter covers the following topics:

- Overview, page 21-2
- Guest Services Functionality, page 21-2
- Cisco ISE Guest Service Default Portals, page 21-11
- Guest Licensing, page 21-12
- Guest High Availability and Replication, page 21-13
- Guest Service Control, page 21-14
- Operating System and Browser Support, page 21-14
- Configuring Guest Policy Conditions, page 21-14
- Sponsor Group Policy, page 21-16
- Sponsor Groups, page 21-20
- Mapping Active Directory Groups to Sponsor Groups, page 21-23
- Creating and Testing Sponsor User to Access the Sponsor Portal, page 21-24
- Creating Guest Users, page 21-26
- SMTP Server Settings for Email Notifications, page 21-27
- General Settings, page 21-27
- Sponsor Settings, page 21-29
- Guest Settings, page 21-45
- Monitoring Sponsor and Guest Activity, page 21-74
- Audit Logging, page 21-75

Overview

Cisco Identity Services Engine (ISE) Guest service allows users, such as guests, visitors, contractors, consultants, and customers to access a network (using HTTPS), whether the network is a corporate intranet or the public Internet. The network is defined through a VLAN and downloadable access control list (DACL) configuration in the network access device (NAD).

Cisco ISE Guest service allows users with the appropriate privileges to easily create sponsor accounts and temporary guest accounts. The Cisco ISE Guest Service performs full authentication of sponsors.

Note Cisco ISE currently supports up to 37K active Guest accounts.

Sponsors and Guests

Sponsors are users who can create guest accounts. Cisco ISE allows sponsors to provide account details to the guest by printout, email, or short message service (SMS). The entire experience, from user account creation to guest network access, is stored for audit and reporting purposes.

When a guest user first attaches to the local network, either through a wireless or hard-wire connection, the user is placed in a segregated network with limited access. You can define this segregated network through the VLAN and DACL configuration on the wireless LAN controller (WLC) or NAD. In order for a guest user to function properly, the WLC or NAD must support captive HTTPS portal login scenarios where login URLs can be mapped to RADIUS servers.

Default Portals

The Cisco ISE Guest Service provides the following configurable default portals:

- Guest portal
- Sponsor portal
- Device registration web authentication portal

The Cisco ISE Guest Service supports customizable default portals to handle Guest User login, as well as the ability to create and manage Guest User accounts. Guest accounts are defined for specified time periods that are established at the time of creation.

Guest Services Functionality

To gain full access to the network, a guest opens a browser window and makes an HTTPS request by entering the URL for a web site, such as www.cisco.com or yahoo.com. The guest has not been authorized and so has limited initial access.

The Guest User Portal is configured as the captive portal for WLC Local WebAuth. In the case of wired NAD, a URL-redirect value is returned to the NAD from Cisco ISE during an initial MAB lookup failure. The guest is ultimately presented with a login page where they can enter a username and password.

Cisco ISE Guest Services support the following functions:

- NAD with Central WebAuth, page 21-3
- Wireless LAN Controller with Local WebAuth, page 21-4
- Wired NAD with Local WebAuth, page 21-5
- Device Registration WebAuth, page 21-8

NAD with Central WebAuth

This scenario applies to wireless and wired network access devices. In this scenario, the guest user's credentials are added to the Cisco ISE session cache and a Change of Authorization (CoA) is requested with the NAD. The NAD makes a new authorization request to the Cisco ISE server. The session cache attributes are used to fully authenticate and authorize the guest user.

Note WLC added support (7.2 or later) for CoA for Central WebAuth, so that a NAD can connect to the Cisco ISE network via wired or wireless means using the same configuration method.

If your client's machine is hard wired to a NAD, the guest service interaction takes the form of a failed MAB request that leads to a guest portal Central WebAuth login.

The following steps outline the process for Central WebAuth triggered by a MAB failure:

1. The client connects to the NAD through a hard-wired connection. There is no 802.1X supplicant on the client.
2. An authentication policy with a service type for MAB allows a MAB failure to continue and return a restricted network profile containing a URL-redirect for Central WebAuth user interface.
3. The NAD is configured to post MAB requests to the Cisco ISE RADIUS server.
4. The client machine connects and the NAD initiates a MAB request.
5. The Cisco ISE server processes the MAB request and does not find an end point for the client machine. This MAB failure resolves to the restricted network profile and returns the URL-redirect value in the profile to the NAD in an access-accept. To support this function, ensure that an Authorization Policy exists featuring the appropriate "NetworkAccess:UseCase=Hostlookup" and "Session:Posture Status=Unknown" conditions.

   The NAD uses this value to redirect all client HTTPS traffic on port or 8443 to the URL-redirect value. The standard URL value in this case is:

   https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&action=cwa.
6. The client initiates an HTTPS request to any URL using the client browser.
7. The NAD redirects the request to the URL-redirect value returned from the initial access-accept.
8. The gateway URL value with action CWA redirects to the guest portal login page.
9. The client enters the username and password and submits the login form.
10. The guest action server authenticates the user credentials provided.
11. If the credentials are valid, the username and password are stored in the local session cache by the guest action server.
12. For a non-posture flow (authentication without further validation), the following applies:

    If the guest portal is not configured to perform Client Provisioning, the guest action server sends a CoA to the NAD through an API call. This CoA will cause the NAD to reauthenticate the client using the RADIUS server. This reauthentication makes use of the user credentials stored in the session cache. A new access-accept is returned to the NAD with the configured network access. If Client Provisioning is not configured and the VLAN is in use, the guest portal performs VLAN IP renew.

    The user does not have to re-enter their credentials in this process. The name and password entered for the initial login are used automatically.

13. For a posture-flow, the following applies:

    The guest portal is configured to perform Client Provisioning, and the guest action redirects the client browser to the Client Provisioning URL. (You can also optionally configure the Client Provisioning Resource Policy to feature a “NetworkAccess:UseCase=GuestFlow” condition.)

    Because there is no Client Provisioning or Posture Agent for Linux, the guest portal redirects to Client Provisioning, which in turn redirects back to a guest authentication servlet to perform optional IP release/renew and then CoA.

    a. With redirection to the Client Provisioning URL, the Client Provisioning subsystem downloads a non-persistent web-agent to the client machine and performs posture check of the client machine. (You can optionally configure the Posture Policy with a “NetworkAccess:UseCase=GuestFlow” condition.)

    b. If the client machine is non-compliant, ensure that you have configured an Authorization Policy that features “NetworkAccess:UseCase=GuestFlow” and “Session:Posture Status=NonCompliant” conditions.

    c. When the client machine is compliant, ensure that you have an Authorization policy configured with the conditions “NetworkAccess:UseCase=GuestFlow” and “Session:Posture Status=Compliant.” From here, the Client Provisioning issues a CoA to the NAD. This CoA will cause the NAD to reauthenticate the client using the RADIUS server. This reauthentication makes use of the user credentials stored in the session cache. A new access-accept is returned to the NAD with the configured network access.

Note “NetworkAccess:UseCase=GuestFlow” applies for Active Directory and LDAP users logging in as guest users.

Wireless LAN Controller with Local WebAuth

This section covers the following scenario for wireless LAN controllers with Local WebAuth:

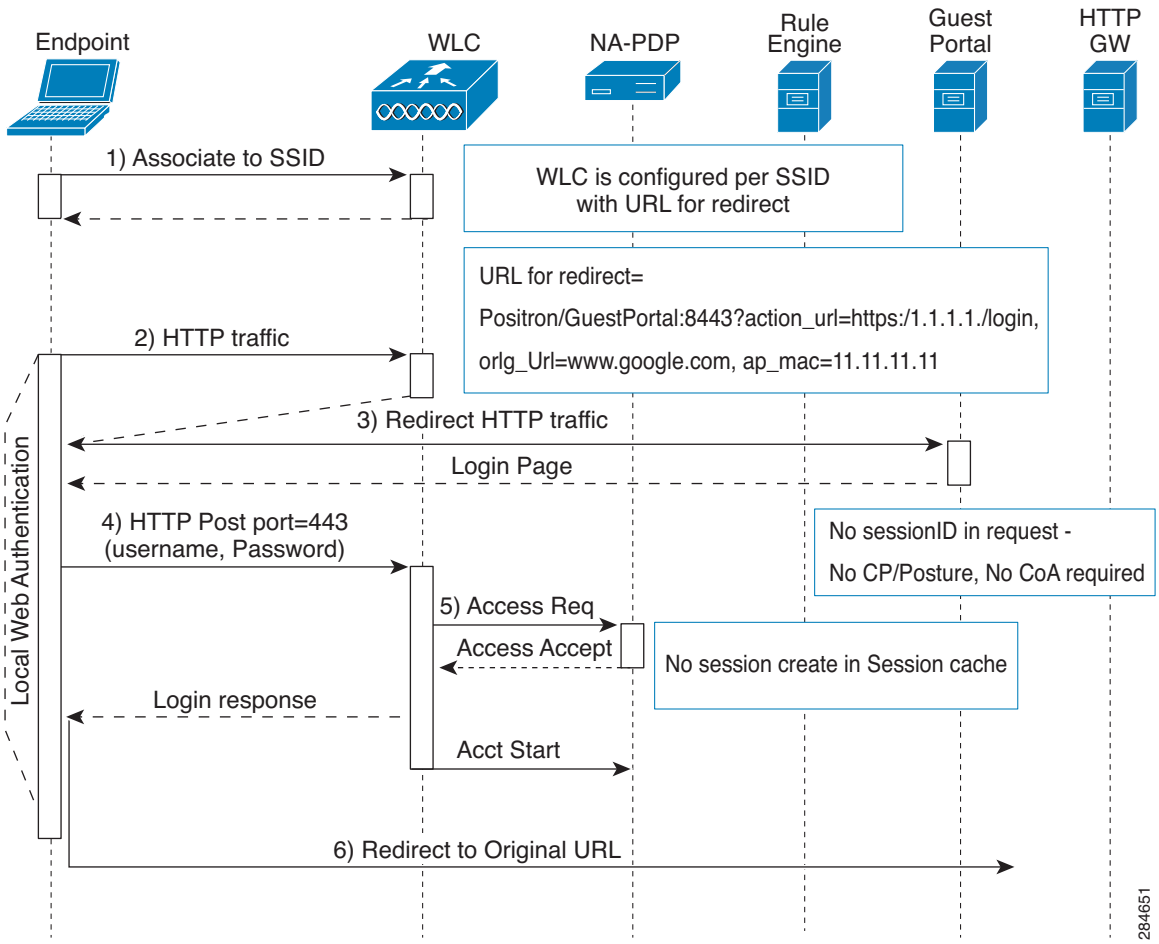
- Non-Posture Flow, page 21-4

Non-Posture Flow

A non-posture flow is a process of authentication without further validation. In this scenario, the user logs in and is directed to the wireless LAN controller (WLC). The WLC then redirects the user to this guest portal where they are prompted to enter a username and password, and perform an optional accept use policy (AUP) and password change. When this is complete, the user's browser will be redirected back to the WLC to log in again.

The WLC will now be able to log the user in via RADIUS. When this is complete, the WLC will redirect the client browser to their original destination. For an illustrated example of this process flow, see Figure 21-1.

Figure 21-1 Local WebAuth Non-Posture Flow



Wired NAD with Local WebAuth

In this scenario, the Guest User Login portal redirects the guest user's login request to the switch. The login request is in the form of an HTTPS URL posted to the switch, and contains the user credentials. The switch receives the user login request, and authenticates the user using a configured RADIUS server that points to the Cisco ISE RADIUS server implementation.

The following steps outline the process for Wired NAD with Local WebAuth:

1. Cisco ISE requires a login.html file with HTML redirect to be uploaded to the NAD. This login.html is returned to the client browser for any HTTPS request made.
2. The client browser in turn is redirected to the Cisco ISE guest portal where the user's credentials are submitted.
3. After the AUP and change password is processed (if configured in the Multi-Portal configuration), the guest portal redirects the client browser to post the user credentials on to the NAD.
4. The NAD makes a RADIUS request to the Cisco ISE to authenticate and authorize the user.

Configuring the Switch

This section describes the process of configuring the switch for Wired NAD with Local WebAuth.

To configure the switch for Wired NAD with Local WebAuth, complete the following steps:

Step 1 Configure the HTML Login Page, page 21-6.

Step 2 Enable the HTTPS Server on the Switch, page 21-6.

Step 3 Upload Success, Expiry, and Failure Pages, page 21-7.

Step 4 Configure Web Authentication, page 21-7.

Configure the HTML Login Page

The IP address and port values must be changed in the following HTML code for the login.html page to those being used by the Cisco ISE Policy Services nodes. The default port is 8443.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/guestportal/portal.jsp?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/guestportal/portal.jsp?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</HTML>
```

Because the custom login page is a public web form, consider these guidelines:

- The login form must accept user entries for the username and password and must show them as **uname** and **pwd**.
- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

Enable the HTTPS Server on the Switch

To use web-based authentication, you must enable the HTTPS server within the switch. To do so, use the following commands:

Command	Purpose
ip http secure-server	Enables HTTPS server.

Upload Success, Expiry, and Failure Pages

Additional pages for success, expiry, and failure can also be uploaded to the NAD. You can use customized HTML pages; there is no Cisco ISE specific information required.

Configure Web Authentication

To configure web authentication, complete the following steps:

Step 1 Configure web authentication to display four substitute HTML pages to the user in place of the switch default HTML pages during web-based authentication.

Step 2 To specify the use of your custom authentication proxy web pages, first store your custom HTML files on the switch flash memory. To copy your HTML files to the switch flash memory, run the following command on the switch:

```
copy tftp/ftp flash
```

Step 3 After copying your HTML files to the switch, perform the following commands in global configuration mode:

a.	**ip admission proxy http login page file** *device:login-filename*	Specifies the location in the switch memory file system of the custom HTML file to use in place of the default login page. The device: is flash memory.
b.	**ip admission proxy http success page file** *device:success-filename*	Specifies the location of the custom HTML file to use in place of the default login success page.
c.	**ip admission proxy http failure page file** *device:fail-filename*	Specifies the location of the custom HTML file to use in place of the default login failure page.
d.	**ip admission proxy http login expired page file** *device:expired-filename*	Specifies the location of the custom HTML file to use in place of the default login expired page.

Step 4 Using the following guidelines, configure your customized authentication proxy web pages:

- To enable the custom web pages feature, specify all four custom HTML files. If you specify fewer than four files, the internal default HTML pages are used.
- The four custom HTML files must be present on the flash memory of the switch. The maximum size of each HTML file is 8 KB.
- Any images on the custom pages must be on an accessible HTTPS server. Configure an intercept ACL within the admission rule.
- Any external link from a custom page requires configuration of an intercept ACL within the admission rule.
- To access a valid DNS server, any name resolution required for external links or images requires configuration of an intercept ACL within the admission rule.
- If the custom web pages feature is enabled, a configured auth-proxy-banner is not used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature is not available.
- To remove the specification of a custom file, use the **no** form of the command.

  The following example shows how to configure custom authentication proxy web pages:

```
Switch(config)# ip admission proxy http login page file flash:login.htm
Switch(config)# ip admission proxy http success page file flash:success.htm
```

```
Switch(config)# ip admission proxy http fail page file flash:fail.htm
Switch(config)# ip admission proxy http login expired page flash flash:expired.htm
```

Step 5 Verify the configuration of a custom authentication proxy web page, as shown in the following example:

```
Switch# show ip admission configuration
Authentication proxy webpage
    Login page           : flash:login.htm
    Success page         : flash:success.htm
    Fail Page            : flash:fail.htm
    Login expired Page   : flash:expired.htm

Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Device Registration WebAuth

This section outlines the authentication process a guest user goes through using device registration web authentication (DRW), as well as how to set up Device Registration WebAuth on a Cisco ISE network. This section includes the following subsections:

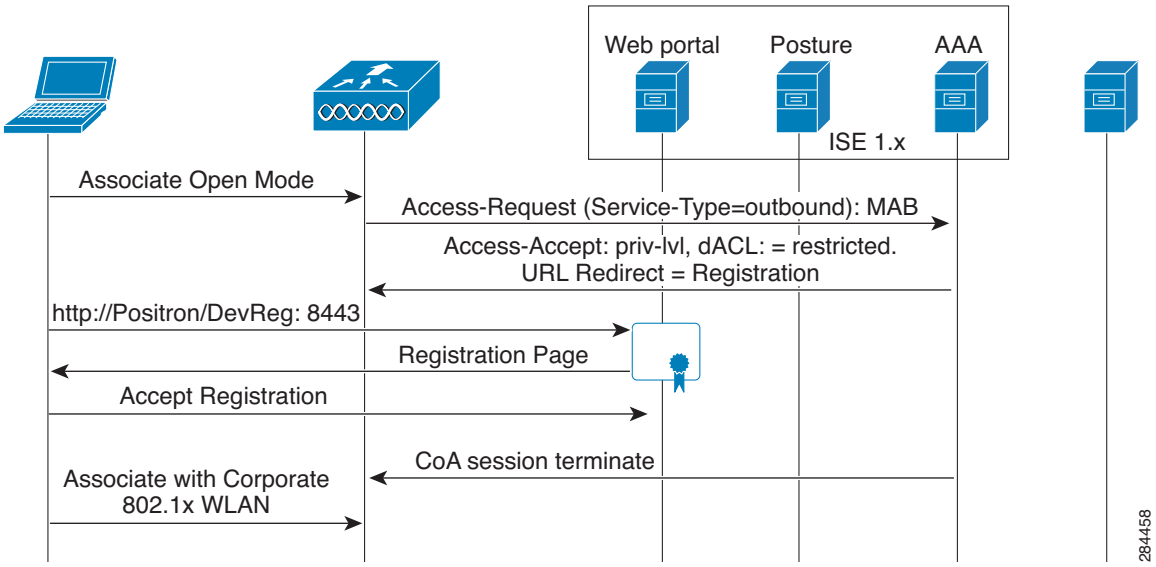
- Device Registration Web Authentication Process, page 21-8
- Configuring Device Registration WebAuth, page 21-10

Note The WLC must be configured so that it sends the client MAC address in the calling station ID value when making RADIUS access requests to ISE.

Device Registration Web Authentication Process

In this scenario, the guest user connects to the network with a wireless connection that sends an initial MAB request to the Cisco ISE node. If the user's MAC address is not in the endpoint identity store or is not marked with an AUP accepted attribute set to true, ISE responds with a URL redirection authorization profile. The URL redirection presents the user with an AUP acceptance page when the user attempts to go to any URL.

Figure 21-2 Device Registration WebAuth Flow



The following steps outline the process for Device Registration WebAuth:

1. A guest user connects to the network using a wireless connection and has a MAC address that is not in the endpoint identity store or is not marked with an AUP accepted attribute set to true, and receives a URL redirection authorization profile. The URL redirection presents the user with an AUP acceptance page when the guest user attempts to go to any URL.
2. If the guest user accepts the AUP, their MAC address is registered as a new endpoint in the endpoint identity store (assuming the endpoint does not already exist). The new endpoint is marked with an AUP accepted attribute set to true, to track the user's acceptance of the AUP. An administrator can then assign an endpoint identity group to the endpoint, making a selection from the Guest Management Multi-Portal Configurations page.
3. If the guest's endpoint already exists in the endpoint identity store, the AUP accepted attribute is set to true on the existing endpoint. The endpoint's identity group is then automatically changed to the value selected in the Guest Management Multi-Portal Configurations page.
4. If the user does not accept the AUP or an error occurs in the creation of the endpoint, an error page appears.
5. After the endpoint is created or updated, a success page appears, followed by a CoA termination being sent to the NAD/WLC.
6. After the CoA, the NAD/WLC reauthenticates the user's connection with a new MAB request. The new authentication finds the endpoint with its associated endpoint identity group, and returns the configured access to the NAD/WLC.

Note The CoA type for both wired and wireless is Termination CoA. You can configure device registration authentication (DWR) to perform VLAN IP Release and Renew, thereby changing the CoA type for both wired and wireless to Change of Auth.

Configuring Device Registration WebAuth

This section explains the process for configuring Device Registration WebAuth, and the following general steps:

1. Configure the Device Registration WebAuth, page 21-10.
2. Create a DRW Authorization Profile, page 21-10.
3. Create a DRW Authorization Policy Rule, page 21-10.

Note You must have Cisco ISE administrator privileges, to configure Device Registration WebAuth (DRW).

Configure the Device Registration WebAuth

You can configure Device Registration WebAuth (DRW) using the process outlined in the following steps:

1. Go to **Administration > Guest Management > Settings > Multi-Portal Configurations** in the Cisco ISE Admin user interface.
2. Choose to set the Device Registration WebAuth portal as the default Guest Portal, then choose the standard HTML pages provided in Cisco ISE, or you can upload customized HTML pages and images.
3. You can create multiple versions of each portal type, assigning each version a unique name. The portal name must be used in the URL-redirect value that is returned in the authorization profile, to specify the portal as the one that is used to handle requests.
4. Select an endpoint identity group to which newly created endpoints are then assigned. The identity group is then used in the authorization policies to control endpoint access.
5. Next, Create a DRW Authorization Profile, page 21-10.

Create a DRW Authorization Profile

Device Registration WebAuth requires that you set up a special authorization profile. To create an authorization profile for DRW, use the steps outlined in the following process:

1. Go to the **Policy > Policy Elements > Results > Authorization > Authorization Profiles** page in the Cisco ISE Admin user interface.
2. Create an authorization profile using the name of the Device Registration WebAuth portal that you specified in Configure the Device Registration WebAuth, page 21-10.
3. Next, Create a DRW Authorization Policy Rule, page 21-10.

For more information, see Cisco ISE Authorization Policies and Profiles, page 17-5.

Create a DRW Authorization Policy Rule

After the guest user verifies the Accept User Policy, an endpoint is created and appears in the internal endpoint identity store. The endpoint is created using the MAC address and has the AUP Accepted attribute set to true.

To create a DRW authorization policy rule, use the steps outlined in the following process:

1. Create a new authorization policy or modify an existing policy, as described in Creating a New Authorization Policy, page 17-14 or Duplicating and Modifying an Existing Authorization Policy, page 17-16.
2. Add the DRW authorization profile as the permissions in an authorization policy rule.

   This setting causes a URL-redirect cisco av pair to be returned to the WLC for the initial MAB request, when the request matches the authorization policy rule. The URL-redirect takes the following form, where:

   ip:port = the IP address and port number respectively

   DRWPortal = the unique portal name

https://ip:port/guestportal/gateway?sessionID=SessionIdValue&portal=DRWPortal&action=cwa

3. You can also use the endpoint identify group to affect the rule evaluation and final client access.

   The endpoint identity group is set to the selection that you make on the Multi-Portal Configurations page (Administration > Guest Management > Settings > Multi-Portal Configurations) in the Cisco ISE Admin user interface.

For more information on authorization policies and policy rules, see Chapter 17, "Managing Authorization Policies and Profiles."

Cisco ISE Guest Service Components

The Cisco ISE Guest service is composed of three main components:

- Guest—The guest user is the person who needs a guest user account to access the network.
- Sponsor—The sponsor user is the person who creates the guest user account. This person is often an employee of the organization. For example, a lobby ambassador who creates and manages guest user accounts through a sponsor-oriented web portal. Cisco ISE authenticates sponsors through a local database, or through external Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory identity stores.
- Admin—The admin user is the administrator who configures and maintains the Cisco ISE appliance.

Cisco ISE Guest Service Default Portals

The Cisco ISE Guest Services consists of the following portals:

- Cisco ISE Admin Portal, page 21-12
- Sponsor Portal, page 21-12
- Guest User Portal, page 21-12
- Device Registration WebAuth Portal, page 21-12

Cisco ISE Admin Portal

The admin portal facilitates in configuring global policies for the sponsor and guest users. You can configure user groups and policies from the admin portal. From the Cisco ISE Admin portal you can configure the following:

- Sponsor Groups.
- Sponsor group policies.
- General settings like purge and port.
- Sponsor portal settings like the language templates, sponsor portal customization, sponsor authentication source.
- Guest settings like username policy, password policy, guest portal policy, guest details policy, multi-portal settings, time profiles.
- Client uploadable multi portals.

Sponsor Portal

The sponsor portal facilitates the creation and management of guest user accounts. The sponsor portal allows you to perform the following functions:

- Creating, editing, deleting, suspending, reinstating guest user accounts.
- Viewing guest details.

Guest User Portal

The Guest User Portal facilitates the guest user login and consists of the following elements:

- Guest User Login screen with username and password fields.
- Accept Use Policy screen. This is an optional Terms of Use agreement.
- Required Password Change screen, which is optional at first login and later with configurable password expiration.
- Allow Password Change screen where the user can optionally change their password.
- Self Registration screen, which is an optional screen allows guests to set up their own user account.
- Device Registration.

Device Registration WebAuth Portal

The Device Registration WebAuth (DRW) portal facilitates guest user login through a wireless connection, providing the same elements as the Guest User Portal.



Note The wireless LAN controller (WLC) must be configured to send the client MAC address in the calling station ID value when making RADIUS access requests to the Cisco ISE server.

Guest Licensing

Guest services are available in Cisco ISE with both base and advanced licensing. When you first install Cisco ISE, Guest services are available with the 90-day evaluation license that comes as part of Cisco ISE. After that, you must enter a base or advanced license through the Administrator user interface to keep both the Guest and Sponsor portals from returning an HTTP 503 error response, reporting to users that the service is not available.

For more information on Cisco ISE licensing, see Chapter 12, "Managing Licenses."

Guest High Availability and Replication

Cisco ISE guest services make use of the Distributed Management System of the Cisco ISE to allow for multiple Cisco ISE nodes to communicate with one another in a deployment. In a multi-node distributed deployment, you specify a single node to be the master or the designated primary node. You make configurations for all the nodes in the deployment on the primary node, and then the configurations are replicated to the secondary nodes.

You must register a secondary node with the designated primary node in the deployment. Once a node is registered, the primary database is replicated to the secondary node it restarts as a node in the deployment.

Cisco ISE guest services function on either a primary or secondary. When running on a secondary, changes to the guest user accounts made through the Guest or Sponsor portals are propagated to the primary, and then replicated throughout the deployment.

Guest portals must be located on the same secondary nodes where the Cisco ISE Network Access is configured to handle RADIUS requests in the NAD.

For example, if node A is used to handle RADIUS requests for a NAD, the Guest portal must also be enabled on the same node A for the guest services to work correctly.

See "Guest Service Control" section on page 21-14 for details on enabling guest services on a node.

The Sponsor portal should be allowed to work on any node in a deployment, as long as that node also has Policy Services functionality enabled. For Sponsor portal updates to occur, the primary node with Administration persona must be online. If the node with Administration persona is offline, you can only view the account details. You cannot make any changes to the account.

The Guest portal can run on a node that assumes the Policy Services persona when the primary node with Administration persona is offline. However, it has the following restrictions:

- Self registration is not allowed
- Device Registration is not allowed
- The AUP is shown at every login even if first login is selected
- Change Password is not allowed and accounts are given access with the old password.
- Maximum Failed Login is not be enforced

You can make Guest administration user interface action only from the primary Admin user interface. All configuration made for guest service is the same for all nodes in the deployment.

Multiportal uploads to the primary is replicated to the secondary nodes and installed as part of the standard data replication system.

Guest and Sponsor portal port number configuration is replicated to secondary nodes and the secondary node is restarted once the replication is complete.

Note The whole deployment uses the same configuration for the portal ports.

Guest Service Control

The Guest and Sponsor portal can be disabled on a Cisco ISE node through the Cisco ISE Admin user interface.

To enable or disable Guest and Sponsor portals on any node, complete the following steps:

Step 1 From the Cisco ISE Administration interface, choose **Administration > System > Deployment**

Deployment Nodes page appears, displaying all the Cisco ISE nodes in the deployment.

Step 2 Select the node you wish to modify and choose **Edit**.

Step 3 Under the Policy Services section, check or uncheck **Enable Session Service** check box. This will enable or disable the Guest and Sponsor services portal.

Operating System and Browser Support

Refer to the *Cisco Identity Services Engine Network Component Compatibility, Release 1.1* document for information on operating systems and browsers supported by the Cisco ISE Guest services.

Configuring Guest Policy Conditions

Cisco ISE provides a way to create conditions that are individual, reusable policy elements that can be referred from other rule-based policies. You can create conditions from within the policy pages and as separate policy elements to be reused by other types of Cisco ISE policies such as Sponsor group or Client Provisioning policies. Whenever a policy is being evaluated, the conditions that comprise it are evaluated first.

The guest simple and compound conditions are used while you create sponsor group policies.

Simple Conditions

Simple conditions consist of an attribute, an operator, and a value. You can create simple conditions from within the policy pages and also as separate policy elements that can be reused in policies. Cisco ISE allows you to create, edit, and delete simple authentication conditions. This page lists all the simple authentication policy conditions that you have defined in Cisco ISE.

See "Configuring Policy Elements Conditions" section on page 17-17, for more detailed information.

See "Creating Simple Conditions" section on page 21-15, for information on how to define simple conditions.

Related Topics

- Creating Simple Conditions, page 21-15
- Creating a New Sponsor Group Policy, page 21-17

Creating Simple Conditions

To create simple conditions as separate policy elements, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 From the left navigation pane, click the greater-than sign ">" next to Guest.

Step 3 From the left navigation pane, click **Simple Conditions.**

The Guest Simple Conditions page appears.

Step 4 Click **Add** to add a new condition.

Step 5 Enter the following information:

- Name—Name of the reusable condition.
- Description—An optional description for the condition.
- Attribute—Choose the attribute on which you want to build the condition. Click the drop-down arrow to select the attribute from the dictionary.
- Operator—Choose the operator from the drop-down list box. This list box is populated only after you select the attribute.
- Value—Select a value from the drop-down list box. This list box is populated only after you select the attribute.

Note For some attributes, you can enter the value.

Step 6 Click **Submit**.

You can now use this condition in creating Sponsor Group Policies.

Next Step

See the "Creating a New Sponsor Group Policy" section on page 21-17 for information on how to define a sponsor group policy using the simple conditions that you have created.

Compound Conditions

Compound conditions are made up of two or more simple conditions. You can create compound conditions as reusable objects from within the policy creation page or from the Conditions page. This page lists all the compound conditions that you have defined in Cisco ISE.

See "Configuring Policy Elements Conditions" section on page 17-17, for more detailed information.

See "Creating Compound Conditions" section on page 21-16 for information on how to create compound conditions.

Related Topics

- Creating Compound Conditions, page 21-16
- Creating a New Sponsor Group Policy, page 21-17

Creating Compound Conditions

To create a compound condition from the Conditions page, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions**.

Step 2 From the left navigation pane, click the greater-than sign ">" next to Guest.

Step 3 From the left navigation pane, click **Compound Conditions.**

The Guest Compound Conditions page appears. This page lists any compound conditions that have been defined.

Step 4 Click **Add** to add a new compound condition.

Step 5 Enter a name for the compound condition. You can enter an optional description.

Step 6 Click **Select Existing Condition from Library** to select an existing simple condition or click **Create New Condition** to select an attribute, operator, and value from the expression builder.

a. If you have chosen to create a new condition, from the Select Attribute drop-down list box, choose an attribute from the dictionary based on which you want to create a condition.

b. After you have selected an attribute:

- Choose an operator (Equals, Not Equals, Matches, and so on) from the drop-down box.
- Choose the value from the drop-down list box, if available or enter a value in the text box.
- To save this condition to be reused in other policies, click **Add Condition to Library** from the **Actions** button that appears in the same row.
- Enter a name for this condition in the Condition Name text box and click the () icon.

  The condition is saved as a simple condition and will be available for use in other policies.

Step 7 To add more conditions, click **Actions** at the end of this row.

Step 8 Click **Add Attribute/Value** to create a new condition or click **Add Condition from Librar**y to add an existing simple condition.

Step 9 Select the operand from the drop-down list box. You can select either AND or OR and the same operand will be used between all the conditions in this compound condition.

Step 10 Repeat the process from Step 5 to add more conditions.

Step 11 After you have added all the conditions, click **Submit** to create this compound condition.

Next Step

See the "Creating a New Sponsor Group Policy" section on page 21-17 for information on how to define a sponsor group policy using the compound conditions that you have created.

Sponsor Group Policy

The sponsor portal processes the sponsor group policy that allows you to log into the sponsor portal. The sponsor portal obtains the guest sponsor group from the matching sponsor group policy that allows you to access the sponsor portal. The guest sponsor groups contain a set of permissions and user settings that enable you to access the sponsor portal when you log into the sponsor portal. The sponsor portal uses

the access permissions in the selected guest sponsor group to limit access within the portal. If your credentials fail, or if the sponsor group policy does not match the user settings that are defined for you when you log into the sponsor portal, then the portal returns you to the Sponsor Portal Login page.

A sponsor group policy contains one or more user roles and identity groups. It also contains one or more attribute conditions that allow you to assign the guest sponsor group. The conditions that are used in the sponsor group policy are the attributes that are selected from the dictionary attribute. One or more sponsor group policies assign you to the guest sponsor group.

A internal user that you create and store in the Cisco ISE database, and that is locally assigned to a user role or an identity group, can be a sponsor user. For the internal user to be identified as a sponsor user, the user needs to be assigned to a guest sponsor group. If you assign the internal user to a user role or identity group, and the internal user possesses the attribute conditions that are defined in the sponsor group policy, then the internal user is assigned to the guest sponsor group that is selected in the sponsor group policy.

Internal users are mapped to sponsor groups by assigning an identity group role that is used in a sponsor group policy. If both the identity group role and the conditions of the sponsor group policy match the internal user, that user will be mapped to the sponsor group associated with that sponsor group policy. For more information on how to map identity groups to sponsor groups, see "Mapping Active Directory Groups to Sponsor Groups" section on page 21-23.

The sponsor user can also originate from an external identity store like LDAP or Active Directory. For the external user to be identified as a sponsor user, the attributes from the external identity store need to match the conditions in the sponsor group policy that map the external user to a local guest sponsor group. If the external user possesses the attribute conditions that are defined in a sponsor group policy, then the user is assigned to the guest sponsor group that is selected in the sponsor group policy.

The Cisco ISE deployment contains the following guest sponsor groups by default:

- SponsorAllAccount—contains a set of permissions by default that allow you to perform the tasks on all the guest accounts.
- SponsorGroupOwnAccounts—contain a set of permissions that allow you to perform the tasks on the guest accounts that you own.
- SponsorGroupGrpAccounts—contains a set of permissions that allow you to perform the tasks on the guest accounts that you own, as well as all guest accounts that belong to the sponsors associated to the same sponsor group.

You can also create your own sponsor group and associate it to any identity group in the sponsor group policy.

Related Topics

Creating a New Sponsor Group Policy, page 21-17

Creating a New Sponsor Group Policy

Prerequisites:

Before you begin this procedure you should have created the following condition types:

- Simple Conditions, page 21-14
- Compound Conditions, page 21-15

To create a new sponsor group policy, complete the following steps:

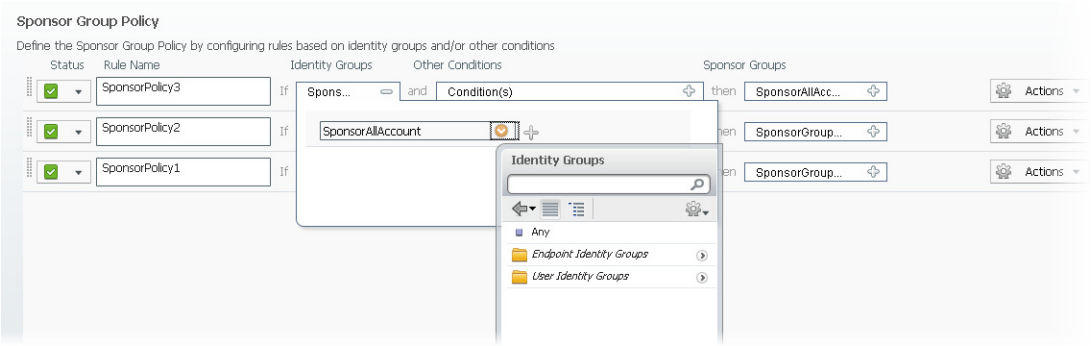
Step 1 Choose **Administration > Guest Management > Sponsor Group Policy**.

Step 2 Click **Actions** to select either **Insert New Rule Above** or **Insert New Rule Below**.

A new policy entry appears in the position you designated in the Sponsor Group Policy window.

Step 3 Enter values for the following sponsor policy fields:

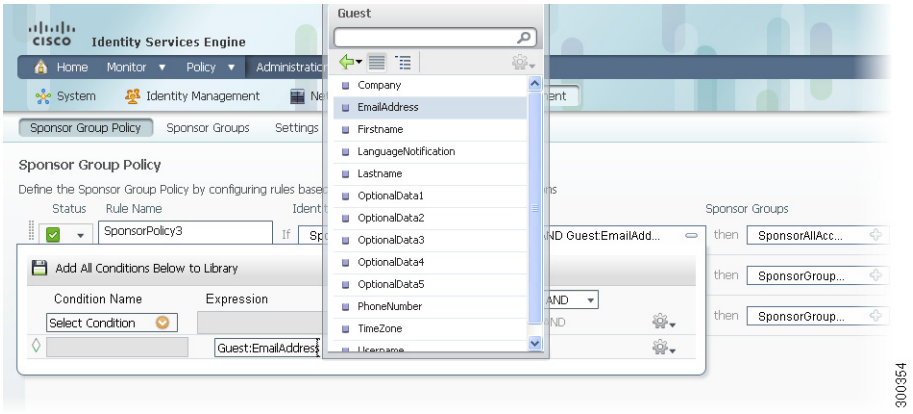
- Rule Name—Enter a name for the new policy.
- Identity Groups—Choose a name for the identity group associated with the policy.
  - Click **+** (“plus” sign) to display a drop-down list of group choices, or choose **Any** for the policy for this identity group to include all users.



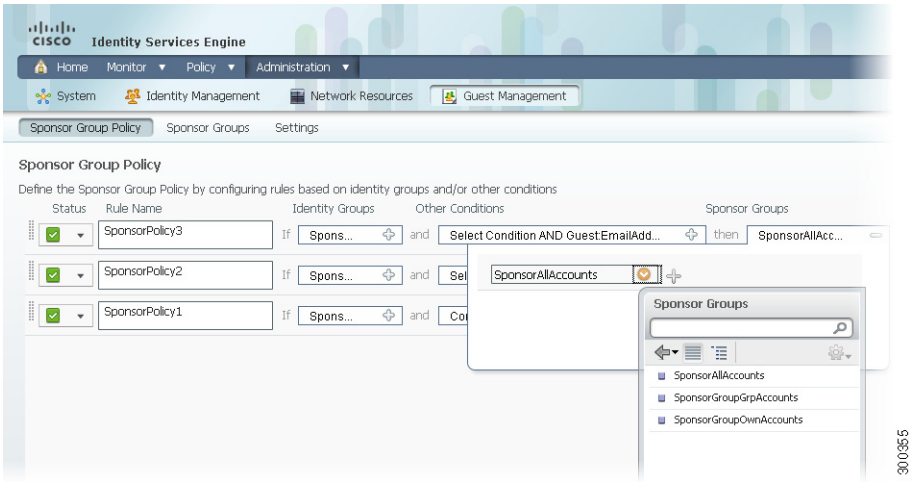
- Other Conditions—Choose the types of conditions or attributes for the identity group associated with the policy. Click **+** next to Condition(s) to display the following list of condition and attribute choices to configure:
  - Select Existing Condition from the Library—This lets you select a Condition Name option from the pull-down list (Simple Conditions, Compound Conditions, or Time and Date Conditions) as needed.



  - Create new condition (Advanced option)—This displays a list of dictionaries that contain specific attributes related to the dictionary type.



- Sponsor Group—Choose the sponsor group to associate with this sponsor group policy. Click **+** next to Sponsor Group to select a group option from the drop-down list.



Step 4 Click **Save** to save your changes to the Cisco ISE system database and create this new sponsor group policy.

Modifying an Existing Sponsor Group Policy

To modify an existing sponsor group policy, complete the following steps:

Step 1 Choose **Administration > Guest Management > Sponsor Group Policy**.

Step 2 To choose the sponsor group policy you want to modify, click **Actions** for that policy row and select **Duplicate above** or **Duplicate below**.

A duplicate policy entry appears in the Standard panel of the Sponsor Group Policy window (either above or below the existing policy that you selected).

Step 3 Enter a new name for this policy in the **Rule Name** field.

Step 4 Modify the desired values to create the new sponsor group policy in the corresponding fields by selecting different option choices.

Step 5 Click **Save** to save your changes to the Cisco ISE database, which creates this new sponsor group policy.

Deleting an Existing Sponsor Group Policy

To delete an existing authorization policy, complete the following steps:

Step 1 Choose **Administration > Guest Management > Sponsor Group Policy**.

Step 2 To select the sponsor group policy you want to delete, click **Actions** for that policy row and choose **Delete**.

A confirmation dialog appears in the Standard panel of the Sponsor Group Policy window.

Step 3 Click **OK** to confirm that you want to delete the sponsor group policy.

Step 4 Click **Save** to save your changes to the Cisco ISE system database and delete this sponsor group policy.

Note If you do not click **Save**, you will only delete the sponsor group policy locally.

Related Topics

Sponsor Group Policy, page 21-16

Sponsor Groups

Guest sponsor groups contain the permissions and settings for the sponsor user. Sponsor users belonging to a particular sponsor group have a certain set of permissions and settings when logged into the sponsor portal. You can set role-based permissions for sponsors to allow or restrict access to different functions, such as creating accounts, modifying accounts, and sending account details to guests by email or short message service (SMS).

For example, if you want a set of sponsors to be unable to log in for a short period of time while some configuration is being changed, you can set the sponsor group permission to prevent login. This way you can restrict a set of sponsor users from logging in without having to remove the sponsor group.

This section covers the following procedures:

- Creating and Editing Sponsor Groups, page 21-21
- Deleting the Sponsor Group, page 21-22

Creating and Editing Sponsor Groups

To create a sponsor group, complete the following steps:

Step 1 From the Cisco ISE Administration interface, choose **Administration > Guest Management > Sponsor Groups**, which displays the Guest Sponsor Groups page.

Step 2 Click one of the following:

- **Add**—To create a new sponsor group
- **Edit**—To edit an existing sponsor group

Step 3 Give the name and description for the new sponsor group under the General tab.

Step 4 Complete the following settings under the Authorization Levels tab:

a. Set **Yes** or **No** permission for the following:

- Allow Login
- Create Accounts
- Create Random Accounts
- Import CSV
- Send Email
- Send SMS
- View Guest Password
- Allow Printing Guest Details

b. Choose one of the following options for View/Edit Accounts:

- No—Sponsors are not allowed to edit any guest accounts.
- All Accounts—Sponsors are allowed to edit/view all guest accounts.
- Group Accounts—Sponsors are allowed to edit guest accounts created by anyone in the same sponsor user group.
- Own Account—Sponsors are allowed to edit only the guest accounts they created.

c. Choose one of the following options for Suspend/Reinstate Accounts:

- No—Sponsors are not allowed to suspend any guest accounts.
- All Accounts—Sponsors are allowed to suspend or reinstate all guest accounts.
- Group Accounts—Sponsors are allowed to suspend guest accounts created by anyone in the same sponsor user group.
- Own Account—Sponsors are allowed to suspend only the guest accounts they created.

d. Account Start Time—This setting restricts the number of days the sponsor can specify for starting the guest account. This is applicable only for the Start End type of time profile.

e. Maximum Duration of Account—This setting specifies the maximum duration for which a guest account can be active. The expiration date is based on the maximum duration of the account or the time profile duration, whichever is minimum. This value overrides the maximum duration value set by the sponsor during the creation of the guest account when this value is less than the one specified in the time profile.

Step 5 Choose the guest roles that the sponsor group user would be allowed to assign to the guest user, under the Guest Roles tab.

Guest roles allow a sponsor to assign different levels of access to a guest account. These roles are used in the authorization policies to relate guest user accounts to identity groups.

Step 6 Choose the following time profiles that the sponsor group user would be allowed to assign to the guest accounts, under the Time Profiles tab:

- DefaultOneHour—The guest user can login within one hour of the account creation, after which the account expires. This means that the account start time is equal to the user creation time and end time is one hour from the start time.
- DefaultFirstLogin—The account start time starts when the guest user first logs in to the guest portal. The end time depends on the configuration which is set in that time profile.
- DefaultStartEnd—The sponsor can select both the account start and end time.

Time profiles provide a way to give different levels of time access to different guest accounts. Sponsors under any sponsor group do not have permission to make any changes to the time profiles.

Step 7 Click **Submit**.

For More Information

See "Configuring Network Access and Sponsor Users" section on page 4-9 for more information on guest roles.

See "Time Profiles" section on page 21-70 for more information on time profiles.

Related Topics

- Sponsor Groups, page 21-20
- Deleting the Sponsor Group, page 21-22

Deleting the Sponsor Group

This section shows you how to delete an existing sponsor group.

Note You are not allowed to delete sponsor groups that are in use in a sponsor group policy.

To delete sponsor groups, complete the following steps

Step 1 From the Cisco ISE Administration interface, select **Administration > Guest Management > Sponsor Groups.**

Step 2 Check the check box to select the sponsor group(s) to be deleted.

Step 3 Click **Delete**.

For More Information

See "Sponsor Group Policy" section on page 21-16 for more information on sponsor group policy.

Related Topics

- Sponsor Groups, page 21-20
- Creating and Editing Sponsor Groups, page 21-21

Mapping Active Directory Groups to Sponsor Groups

Prerequisite

Before beginning this task, you should have understood and successfully performed Configuring Active Directory Groups, page 5-11.

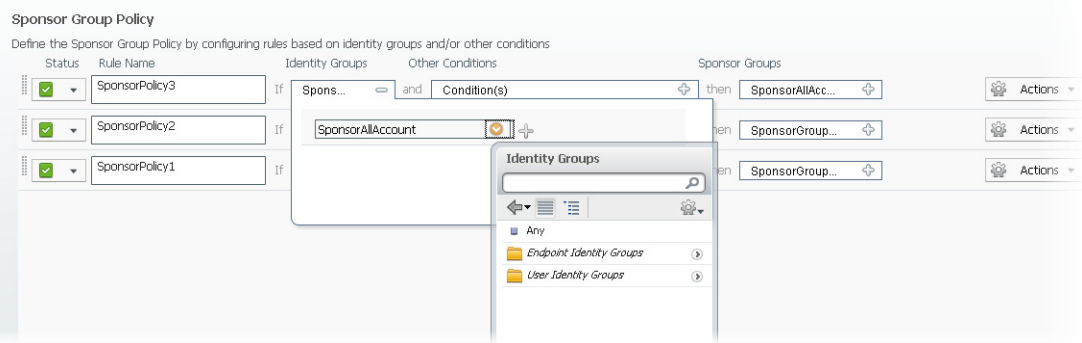
To map the Active Directory (AD) groups to the sponsor groups:

Step 1 Choose **Administration > Guest Management > Sponsor Group Policy**.

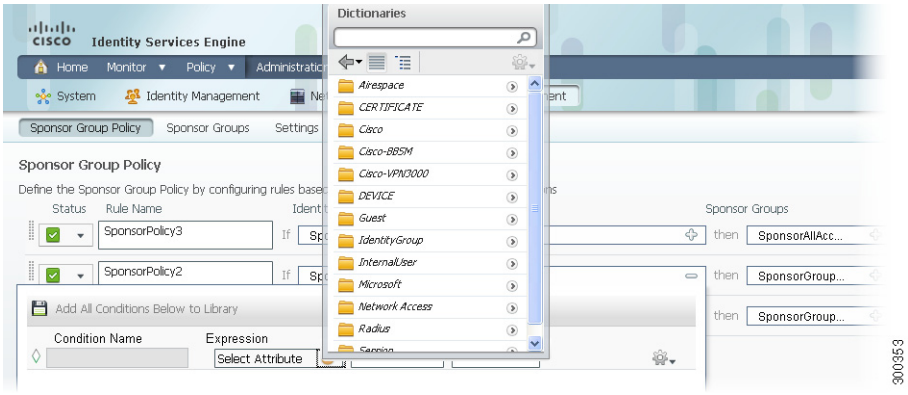
The Sponsor Group Policies page appears.

Step 2 Enter values for the following sponsor policy fields:

- Rule Name—Enter a name for the new policy.
- Identity Groups—Choose **Any** as the Identity Group since there is no group mapping with the internal groups.



- Other Conditions—Create a condition that maps the external groups to one of the populated groups. When you create the condition you will find a dictionary entry for the AD identity store that you would have created while configuring AD.
- Sponsor Group—Select the Sponsor Group to which you want this AD condition to map.



Step 3 Click **Save.**

Related Topics

- Sponsor Group Policy, page 21-16
- Creating a New Sponsor Group Policy, page 21-17
- Sponsor Groups, page 21-20

Creating and Testing Sponsor User to Access the Sponsor Portal

Before you can log into the Sponsor portal, you must first create a sponsor user. There are no predefined sponsor users in Cisco ISE. This section shows you how to create a sponsor user, and then test the sponsor user by logging into the sponsor portal.

Creating a Sponsor User

Prerequisite

You should have created a sponsor group, as described in Creating and Editing Sponsor Groups, page 21-21.

To create a sponsor user and assign the user to a sponsor group, complete the following steps:

Step 1 Go to **Administration > Identity Management > Identities > Users**.

Step 2 Click the plus sign (**+**) to create a new network access user.

Step 3 Enter values for the Network Access User fields.

For more information, see Configuring Network Access and Sponsor Users, page 4-9.

Step 4 Choose one of the following sponsor user groups from the drop-down list:

- SponsorAllAccounts
- SponsorGroupAccounts
- SponsorOwnAccounts

Note These selections are identity groups and not sponsor groups. Sponsor groups are determined from the identity group based on the sponsor policies.

Step 5 Click **Submit**. The sponsor user is created.

Step 6 To test the sponsor user, proceed with Logging into the Sponsor Portal to Test a Sponsor User, page 21-25.

Logging into the Sponsor Portal to Test a Sponsor User

This task shows you how to log into the Sponsor portal and test the sponsor user account you created in the previous section.

Prerequisite

You must have successfully completed the task of Creating a Sponsor User, page 21-24.

To log into the Sponsor portal and test a user account, complete the following steps:

Step 1 To log into the sponsor portal, open a browser window and enter the following URL in the address field, substituting the *ipaddress* variable for the IP address of the Cisco ISE server:
https://*ipaddress*:8443/sponsorportal

The sponsor portal login screen appears.

Step 2 Log in using the credentials you specified when you created the sponsor user.

Next Step

See the "Setting Ports for the Sponsor and Guest Portals" section on page 21-28 for information on how to assign ports for the Sponsor and Guest portals.

Creating Guest Users

This section shows you how to create guest user accounts through the Cisco ISE Admin portal. You can also create guest user accounts through the Sponsor portal, as a sponsor. For instructions on how to create guest users through the Sponsor portal, see the *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1.*

Note When you create guest user accounts through the Admin portal (rather than the Sponsor portal) the users are not automatically required to change their passwords after they first log in. Guests accounts created through the Sponsor portal automatically redirect the users to the Change Password page after they log in for the first time.

To create a guest account through the Admin portal, complete the following steps:

Step 1 In the Cisco ISE Admin user interface, choose **Administration > Identity Management > Identities**.

Step 2 In the Identities panel on the left, expand **Users**. Then in the right panel, click **Add**.

Step 3 In the Network Access User panel, do the following:

a. Enter a name for the account in the **Name** field.

b. Choose **Enabled** or **Disabled,** as desired. Enabled is selected by default.

c. Enter an **Email** address.

Step 4 In the Password panel, enter a **Password** for the account, and then **Re-Enter Password**.

Step 5 In the User Information panel, enter the **First Name** and **Last Name** of the user.

Step 6 In the Account Options panel, enter a **Description** for the account and check the **Password Change** check box if you want the user to change their password on the next login.

Note If you do not check the Password Change check box, the user is not automatically redirected to the Change Password page on their next login.

Step 7 In the User Groups panel, choose **Guest** from the pop-up dialog, and then click **Submit**.

SMTP Server Settings for Email Notifications

You must set up a Simple Mail Transfer Protocol (SMTP) server to send email notification to the guest user. This server is also used to send email to the short message service (SMS) gateway to deliver the SMS text message.

To set the SMTP server, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > System > Settings > SMTP Server.** The SMTP Server Settings page appears.

Step 2 In the SMTP Server field, type the host name of the outbound SMTP server to which you need to deliver email. For the email notification to function appropriately, the SMTP host server must be accessible from the Cisco ISE server. The maximum length for this field is 60 characters.

Step 3 Choose the **Enable Notifications** option to enable mail functionality globally.

Step 4 Choose **Use email address from Sponsor**, to send guest notification email from the email address of the sponsor.

Step 5 If you want to specify a different email address, choose **Use Default email address** and type the email address from which you want guest notification emails to be sent (for example, username@domain.com).

Step 6 Click **Save**.

For More Information

See *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1* for more information on the sponsor portal and how to create guest users.

Related Topic

- Setting Ports for the Sponsor and Guest Portals, page 21-28
- Purging Guest User Records, page 21-28

General Settings

You can configure general settings like the port and SMTP server settings.

- Setting Ports for the Sponsor and Guest Portals, page 21-28
- Purging Guest User Records, page 21-28

Setting Ports for the Sponsor and Guest Portals

The sponsors and guests access the portal using HTTPS. The default settings for the sponsor and guest portals is HTTPS on port 8443.

To configure the protocols and port numbers for the sponsor and guest portals, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings.**

Step 2 In the Settings panel, expand **General** and choose **Ports.**

Step 3 Assign a port number for Guest Portal Settings. Port 8443 is the default.

Step 4 Assign a port number for Sponsor Portal Settings. Port 8443 is the default.

Step 5 To specify a Default Sponsor URL, check the check box and enter a fully qualified domain name (FQDN) in the text field, such as: guest.yourcompany.com

Step 6 Click **Save**.

Accessing the Sponsor Portal

To access the sponsor portal enter the following URL, substituting the ip_address variable with the IP address of the Cisco ISE server:

`https://ip_address:8443/sponsorportal`

Accessing the Guest Portal

To access the guest portal enter the following URL, substituting the ip_address variable with the IP address of the Cisco ISE server:

`https://ip_address:8443/guestportal/Login.action`

For More Information

See *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1* for more information on the sponsor portal.

Related Topics

Purging Guest User Records, page 21-28

Purging Guest User Records

You can purge the expired guest user records from the system. You can configure the purge settings for an automatic purge at a regular interval of time or you can do a manual purge by clicking the Purge Now button.

To schedule the purge of expired guest user records, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings.**

Step 2 In the Settings panel, select **General > Purge**.

Step 3 To schedule a purge operation, check the **Enable purge settings for expired guest accounts** check box.

Step 4 Configure the following available options:

a. Enter the purge interval, in number of days. Valid range is 1-365.

b. Specify the hour of the day when the purge should occur.

Date of last purge displays the date and time when the last purge operation occurred.

Date of next purge displays the date and time when the next purge operation is scheduled to occur.

Step 5 To immediately execute a purge of expired guest user records, click **Purge Now**.

This executes a purge manually even if Enable purge check box is not checked. This option provides you the freedom to purge records whenever you seem fit.

Step 6 Click **Save**.

There might be a 15 minute sleep cycle after the scheduled purge time. After this the system checks whether it is the correct hour and date to start the purge. Due to this sleep cycle, it takes up to 15 minutes for the purge to start after configured hour.

If the Cisco ISE server is down and the purge operation did not execute, it will not run again until the next time the server is running at the correct hour.

By default, the purge operation is enabled and executes every 15 days, at 23:00 hrs.

Note Purge only runs on primary or standalone nodes.

Related Topics

Setting Ports for the Sponsor and Guest Portals, page 21-28

Sponsor Settings

You can configure sponsor settings under this sub menu. The following configuration options are available here:

- Specifying an Authentication Source, page 21-29
- Specifying a Simple URL for Sponsor Portal Access, page 21-30
- Creating a Custom Portal Theme, page 21-31
- Applying Language Templates, page 21-34

Specifying an Authentication Source

To allow a sponsor user to log into the sponsor portal, you have to choose an identity store sequence. This sequence is used with the login credentials of the sponsor to authenticate and authorize the sponsor for access to the sponsor portal. The sequence can include external stores as well as the local Cisco ISE identity store. The identity store sequence defines which stores should be accessed and in what order they should be accessed to resolve the authentication of a sponsor user.

There is one sequence value used for all the sponsor logins. It is up to the administrator to set up one of these sequences at install time.

By default, internal users are allowed to access the sponsor portal. You can set an identity store sequence to over ride this default setting. Also, internal NSF users must be assigned to an identity group that is related to a sponsor group through a sponsor group policy, to gain access to the sponsor portal.

Note External sponsors will not have access to the sponsor portal until the identity store sequence value is selected.

When the primary node with Administration persona is down, Sponsor administrators cannot create new guest user accounts. During this time, the guest and sponsor portals will provide read-only access to already created guest and sponsor users respectively. Also, a sponsor admin who has never logged into the sponsor portal before the primary Administration node went offline, will not be able to login to the sponsor portal until a secondary Administration node is promoted or the primary Administration node becomes available.

Prerequisite

Before beginning this task, you should have successfully completed Creating Identity Source Sequences, page 5-52.

To set the identity store sequence for sponsor authentication, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings > Sponsor > Authentication Source.**

Step 2 From the Identity Store Sequence drop-down list, choose the sequence to be used for the sponsor authentication.

Step 3 Click **Save**.

For More Information

See *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1* for more information on the sponsor portal.

Related Topics

- Creating a Custom Portal Theme, page 21-31
- Applying Language Templates, page 21-34

Specifying a Simple URL for Sponsor Portal Access

As a Cisco ISE admin, you can specify a fully qualified domain name (FQDN) URL so that it automatically resolves to the sponsor portal on a given node in a deployment. For example, you could set https://guest.company.com so that it resolves to the sponsor portal.

Warning **Making a change to the ports or FQDN value restarts all the nodes in the deployment, placing the new settings in the server.xml file of each node.**

To specify a FQDN URL for sponsor portal, complete the following steps:

Step 1 In the Cisco ISE Admin user interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **General > Ports**. The Guest / Sponsor Portal Settings page appears on the left.

Note If the sponsor portal is configured on any port other than 80, the sponsor is automatically redirected to the actual port that is configured. This redirection replaces the address in the sponsor's browser window.

Step 3 Under Sponsor Portal Settings, select the **Default Sponsor URL** check box and enter a fully qualified domain name URL in the text field. For example, you might enter guest.yourcompanyname.com.

Step 4 Click **Save**.

All nodes in the deployment restart, placing the new settings in the server.xml file of each node.

Step 5 Configure the network DNS server so that it resolves the FQDN to the ISE sponsor portal node.

Creating a Custom Portal Theme

You can customize a portal theme, changing text, banners, background color, and images. This functionality allows you to change the appearance of a portal without having to upload customized HTML files to the Cisco ISE server.

This section shows you how to create a custom portal theme, by setting and applying customized options. You can follow the same steps to modify an existing customized portal theme.

Note Supported image formats include jpg, jpeg, gif, and png.

To customize a portal theme, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **General > Portal Theme**. The Portal Theme page appears on the right.

Step 3 Customize the portal theme in the following ways:

- Change the Login Page Logo, page 21-32
- Change the Login Page Background Image, page 21-32
- Customize the Banner Logo, page 21-32
- Customize the Banner Background Image, page 21-33
- Change the Login Background Color, page 21-33

- Customize the Banner Background Color, page 21-33
- Customize the Content Background Color, page 21-34

Step 4 Click **Save**.

Change the Login Page Logo

This setting allows you to change the logo on the portal Login page. You can choose the default Cisco logo or upload a custom image.

To upload a custom login page logo, complete the following steps:

Step 1 Select **Upload New File** from the drop-down menu.

Step 2 Click **Browse**, navigate to and select the desired image file.

Step 3 Click **Open**.

Recommended guidelines for a login page logo image are as follows:

- Height: 16-480 pixels
- Width: 16-480 pixels

Change the Login Page Background Image

This setting allows you to change the background image on the portal login page. You can choose the default Cisco background or upload a custom background image.

To upload a custom background image, complete the following steps:

Step 1 Select **Upload New File** from the drop-down menu.

Step 2 Click **Browse**, navigate to and select the desired image file.

Step 3 Click **Open**.

Customize the Banner Logo

This setting allows you to change the portal banner logo. You can choose the default Cisco banner or upload a custom banner logo.

To upload a custom banner logo, complete the following steps:

Step 1 Select **Upload New File** from the drop-down menu.

Step 2 Click **Browse**, navigate to and select the desired image file.

Step 3 Click **Open**.

Customize the Banner Background Image

This setting allows you to change the portal banner background image. You can choose the default Cisco background or upload a custom background image.

To upload a custom banner background, complete the following steps:

Step 1 Select **Upload New File** from the drop-down menu.

Step 2 Click **Browse**, navigate to and select the desired image file.

Step 3 Click **Open**.

Change the Login Background Color

This setting allows you to change the background color of the portal login page.

To change the login page background color, complete the following steps:

Step 1 Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format, such as the following: FFFFFF.

Each pair of hexadecimal digits expresses an RGB value from 0-255.

Step 2 Click **Show Color** to display the specified color.

Customize the Banner Background Color

This setting allows you to change the banner background color of the portal.

To set the login background color, complete the following steps:

Step 1 Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format, such as the following: FFFFFF.

Each pair of hexadecimal digits expresses an RGB value from 0-255.

Step 2 Click **Show Color** to display the representative color.

Customize the Content Background Color

This setting allows you to change the content background color for the portal pages.

To change the content background color for the portal, complete the following steps:

Step 1 Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format such as FFFFFF.

Each pair of hexadecimal digits expresses an RGB value from 0-255.

Step 2 Click **Show Color** to display the representative color.

Note The login page background image or the banner image always override the content background color, unless the images are transparent.

For More Information

See *Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.1* for more information on the sponsor portal.

Related Topics

- Specifying an Authentication Source, page 21-29
- Applying Language Templates, page 21-34

Applying Language Templates

All the Cisco ISE supported language templates are active by default for a given browser locale. A Cisco ISE administrator has the option of modifying a standard language template, or creating a custom template for the sponsor portal user interface and the guest account notification text. This allows the administrator to control the language displayed for guests in print, email, or text-messages.

For information on UTF-8 support in language templates, see UTF-8 Character Support in the User Interface, page 21-36.

Note You are not allowed to create a new language template that uses the same browser locale mapping as an existing language template. Each language template must use a unique browser locale mapping.

This section describes the following topics and procedures:

- Internationalization and Localization, page 21-35
- Selecting a Standard Language Template, page 21-38
- Configuring Sponsor Language Templates, page 21-37
- Configuring Guest Language Templates, page 21-47

Internationalization and Localization

Cisco ISE internationalization adapts the user interface for supported languages. Localization of the user interface incorporates locale-specific components and translated text. In Cisco ISE, Release 1.1 internalization and localization support includes text in the user interface, such as labels, messages, as well as user input in text fields.

Supported Languages

Cisco ISE, Release 1.1 provides localization and internalization support for the following languages for the sponsor and guest portals:

Table 21-1 Supported Languages and Browser Locales

Language	Browser Locale
Chinese traditional	zh-tw
Chinese simplified	zh-cn
English	en
French	fr-fr
German	de-de
Italian	it-it
Japanese	ja-jp
Korean	ko-kr
Portuguese	pt-br (Brazilian)
Russian	ru-ru
Spanish	es-es

Internationalization and localization applies to all supported internet browsers.

Note Different browsers may use different locale IDs. The administrator can duplicate language templates on the Admin portal to resolve any browser locale differences.

Guest Portal

The Guest portal can be localized to present user interface elements in all supported language locales. This includes text, field names, button labels, and messages. You can configure supported language templates on the administrative portal.

Default templates for supported languages are included in a standard Cisco ISE installation. If an un-supported locale is requested by client browser, the English locale default portal is displayed.

The following Guest portal input fields support UTF-8:

- Login user name
- Login password
- All fields on the self-registration page

UTF-8 Character Support in the User Interface

The following table lists the fields in the Cisco ISE Admin user interface, and applicable Guest Portal fields, that support UTF-8 characters for data entry and viewing.

Table 21-2 Admin User Interface UTF-8 Character Fields

Admin User Interface Element	UTF-8 Fields
Network access user configuration	• User name • First name • Last name • Email
User list	• All filter fields • Values shown on the User List page • Values shown on the left navigation quick view
User password policy	• Advanced > Password may not contain characters
Administrator list	• All filter fields • Values shown on the Administrator List page • Values shown on the left navigation quick view
Admin login page	• User name
RSA	• Messages • Prompts
RADIUS token	• Authentication tab > Prompt
Posture Requirement	• Name • Remediation action > Message shown to Agent User • Requirement list display
Posture conditions	• File condition > File path • Application condition > Process name • Service condition > Service name • Conditions list display
Guest settings	• Sponsor > Language Template: all supported languages, all fields • Guest > Language Template: all supported languages, all fields • Guest > Password Policy

Admin User Interface Element	UTF-8 Fields
System settings	• SMTP Server > Default email address
Operations > Alarms > Rule	• Criteria > User • Notification > Email Notification user list
Operations > Reports	• Operations > Live Authentications > Filter fields • Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	• General Tools > RADIUS Authentication Troubleshooting > Username
Policies	• Authentication > value for the av expression within policy conditions • Authorization / posture / client provisioning > other conditions > value for the av expression within policy conditions
Attribute value in policy library conditions	• Authentication > simple condition / compound condition > value for the av expression • Authentication > simple condition list display • Authentication > simple condition list > left navigation quick view display • Authorization > simple condition / compound condition > value for the av expression • Authorization > simple condition list > left navigation quick view display • Posture > Dictionary simple condition / Dictionary compound condition > value for the av expression • Guest > simple condition / compound condition > value for the av expression

Note Cisco ISE 1.1 does not support UTF-8 characters in certificates.

Configuring Sponsor Language Templates

As a Cisco ISE administrator, you can add, modify, and delete custom language templates for both the sponsor and guest portals. You can also duplicate standard language templates, which you then modify to create a custom template. This section shows you how to configure language templates for the sponsor portal.

Note If you create a custom language template with a name that conflicts with a default template name, your template is automatically renamed after an upgrade and restore. After an upgrade and restore, default templates revert back to their default settings, and any templates with names that conflict with defaults are renamed as follows: user_{LANG_TEMP_NAME}.

For information on how to specify language templates for the guest portal, see Configuring Guest Language Templates, page 21-47.

This section covers the following topics:

- Selecting a Standard Language Template, page 21-38
- Adding a Custom Sponsor Language Template, page 21-38
- Editing and Duplicating a Sponsor Language Template, page 21-39
- Deleting a Custom Sponsor Language Template, page 21-40

Selecting a Standard Language Template

This procedure shows you how to specify any of the standard language templates for the sponsor portal, and configure the options.

To specify a standard language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template** to set the language for the sponsor portal.

Step 3 Select one of the language templates from the list.

Step 4 Specify configuration options for the template, as described in Step 5 of Adding a Custom Sponsor Language Template, page 21-38.

Adding a Custom Sponsor Language Template

This section shows you how to create a custom language template that you can apply to the sponsor portal.

Note You are not allowed to create a new language template using the same browser locale mapping as an existing language template. Each language template must use a unique browser locale mapping.

To add a custom sponsor language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template**.

Step 3 Click **Add** to create a new language template.

Step 4 Enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.

Step 5 Set the options on the following popup dialogs:

- Configure View All Guest Accounts
- Configure Create Single Guest Account
- Configure Create Random Guest Accounts
- Configure Import Guest Accounts
- Configure Bulk Create Status Display
- Configure Bulk Print Tabular Display
- Configure Sponsor Settings Customizations

- Configure Email Notification
- Configure SMS Text Notification
- Configure Print Notification
- Configure Date/Time Formats
- Configure Info/Error Messages
- Configure Popup Dialog Messages
- Configure Miscellaneous Items (Login/Banner/Drawer)

Step 6 Click **Submit**.

Some example configurations are presented in the following sections:

- Configuring a Template to Create a Single Guest Account, page 21-40
- Configuring a Template for Guest Notification, page 21-41

Related Topics

- Internationalization and Localization, page 21-35
- Selecting a Standard Language Template, page 21-38
- Editing and Duplicating a Sponsor Language Template, page 21-39
- Deleting a Custom Sponsor Language Template, page 21-40

Editing and Duplicating a Sponsor Language Template

This section shows you how to edit an existing language template, or duplicate and then modify a language template.

Note It is recommended that you copy and rename a default template to a unique name before making modifications. This ensures that you have the original template to go back to in case of an error.

To edit and duplicate a language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template** to configure a template for the sponsor portal.

Step 3 Select a language template from the list and do one of the following:

- Click **Edit** and modify the **Description** and valid **Browser Locale Mapping**, as necessary.
- Click **Duplicate** and enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.

Step 4 Modify the template configuration options as described in Step 5 of Adding a Custom Sponsor Language Template, page 21-38.

Step 5 Click **Submit**.

Related Topics

- Internationalization and Localization, page 21-35
- Selecting a Standard Language Template, page 21-38
- Adding a Custom Sponsor Language Template, page 21-38
- Deleting a Custom Sponsor Language Template, page 21-40

Deleting a Custom Sponsor Language Template

This section shows you how to delete a custom language template that is no longer needed.

Note You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

To delete a custom language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template**.

Step 3 Select the custom language template from the list, and click **Delete**.

Related Topics

- Internationalization and Localization, page 21-35
- Selecting a Standard Language Template, page 21-38
- Adding a Custom Sponsor Language Template, page 21-38
- Editing and Duplicating a Sponsor Language Template, page 21-39

Configuring a Template to Create a Single Guest Account

The Create Single Guest Account template includes the fields that appear in the Create Single Guest Account page in the sponsor portal. You can customize each field name and button in the manner and language in which you want them to appear in the sponsor portal.

Note The default configuration is English on all fields, unless changed.

To configure the Create Single Guest Account template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template**. The Sponsor Portal Language Templates page is displayed.

Step 3 Check the check box to select a template and Click **Edit**.

The Edit Language Template page appears.

Step 4 Click **Configuring Template for Create Single Guest Account** button.

Step 5 Edit the desired fields.

Step 6 Click **Save**.

Related Topics

- Configuring a Template for Guest Notification, page 21-41
- Applying Language Templates, page 21-34
- Selecting a Standard Language Template, page 21-38
- Deleting a Custom Sponsor Language Template, page 21-40

Configuring a Template for Guest Notification

When a guest account is created, the details of the account need to be passed from the sponsor to the guest. The Cisco ISE guest services provides the following ways to do this:

- Manually read the details to the guest from the screen.
- Print out the details out on paper.
- Send the details in an email.
- Send the details as an SMS text message.

Email and SMS text message notification require email servers to be configured.

The following sections describe how to configure different notification templates:

- Configuring a Template for Email Notification, page 21-41
- Configuring a Template for SMS Text Message Notification, page 21-43
- Configuring a Template for Print Notification, page 21-44

Configuring a Template for Email Notification

In the Email Notification template you can specify the subject and the body of the email that will be sent to guests for their account notification.

To configure the Email Notification template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template**. The Sponsor Portal Language Templates page is displayed.

Step 3 Check the check box to select a language template from the list and click **Edit**.

Step 4 Click **Configuring Template for Email Notification**.

Step 5 Type the subject of the email in the Subject text box. This value appears as the subject of the email notification when it is sent to the guest.

Step 6 Type the email body in the Layout text box. This contains the account login information for the guest user.

You can use HTML tags and special variables for formatting the language template for e-mail notification. The following is an example of the login information for the body of an email in an English language template:

Welcome to the Guest Portal, your username is %username% and password is %password%

The *%username%* and *%password%* strings will be replaced with the username and password values from the Guest User account.

In the email body you can use the following special variables to provide the details for the created guest account.

- %USERNAME% = The username created for the guest.
- %PASSWORD% = The password created for the guest.
- %STARTTIME% = The time from which the guest account will be valid.
- %ENDTIME% = The time at which the guest account will expire.
- %FIRSTNAME% = The first name of the guest.
- %LASTNAME% = The last name of the guest.
- %EMAIL% = The email address of the guest.
- %TIMEZONE% = The time zone of the user.
- %MOBILENUMBER% = The mobile number of the guest.
- %OPTION1% = Optional field for editing.
- %OPTION2% = Optional field for editing.
- %OPTION3% = Optional field for editing.
- %OPTION4% = Optional field for editing.
- %OPTION5% = Optional field for editing.
- %DURATION% = Duration of time for which the account will be valid.
- %RESTRICTEDWINDOW% = The time window during which the guest is not allowed to login.
- %TIMEPROFILE% = The name of the time profile assigned.

Note The special variables must be provided with either uppercase or lowercase letters. For example, the string for username should be %USERNAME% or %username%. Do not provide the string as %UserName%, which will not work.

Step 7 Click **Save**.

Related Topics

- Configuring a Template for Print Notification, page 21-44
- Configuring a Template to Create a Single Guest Account, page 21-40

Configuring a Template for SMS Text Message Notification

In the SMS Text Message Notification template you can set the SMS gateway, the subject and the message of the SMS.

The SMS Notification uses a third-party SMS gateway that allows email messages sent to the gateway containing formatted text messages to be forwarded through SMS to the specified end user account. An example of an SMS gateway is clickatell.com. You should have a valid account with the third party. Cisco does not provide a default account. SMS messages are sent by email to this gateway with a specific format defined by the third-party gateway.

To configure the SMS Text Message Notification template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template**. The Sponsor Portal Language Templates page is displayed.

Step 3 Select a language template from the list and click **Edit**.

Step 4 Click **Configure Template for SMS Text Message Notification.**

Step 5 Type the subject of the text SMS. This value appears as the subject of the SMS notification when it is sent to the guest.

Step 6 Type the SMS gateway in the Destination text box.

Step 7 Type the SMS body in the Layout text box. This contains the account login information for the guest user.

You can use HTML tags and special variables for formatting the language template for SMS notification. You can use the following special variables, which will be replaced with the details from the created guest account:

- %USERNAME% = The username created for the guest.
- %PASSWORD% = The password created for the guest.
- %STARTTIME% = The time from which the guest account will be valid.
- %ENDTIME% = The time at which the guest account will expire.
- %FIRSTNAME% = The first name of the guest.
- %LASTNAME% = The last name of the guest.
- %EMAIL% = The email address of the guest.
- %TIMEZONE% = The time zone of the user.
- %MOBILENUMBER% = The mobile number of the guest.
- %OPTION1% = Optional field for editing.
- %OPTION2% = Optional field for editing.
- %OPTION3% = Optional field for editing.
- %OPTION4% = Optional field for editing.
- %OPTION5% = Optional field for editing.
- %DURATION% = Duration of time for which the account will be valid.
- %RESTRICTEDWINDOW% = The time window during which the guest is not allowed to login.
- %TIMEPROFILE% = The name of the time profile assigned.

To send the text message to the mobile phone number of the guest, use the variable %MOBILENUMBER%. The %MOBILENUMBER% variable is replaced by the mobile phone number as entered by the sponsor.

Note The special variables must be provided with either uppercase or lowercase letters. For example, the string for username should be %USERNAME% or %username%. Do not provide the string as %UserName%, which will not work.

Step 8 Click **Save.**

Related Topics

- Configuring a Template for Email Notification, page 21-41
- Configuring a Template for Print Notification, page 21-44
- Configuring a Template to Create a Single Guest Account, page 21-40

Configuring a Template for Print Notification

In the Print Notification template, you can set the guest account details, which the sponsor can bring up in a browser, print, and hand to the guest after the account is created.

To configure the SMS Text Message Notification template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Sponsor > Language Template**. The Sponsor Portal Language Templates page is displayed.

Step 3 Select a language template from the list and click **Edit**.

Step 4 Click **Configure Template for Print Notification**

Step 5 In the Page Header text box, type the header of the page that will be printed.

Step 6 In the Layout text box, type the text to be printed. This contains the account login information for the guest user.

You can use HTML tags and special variables for formatting the language template for print notification. You can use the following special variables, which will be replaced with the details from the created guest account:

- %USERNAME% = The username created for the guest.
- %PASSWORD% = The password created for the guest.
- %STARTTIME% = The time from which the guest account will be valid.
- %ENDTIME% = The time at which the guest account will expire.
- %FIRSTNAME% = The first name of the guest.
- %LASTNAME% = The last name of the guest.
- %EMAIL% = The email address of the guest.
- %TIMEZONE% = The time zone of the user.
- %MOBILENUMBER% = The mobile number of the guest.

- %OPTION1% = Optional field for editing.
- %OPTION2% = Optional field for editing.
- %OPTION3% = Optional field for editing.
- %OPTION4% = Optional field for editing.
- %OPTION5% = Optional field for editing.
- %DURATION% = Duration of time for which the account will be valid.
- %RESTRICTEDWINDOW% = The time window during which the guest is not allowed to login.
- %TIMEPROFILE% = The name of the time profile assigned.

Note The special variables must be provided with either uppercase or lowercase letters. For example, the string for username should be %USERNAME% or %username%. Do not provide the string as %UserName%, which will not work.

Step 7 Click **Save**.

Related Topics

- Configuring a Template for Email Notification, page 21-41
- Configuring a Template for SMS Text Message Notification, page 21-43
- Configuring a Template to Create a Single Guest Account, page 21-40

Guest Settings

You can configure guest settings under this sub menu. The following configuration options are available here:

- Configuring Details Policy, page 21-45
- Configuring Guest Language Templates, page 21-47
- Multi-Portal Configurations, page 21-49
- Configuring Guest Portal Policy, page 21-68
- Configuring Guest Password Policy, page 21-69
- Time Profiles, page 21-70
- Configuring Guest Username Policy, page 21-73

Configuring Details Policy

The details policy determines the data that the sponsor needs to enter to create a guest account. In the details page, the Cisco ISE administrator must define the fields that should appear on the Sponsor Guest User Create and Edit pages and in the Guest User Self Registration page.

To configure a details policy, complete the following steps:

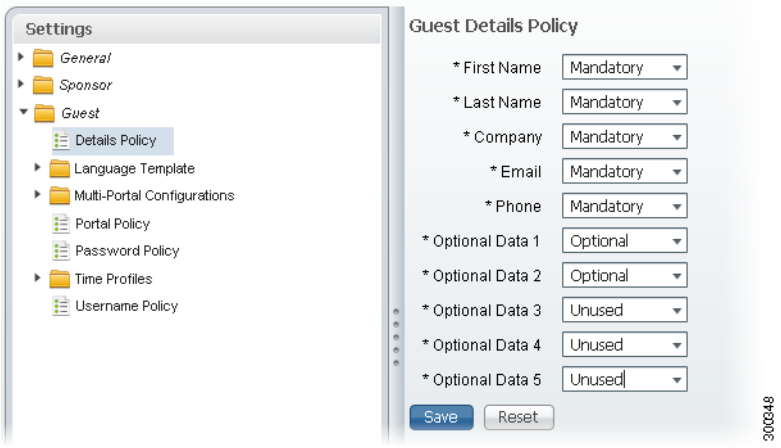
Step 1 From the Cisco ISE Administration interface, select **Administration > Guest Management > Settings.**

Step 2 In the Settings panel on the left, select **Guest > Details Policy**.

Step 3 Specify one of the following settings for each dialog field, as shown in Figure 21-3:

- Mandatory—If a field is set to mandatory it is displayed on the Guest User Account Create and Edit pages and it is required for the sponsor to complete.
- Optional—If a field is set to optional it is displayed on the Guest User Account Create and Edit pages. However, the sponsor can choose not to complete the field.
- Unused—If a field is set to unused it is not displayed on the Guest User Account Create and Edit page.

Figure 21-3 Details Policy Page



There are five Additional Fields that you can use to add any additional information that you require sponsors to fill out when creating guest accounts. These are described on the Details page as Additional Fields 1 through Additional Fields 5.

Note When **Create username from email address** is selected in Username Policy, you can not disable Email option in Guest Details Policy. See "Configuring Guest Username Policy" section on page 21-73 for more details.

See Dictionaries and Dictionary Attributes, page 7-1 for details on editing the field names.

Step 4 Click **Submit**.

Related Topics

- Configuring Guest Language Templates, page 21-47
- Multi-Portal Configurations, page 21-49
- Configuring Guest Portal Policy, page 21-68
- Configuring Guest Password Policy, page 21-69

- Time Profiles, page 21-70
- Configuring Guest Username Policy, page 21-73

Configuring Guest Language Templates

As a Cisco ISE administrator, you can add, modify, and delete custom language templates for both the sponsor and guest portals. You can also duplicate standard language templates, which you then modify to create a custom template. This section shows you how to configure language templates for the guest portal.

Note If you create a custom language template with a name that conflicts with a default template name, your template is automatically renamed after an upgrade and restore. After an upgrade and restore, default templates revert back to their default settings, and any templates with names that conflict with defaults are renamed as follows: user_{LANG_TEMP_NAME}.

For information about sponsor language templates, see Configuring Sponsor Language Templates, page 21-37.

This section covers the following topics:

- Selecting a Standard Language Template, page 21-47
- Adding a Custom Guest Language Template, page 21-47
- Editing and Duplicating a Guest Language Template, page 21-48
- Deleting a Guest Custom Language Template, page 21-49

Selecting a Standard Language Template

This procedure shows you how to specify a standard language template for the guest portal and configure its options.

To specify a standard language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Guest > Language Template**.

Step 3 Select one of the languages from the list.

Step 4 Specify configuration options for the template, as described in Step 5 of Adding a Custom Guest Language Template, page 21-47.

Adding a Custom Guest Language Template

This section shows you how to create a custom language template that you can apply to the guest portal.

To add a custom language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Guest > Language Template**.

Step 3 Click **Add** to create a new language template.

Step 4 Enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.

Step 5 Set the options on the following popup dialogs:

- Configure Template Definition
- Configure Login Page
- Configure Accept Use Policy
- Configure Change Password
- Configure Self Registration
- Configure Device Registration
- Configure VLAN/Install Release
- Configure Error Messages
- Configure Popup Dialog Messages
- Configure Miscellaneous Items

Step 6 Click **Submit**.

Some example configurations are presented in the following sections:

- Configuring a Template to Create a Single Guest Account, page 21-40
- Configuring a Template for Guest Notification, page 21-41

Related Topics

- Internationalization and Localization, page 21-35
- Selecting a Standard Language Template, page 21-38
- Editing and Duplicating a Guest Language Template, page 21-48
- Deleting a Guest Custom Language Template, page 21-49

Editing and Duplicating a Guest Language Template

This section shows you how to edit an existing guest language template, or duplicate and then modify a language template.

To edit and duplicate a language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Guest > Language Template**.

Step 3 Select the language template from the list and do one of the following:

- Click **Edit** and modify the **Description** and valid **Browser Locale Mapping**, as necessary.
- Click **Duplicate** and enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.

Step 4 Modify the template configuration options as described in Step 5 of Adding a Custom Guest Language Template, page 21-47.

Step 5 Click **Submit**.

Related Topics

- Internationalization and Localization, page 21-35
- Selecting a Standard Language Template, page 21-47
- Adding a Custom Guest Language Template, page 21-47
- Deleting a Guest Custom Language Template, page 21-49

Deleting a Guest Custom Language Template

This section shows you how to delete a custom language template that is no longer needed.

Note You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

To delete a custom language template, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel on the left, select **Guest > Language Template**.

Step 3 Select the custom language template from the list, and click **Delete**.

Related Topics

- Internationalization and Localization, page 21-35
- Selecting a Standard Language Template, page 21-47
- Adding a Custom Guest Language Template, page 21-47
- Editing and Duplicating a Guest Language Template, page 21-48

Multi-Portal Configurations

Cisco ISE provides you with the ability to host multiple portals on the Cisco ISE server. The default portal themes have standard Cisco branding that you can customize through the Cisco ISE Admin user interface. The default portal pages are dynamically generated and provide features such as change password and self registration in the Login Screen.

You can also choose to customize a portal by uploading HTML pages that are specific to your organization. These pages must use plain HTML code and must contain form actions that point to the portal backend servlets. You must define separate HTML pages for login, acceptable use policy (AUP), the change-password function, and self-registration.

Note To access a custom uploaded portal, the portal URL must include the name of the portal specified during the upload.

Related Topics

- Configuring Device Registration WebAuth, page 21-10
- Hosting Multiple Portals, page 21-50
- Sample HTML Code for Creating Portal Pages, page 21-54

Hosting Multiple Portals

Prerequisite

Before beginning this task, you should have successfully understood and configured the following:

- Understanding Authentication Policies, page 16-1
- Configuring the Simple Authentication Policy, page 16-26
- Configuring the Rule-Based Authentication Policy, page 16-29

A predefined DefaultGuestPortal is available under Multi-Portal Configurations. This portal has the default Cisco look-and-feel that you can choose to customize it through the Cisco ISE Admin user interface, or you can upload HTML pages to create a customized portal. To create a personalized portal with custom HTML pages, you must first add a new portal.

Guest Portal URL

The following procedure utilizes the Guest portal URL. For reference, the Guest portal URL for the wired and wireless local web authentication is as follows:

`https://ip:8443/guestportal/portals/PortalName/portal.jsp`

Where the *PortalName* is the name of the portal as it is created during the upload.

The Guest portal redirect URL for CWA is:

`https://ip:port/guestportal/gateway?sessionId=SessionIdValue&portal=PortalName&action=cwa`

The ‘ip’ and ‘port’ values are updated by the RADIUS server as the URL-redirect is returned to the NAD. These values are the IP address and port number for the Cisco ISE guest portal server.

Note The port number 8443 is configurable through **Administration > Guest Management > Settings > General > Port**.

To add a new portal, complete the following steps:

Step 1 From the Cisco ISE Administrator interface, choose **Administration > Guest Management > Settings**.

Step 2 In the Settings panel, choose **Guest > Multi-Portal Configurations**.

Step 3 Click **Add**.

Step 4 On the General tab, enter a **Name** and **Description** for the new portal.

Note The name of the portal is used to access the portal and will appear in the captive portal URL specified in the network access device (NAD) for wireless LAN controller (WLC) setups. For example, a portal with the name *ClientPortal* will have the following access URL: https://*ip address:port number*/guestportal/portals/ClientPortal/portal.jsp

Step 5 Select one of the following portal types:

- Default Portal (Choose customization template and theme)
- Device Web Authentication Portal (Choose customization template and theme), and then specify an Endpoint Identity Group
- Custom Default Portal (Upload files)
- Custom Device Web Authentication Portal (Upload files), and then specify an Endpoint Identity Group

Step 6 Select the **Operations** tab and do the following:

- For a Default Portal make the following selections:
  - Guest users should agree to an acceptable use policy: Not Used, First Login, Every Login. For details, see "Accept Use Policy" section on page 21-52.
  - Allow guest users to change password. See "Change Password" section on page 21-52.
  - Require guest and internal users to change password at expiration. See "Change Password" section on page 21-52.
  - Guest users should download the posture client. See "Client Provisioning Interaction with Guest Portal" section on page 21-53.

    Check the VLAN DHCP Release option to refresh Windows clients IP address after a VLAN change in both wired or wireless environments for Guest with no posture.
  - Guest users should be allowed to do self service. See "Self Registration" section on page 21-53 (If you check this option, ensure that you configure Portal policy as described in "Configuring Guest Portal Policy" section on page 21-68).
  - Guest users should be allowed to do device registration. "Device Registration" section on page 21-53.
  - Check VLAN DHCP Release option, and provide the following values in seconds: Delay to Release, Delay to CoA, and Delay to Renew. For details, see "VLAN DHCP IP Release/Renew" section on page 21-53.
- For a Device Web Authentication Portal, make the following selections:
  - Guest users should agree to an acceptable use policy: Not Used, First Login, Every Login. For details, see "Accept Use Policy" section on page 21-52.
  - Check VLAN DHCP Release option, and provide the following values in seconds: Delay to Release, Delay to CoA, and Delay to Renew. For details, see "VLAN DHCP IP Release/Renew" section on page 21-53.

Step 7 Select the **Customization** tab, and do one of the following:

- Check the Use Browser Locale language check box.
- Uncheck the User Browser Locale language check box and select a standard Language template from the list.

Step 8 To upload custom files, select the Customize File Upload tab, upload the HTML files you have created for the Login, AUP, Change Password, and Self Registration pages. See "Sample HTML Code for Creating Portal Pages" section on page 21-54 for creating the HTML files.

These pages can include images and other links to the upload files. All uploaded files are held in a single directory with no subdirectories. Add "portals/<*portalname*>" to indicate the path to the files in the HTML code. You cannot run any backend scripts in the Cisco ISE server. Only HTML, HTM, JPEG, GIF, PNG, and CSS files are allowed.

Step 9 Under the File Mapping tab, identify and choose the HTML files uploaded for the particular guest pages.

This is important for the guest flow to redirect and display the appropriate client-defined portal pages during the guest login access.

The fields under File Mapping tab are grayed out or enabled based on the selections made in the General tab.

Step 10 For a Default Portal, click the **Authentication** tab and choose the users to be authenticated during the guest login.

- Guest—Guest is the local guest user and Central WebAuth is the non-guest user. If you have a non-guest user or both a guest and non-guest user, you have to specify an identity sequence for the authentication. If Guest is chosen the default portal only authenticates guest user accounts in the local database.
- Central WebAuth—If Central WebAuth is chosen, the specified identity sequence is used to check authentication for the user. This sequence can contain both a local database and external identity stores such as Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory.

  For Central WebAuth to allow network access, appropriate authentication policies must be defined within Cisco ISE for the underlying RADIUS server to process authentication correctly.
- Both—If you chose to authenticate both, the user will be authenticated against the local database guest users first. If a user is not found, authentication will be attempted using the identity sequence.

Step 11 Click **Submit**.

Customizable Guest Portal Pages

The following are customizable Guest portal pages:

- Accept Use Policy, page 21-52
- Change Password, page 21-52
- Self Registration, page 21-53
- Device Registration, page 21-53

Accept Use Policy

This page displays the terms of use of the network, which the user must accept in order to fully enable their account. If the user does not accept the policy the user will not gain expanded network access. For guest users, the AUP can be selected to appear at first login only or at every login.

Change Password

Once the guest user or internal user has accepted the policy Cisco ISE checks if the password has expired, if so the Password Change screen is displayed. External users do not have their password expiration enforced.

To configure the guest password contents, see "Configuring Guest Password Policy" section on page 21-69.

To configure password policy for the internal users, see "User Password Policy" section on page 4-66.

Screens in the default portal show the password criteria for Guest or Internal Users depending on the identity of the User. You can set your own criteria in the custom portals screens.

Self Registration

The Self Registration screen appears as a link on the guest user login page. This screen allows new guest users to fill in their personal information and create a new user account. Upon submission, the user account is created and the new account information is displayed on the screen. The user can print the account information.

User accounts are created with a random generated password. This password follows the password policy that is set for the guest users. The user accounts are created with the default Guest Role and Time Profile as selected in the Guest Portal Policy page.

Device Registration

The Device Registration screen appears as a link on the guest user login page. This screen allows a guest user to register their own network devices based on the MAC address of the devices.

You can configure the maximum number of devices per user from the Guest Portal Policy page and it is a global value for the entire system. The default maximum number of devices per user is five. Lowering this value will not remove existing registered devices, it will only limit the addition of new devices. The default Device Registration page has a list of existing devices for the user. Users can add new devices or remove devices from this page.

You can also add device registration page for your custom portal. But, this page will only have the ability to add new devices. There will be no list of existing devices nor can you delete devices. These limitations exist because listing is a dynamically created page and does not allow customization.

Client Provisioning Interaction with Guest Portal

The guest user portal includes interaction with Client Provisioning application so that the client machine posture can be controlled at the time of a network access request. This interaction consists of redirecting the client browser to download a Client Provisioning agent and controlling posture before allowing full access to the network with a final user login.

You can configure custom portal to perform Client Provisioning and Posture. If you select this option, the guest login flow performs a CWA and the guest portal will be redirected to Client Provisioning after performing AUP and change password checks. In this case, the posture subsystem performs a CoA to the NAD to re-authenticate the client connection once the posture has been assessed.

Note Client Provisioning does not occur in Local Web Authentication scenarios.

If **Vlan Dhcp Release** is selected under Multi-Portal Configurations, posture will perform the client side IP release and renew operation.

Check the **Vlan Dhcp Release** option to refresh Windows clients IP address after VLAN change in both wired or wireless environments for Guest with posture.

VLAN DHCP IP Release/Renew

This affects the CWA user login flow when the network access during the final authorization switches the guest VLAN to a new VLAN. In this case, the old IP of the guest needs to be released before the VLAN change and a new guest IP needs to be requested through DHCP once the new VLAN access is in place. The Cisco ISE server redirects the guest browser to download an applet to perform the IP release renew operation.

The delay to release time should be low since it needs to occur immediately after the applet is downloaded and before the Cisco ISE server directs the NAD to re-authenticate with a CoA request. The default release value is 1 second.

The delay to CoA delays the Cisco ISE from executing the CoA. Here, enough time should be given to allow the applet to download and perform the IP release on the client. The default value is 8 seconds.

The delay to renew value is added to the IP release value and does not begin timing until the control is downloaded. The renew should be given enough time so that the CoA is allowed to process and the new VLAN access granted. The default value is 12 seconds.

For More Information

For switch configuration details and other Cisco ISE deployment information, see Chapter 9, "Setting Up Cisco ISE in a Distributed Environment."

Related Topics

- Configuring Details Policy, page 21-45
- Multi-Portal Configurations, page 21-49
- Configuring Guest Portal Policy, page 21-68
- Configuring Guest Password Policy, page 21-69
- Time Profiles, page 21-70
- Configuring Guest Username Policy, page 21-73

Sample HTML Code for Creating Portal Pages

The following are some example HTML codes that you can use to create multiple guest portal pages:

- Login Form Action and Parameters, page 21-54
- AUP Form Action and Parameters, page 21-57
- Change Password Form Action and Parameters, page 21-59
- Self-Registration Form Action and Parameters, page 21-60
- Device Registration Form Action and Parameters, page 21-62
- Self-Service Result Form Action and Parameters, page 21-64
- Error Page Form Action and Parameters, page 21-65
- Successful Guest Login Form, page 21-66

Note The following HTML examples reference a directory structure for a portal named demo2.

Login Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
<script language='javascript'>

</script>
</head>
<body class="pagebg">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="107"> </td>
  </tr>
  <tr>
```

```
    <td height="172" align="center" valign="middle"><table width="90%" border="0"
align="center" cellpadding="0" cellspacing="0">
        <tr>
          <td width="45%" height="172" align="left" valign="middle"><table width="75%"
border="0" align="left" cellpadding="0" cellspacing="0">
              <tr>
                <td width="27%"><img src="portals/demo2/logo.png" alt="" width="218"
height="63" /></td>
                <td width="73%"><table width="85%" border="0" align="right"
cellpadding="0" cellspacing="0">
                  <tr>
                    <td height="35" align="left" class="headding">ISE 1.1</td>
                  </tr>
                  <tr>
                    <td align="left" class="label">Guest Access</td>
                  </tr>
                  <tr>
                    <td align="left"> </td>
                  </tr>
                  <tr>
                    <td align="left" class="headding1">Version:1.1</td>
                  </tr>
                </table></td>
              </tr>
            </table></td>
          <td width="45%" align="right" valign="middle"><table width="50%" border="0"
cellspacing="0" cellpadding="0">
          <form id="cuesLoginForm" method="POST"
action="/guestportal/LoginCheck.action">
              <tr>
                <td width="32%" height="30" align="left" valign="middle"
class="label">Username :</td>
                <td width="68%" align="left"><input alt="Username:" name="guestUser.name"
id="username" type="text" size="20" value=""/></td>
              </tr>
              <tr>
                <td height="30" align="left" valign="middle" class="label">Password :</td>
                <td align="left"><input alt="Password:" name="guestUser.password"
id="password" type="password" size="20" value=""/></td>
              </tr>
              <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
              </tr>
              <tr>
                <td align="left" valign="middle"> </td>
                <td align="left"><input type="submit" name="button" id="button" value="Log
In" />
                </td>
              </tr>
              <input type="hidden" name="drpPassword" id="drpPassword"  />
              <input type="hidden" name="drpUsername" id="drpUsername"  />
            </form>
<!--          <form id="doSelfService" action="/guestportal/SelfService.action">-->
<!--            <input type="hidden" id="buttonClicked" name="buttonClicked"
value=""></input>-->
<!--            <input type="hidden" id="switch_url" name="switch_url" value=""></input>-->
<!--            <input type="hidden" id="redirect" name="redirect" value=""></input>-->
<!--            <input type="hidden" id="err_flag" name="err_flag" value=""></input>-->
<!--          </form>-->

              <!-- form for self service  -->
              <struts2:form id="selfServiceForm" action="SelfService.action">
```

```
                <input type="hidden" id="buttonClicked" name="buttonClicked"
value="${buttonClicked}"></input>
                <input type="hidden" id="switch_url" name="switch_url"
value="${switch_url}"></input>
                <input type="hidden" id="redirect" name="redirect"
value="${redirect}"></input>
                <input type="hidden" id="err_flag" name="err_flag"
value="${err_flag}"></input>
                </struts2:form>

                <struts2:form id="changePasswordForm"
action="ChangePassLoginMultiPortal.action">
                  <input type="hidden" id="username" name="guestUser.name"
value="${username}"></input>
                  <input type="hidden" id="password" name="guestUser.password"
value="${password}"></input>
                </struts2:form>

               <tr>
                 <td align="left" valign="middle"> </td>
                 <td align="left">   
                 </td>
               </tr>
               <tr>
                 <td align="left" valign="middle"> </td>
                  <td align="left"><a href="javascript:doChangePassword();" class="link"
>Change Password</a>  
                 <a href="javascript:doSelf();"  class="link">SelfService</a>  
                 <a href="javascript:submitMyForm();"  class="link">Device Registration</a>
                 </td>
               </tr>

            </table></td>
        </tr>
      </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>
function doSelf()
{
    document.forms[0].action = "SelfService.action";
    document.getElementById("buttonClicked").value =
document.getElementById("buttonClicked").value;
    document.getElementById("redirect").value = document.getElementById("redirect").value;
    document.getElementById("switch_url").value =
document.getElementById("switch_url").value;
    document.forms[0].submit();
}

function doChangePassword()
{
    //var changePasswordForm = document.getElementById("changePasswordForm");
    //changePasswordForm.submit();
    document.forms[0].action = "ChangePassLoginMultiPortal.action";
    document.getElementById("username").value = document.getElementById("username").value;
    document.getElementById("password").value = document.getElementById("password").value;
    document.forms[0].submit();
}
```

```
function submitMyForm(){
    document.forms[0].action = "DevRegPortalLogin.action";
    document.getElementById("drpUsername").value =
document.getElementById("username").value;
    document.getElementById("drpPassword").value =
document.getElementById("password").value;
    document.forms[0].submit();
}

</script>
```

AUP Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
</head>
<body bgcolor="#ccebfe">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img src="portals/demo2/logo.png"
alt="" width="157" height="44" /></td>
        <td width="72%" class="headding">ISE 1.1 Guest Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td bgcolor="#ccebfe"><table width="98%" border="0" align="center" cellpadding="0"
cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
      <tr>
        <td align="left" class="headding2">Acceptable Use Policy</td>
      </tr>
      <tr>
        <td align="left" >Please accept the policy:<br /><br />

1. You are responsible for </br>(1) maintaining the confidentiality of the password and
</br>(2) all activities that occur under your username and password.
</br></br>
2. Cisco systems offers the Service for activities such as the active use of e-mail,
instant messaging, browsing the World Wide Web and accessing corporate intranets. High
volume data transfers, especially sustained high volume data transfers, are not permitted.
Hosting a web server or any other server by use of our Service is prohibited. Trying to
access someone elseâ ™s account, sending unsolicited bulk e-mail, collection of other
peopleâ ™s personal data without their knowledge and interference with other network users
are all prohibited.
</br></br>
3. Cisco systems reserves the right to suspend the Service if (1) Cisco systems reasonably
believes that your use of the Service is unreasonably excessive or (2) you are using the
Service for criminal or illegal activities.
</br></br>
4. You do not have the right to resell this Service to a third party.

</br></br>
```

```
5. Cisco systems reserves the right to revise, amend or modify these Terms & Conditions,
our other policies and agreements, and aspects of the Service itself. Notice of any
revision, amendment, or modification will be posted on Cisco systemâ ™s website and will
be effective as to existing users 30 days after posting same.
</br></br></td>
      </tr>
      <form action="/guestportal/AcceptPolicy.action" method="post">
      <tr>
        <td align="left"><input  type="checkbox" name="guestUser.acceptUsePolicy"
id="guestUser.acceptUsePolicy" value="false" onclick="javascript:enableButtons()" />Accept
terms and conditions</td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"><input  type="Submit" id="acceptButton"  value="Accept" />
              <input  type="button"  id="declineButton" value="Decline"
onclick="javascript:doDeclineTerms()"/></td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      </form>
    </table></td>
  </tr>
</table>
<form id="declineTerms" onsubmit="return true;" action="/guestportal/DeclinePolicy.action"
method="post"><table class="wwFormTable">
<input type="hidden" id="buttonClicked" name="buttonClicked" value=""></input>
<input type="hidden" id="switch_url" name="switch_url" value=""></input>
<input type="hidden" id="redirect" name="redirect" value=""></input>
<input type="hidden" id="err_flag" name="err_flag" value=""></input>
</table></form>

<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>
enableButtons();
function enableButtons(){
  accepttermsCheckbox = document.getElementById('guestUser.acceptUsePolicy').checked;
  if (!accepttermsCheckbox) {
    document.getElementById('acceptButton').disabled = true;
    document.getElementById('guestUser.acceptUsePolicy').value = false;
  }
  else {
    document.getElementById('acceptButton').disabled = false;
    document.getElementById('guestUser.acceptUsePolicy').value = true;
  }
}
</script>

<script>
function doDeclineTerms()
{
    var declineTermsForm = document.getElementById("declineTerms");
    declineTermsForm.submit();
}
</script>
```

Change Password Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
</head>
<body class="pagebg">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="107"> </td>
  </tr>
  <tr>
    <td height="172" align="center" valign="middle"><table width="90%" border="0"
align="center" cellpadding="0" cellspacing="0">
        <tr>
          <td width="45%" height="172" align="left" valign="middle"><table width="75%"
border="0" align="left" cellpadding="0" cellspacing="0">
              <tr>
                <td width="27%"><img src="portals/demo2/logo.png" alt="" width="218"
height="63" /></td>
                <td width="73%"><table width="85%" border="0" align="right"
cellpadding="0" cellspacing="0">
                  <tr>
                    <td height="35" align="left" class="headding">ISE 1.1</td>
                  </tr>
                  <tr>
                    <td align="left" class="label">Guest Access</td>
                  </tr>
                  <tr>
                    <td align="left"> </td>
                  </tr>
                  <tr>
                    <td align="left" class="headding1">Version:1.1</td>
                  </tr>
                </table></td>
              </tr>
            </table></td>
          <td width="45%" align="right" valign="middle"><table width="65%" border="0"
cellspacing="0" cellpadding="0">
              <form action="/guestportal/ChangePassword.action" method="post">
              <tr>
                <td height="30" align="left" valign="middle" class="label">Enter current
password :</td>
                <td align="left"><input alt="Password:" name="currentpassword"
id="currentpassword" type="password" size="20" value=""/></td>
              </tr>
               <tr>
                <td height="30" align="left" valign="middle" class="label">Enter new
password :</td>
                <td align="left"><input alt="Password:" name="newpassword"
id="newpassword" type="password" size="20" value=""/></td>
              </tr>
               <tr>
                <td height="30" align="left" valign="middle" class="label">Re-enter new
password :</td>
                <td align="left"><input alt="Password:" name="confirmpassword"
id="confirmpassword" type="password" size="20" value=""/></td>
              </tr>
              <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
              </tr>
              <tr>
```

```
                <td align="left" valign="middle"> </td>
               <td align="left"><input type="submit" name="button" id="button" value="Log
In" />
                </td>
              </tr>
             </form>
            </table></td>
        </tr>
      </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>
```

Self-Registration Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
</head>
<body bgcolor="#ccebfe">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img src="portals/demo2/logo.png"
alt="" width="157" height="44" /></td>
        <td width="72%" class="headding">ISE 1.1 Guest Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td valign="top" bgcolor="#ccebfe"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
      <tr>
        <td align="left" class="headding2">Self Registration</td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"><table width="50%" border="0" align="left" cellpadding="0"
cellspacing="0" class="content">
       <form id="selfServiceForm" action="/guestportal/SelfServiceSubmit.action"
method="post">
              <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">First Name :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.firstName" id="firstName" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Last Name :</td>
```

```
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.lastName" id="lastName" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Email Address :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.emailAddress" id="emailId" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Phone Number :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.phoneNumber" id="phoneno" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Company :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.company" id="company" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 1 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData1" id="data1" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 2 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData2" id="data2" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 3 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData3" id="data3" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 4 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData4" id="data4" type="text" size="20" /></td>
              </tr>
               <tr>
                <td width="30%" height="30" align="left" valign="middle"
class="content">Optional Data 5 :</td>
                <td width="70%" align="left"><input alt="Username:"
name="guestUser.optionalData5" id="data5" type="text" size="20" /></td>
              </tr>

       <tr>
       <td width="30%" height="30" align="left" valign="middle" class="content">TimeZone
:</td>
       <td width="70%" align="left"><select name="guestUser.timezone">
       <option value="UTC">UTC</option>
       <option value="America\New_York">America\New_York</option>
       <option value="Europe\London">Europe\London</option>
       </select></td>
       </tr>
              <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
```

```
              </tr>
              <tr>
                <td align="left" valign="middle"> </td>
                <td align="left"><input type="submit" name="button" id="button"
onclick="javascript:doOnSubmit()" value="Submit" />
                <input type="submit" name="button2" id="button2"
onclick="javascript:doCancel()" value="Cancel" />               </td>
              </tr>
             </form>
          </table></td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
    </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>
function doOnSubmit()
{
    var selfServiceForm = document.getElementById("selfServiceForm");
    selfServiceForm.submit();
}
function doCancel()
{
    document.forms[0].action = "Login.action";
    document.forms[0].submit();
}
</script>
```

Device Registration Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
<script language='javascript'>

</script>
</head>
<body bgcolor="#ccebfe">
<form id="deviceRegistrationPortal"  action="/guestportal/RegisterDevice.action"
method="post">

    <input type="hidden" name="drpUsername" id="drpUsername" value="" />
    <input type="hidden" name="devRegLimit" id="devRegLimit" value="" />

    <input type="hidden" name="regDevices" id="regDevices" value="" />
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img src="portals/demo2/logo.png"
alt="" width="157" height="44" /></td>
```

```
        <td width="72%" class="headding">ISE 1.1 Device Registration Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td align="left" valign="top" bgcolor="#ccebfe"><table width="98%" border="0"
align="center" cellpadding="0" cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
      <tr>
        <td align="left"><table width="100%" border="0" cellpadding="0" cellspacing="0"
bgcolor="#abcee4" style="padding:10px; border:#6b93ac solid 1px;">
          <tr>
            <td style="padding:10px 0 0 10px;">Please register your device :<br />
Please note that you can not register more than 5 devices</td>
          </tr>
          <tr>
            <td height="15"></td>
          </tr>
          <tr>
           <td style="padding:0 0 0 10px;"><table width="100%" border="0" cellspacing="0"
cellpadding="0">
  <tr>
    <td width="7%">MAC Address : </td>
    <td width="93%"><input id="registeredMac"  name="registeredMac" type="text" /></td>
  </tr>
</table></td>
          </tr>
           <tr>
            <td height="15"></td>
          </tr>
          <tr>
            <td style="padding:0 0 0 10px;"><input  type="Submit"    value="Register"
/></td>
          </tr>
          <tr>
            <td height="15"></td>
          </tr>
        </table></td>
      </tr>

      <tr>
        <td align="left"> </td>
      </tr>

      <tr>
        <td align="left">
    </td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>

    </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</form>
</body>
</html>
```

Self-Service Result Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
</head>
<body bgcolor="#ccebfe">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img src="portals/demo2/logo.png"
alt="" width="157" height="44" /></td>
        <td width="72%" class="headding">ISE 1.1 Guest Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td valign="top" bgcolor="#ccebfe"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
      <tr>
    <!--INSERT HEADER HERE --><td align="left" class="headding2"> Self Registration
created user: fsdf</td><!--END HEADER HERE -->
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"><table width="50%" border="0" align="left" cellpadding="0"
cellspacing="0" class="content">
          <!--INSERT RESULTS HERE --><tr><td width="30%" align="left" class="content">
User name: fsdf</td></tr><tr><td width="30%" align="left" class="content"> Password:
9F_</td></tr><tr><td width="30%" align="left" class="content"> First Name:
fdsf</td></tr><tr><td width="30%" align="left" class="content"> Last Name:
sdf</td></tr><tr><td width="30%" align="left" class="content"> Email Address:
</td></tr><tr><td width="30%" align="left" class="content"> Phone Number:
</td></tr><tr><td width="30%" align="left" class="content"> Company: </td></tr><tr><td
width="30%" align="left" class="content"> Optional Data 1: </td></tr><tr><td width="30%"
align="left" class="content"> Optional Data 2: </td></tr><tr><td width="30%" align="left"
class="content"> Optional Data 3: </td></tr><tr><td width="30%" align="left"
class="content"> Optional Data 4: </td></tr><tr><td width="30%" align="left"
class="content"> Optional Data 5: </td></tr><!--END RESULTS HERE -->
              <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
              </tr>
              <form id="loginform" action="/guestportal/Login.action" method="post">
          <tr>
                <td align="left" valign="middle"> </td>
                <td align="left"><input type="submit" name="button2" id="button2"
onclick="javascript:doOk()" value="OK" />                </td>
              </tr>
          </form>
          </table></td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
```

```
      <tr>
        <td align="left"> </td>
      </tr>
    </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>

function doOk()
{
    document.forms[0].action = "Login.action";
    document.forms[0].submit();
}
</script>
```

Error Page Form Action and Parameters

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Error Detected</title>
<link href="portals/demo2/style.css" rel="stylesheet" type="text/css" />
<script language='javascript'>

</script>
</head>
<body class="pagebg">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="107"> </td>
  </tr>
  <tr>
    <td height="172" align="center" valign="middle"><table width="90%" border="0"
align="center" cellpadding="0" cellspacing="0">
        <tr>
          <td width="45%" height="172" align="left" valign="middle"><table width="75%"
border="0" align="left" cellpadding="0" cellspacing="0">
              <tr>
                <td width="27%"><img src="portals/demo2/logo.png" alt="" width="218"
height="63" /></td>
                <td width="73%"><table width="85%" border="0" align="right"
cellpadding="0" cellspacing="0">
                  <tr>
                    <td height="35" align="left" class="heading">Error Detected in Guest
Portal</td>

                  </tr>
                  <tr>
           <!--INSERT ERROR HERE -->
                    <td height="35" align="left" class="heading">Second</td>
           <!--END ERROR HERE -->
                  </tr>
                </table></td>
              </tr>
            </table></td>
          <td width="45%" align="right" valign="middle"><table width="50%" border="0"
cellspacing="0" cellpadding="0">

              <tr>
```

```
                <td align="left" valign="middle"> </td>
                <td align="left">   
                </td>
              </tr>

            </table></td>
        </tr>
      </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2009-2011, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>
function doSelf()
{
    document.forms[0].action = "Login.action";
    document.forms[0].submit();
}
</script>
```

Successful Guest Login Form

```
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>Guest Portal Login</title>
<link href="portals/CustomPortal/style.css" rel="stylesheet" type="text/css" />
</head>
<body bgcolor="#ccebfe">
<table width="100%" border="0" align="center" cellpadding="0" cellspacing="0">
  <tr>
    <td height="75" bgcolor="#022d4d"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0">
      <tr>
        <td width="15%" align="left" valign="middle"><img
src="portals/CustomPortal/logo.png" alt="" width="90" height="90" /></td>
        <td width="72%" class="headding">ISE 1.0 Guest Portal</td>
        <td width="13%" align="right" valign="middle" > </td>
      </tr>
    </table></td>
  </tr>
  <tr>
    <td valign="top" bgcolor="#ccebfe"><table width="98%" border="0" align="center"
cellpadding="0" cellspacing="0" class="content">
      <tr>
        <td> </td>
      </tr>
      <tr>
    <!--INSERT HEADER HERE --><td align="left" class="headding2"> CoA Successful
</td><!--END HEADER HERE -->
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"><table width="50%" border="0" align="left" cellpadding="0"
cellspacing="0" class="content">

        <tr>
                <td height="12" align="left" valign="middle"></td>
                <td height="12" align="left"></td>
```

```
              </tr>
              <form id="loginform" action="/guestportal/Login.action" method="post">
          <tr>
                <td align="left" valign="middle"> </td>
                <td align="left"><input type="submit" name="button2" id="button2"
onclick="javascript:doOk()" value="OK" />               </td>
              </tr>
          </form>
          </table></td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
      <tr>
        <td align="left"> </td>
      </tr>
    </table></td>
  </tr>
</table>
<div id="footer">
  <div  style="padding:0 0 0 10px;">2008-2009, Sample App, Inc. All rights reserved.</div>
</div>
</body>
</html>

<script>

function doOk()
{
    document.forms[0].action = "Login.action";
    document.forms[0].submit();
}
</script>
```

Sample style.css

```
@charset "utf-8";
/* CSS Document */

body {
    margin-left: 0px;
    margin-top: 0px;
    margin-right: 0px;
    margin-bottom: 0px;
}
.pagebg {
    background:url("../demo2/pageBg.jpg") repeat-x;
}
.label {
    font-family:Arial, Helvetica, sans-serif;
    color:#FFFFFF;
    font-size:12px;
}
#footer {
    height:23px;
    font-family:Arial, Helvetica, sans-serif;
    color:#022d4d;
    position:absolute;
    width:100%;
    margin:0px auto;
    text-align:left;
    bottom:-0px;
    font-size:12px;
}
```

```
.headding {
font-family:Arial, Helvetica, sans-serif;
color:#ffffff;
font-size:20px;
}
.headding1 {
font-family:Arial, Helvetica, sans-serif;
font-size:12px;
font-weight:bold;
color:#ffffff;
}
.headding2 {
font-family:Arial, Helvetica, sans-serif;
color:#022d4d;
font-size:17px;
font-weight:bold;
}
.headding3 {
font-family:Arial, Helvetica, sans-serif;
color:#022d4d;
font-size:12px;
font-weight:bold;
}
.content {
font-family:Arial, Helvetica, sans-serif;
font-size:11px;
color:#022d4d;
}
.link {font-family:Arial, Helvetica, sans-serif; font-size:11px; color:#ffffff;
text-decoration:none;}
a.link:link {font-family:Arial, Helvetica, sans-serif; font-size:11px; color:#ffffff;
text-decoration:none;}
a.link:hover {font-family:Arial, Helvetica, sans-serif; font-size:11px; color:#ffffff;
text-decoration:underline; }
```

Configuring Guest Portal Policy

The admin can use the guest portal policy page to specify the required flow for the guest user login.

To configure a guest portal policy, complete the following steps:

Step 1 From the Cisco ISE Administration interface, select **Administration > Guest Management > Settings.**

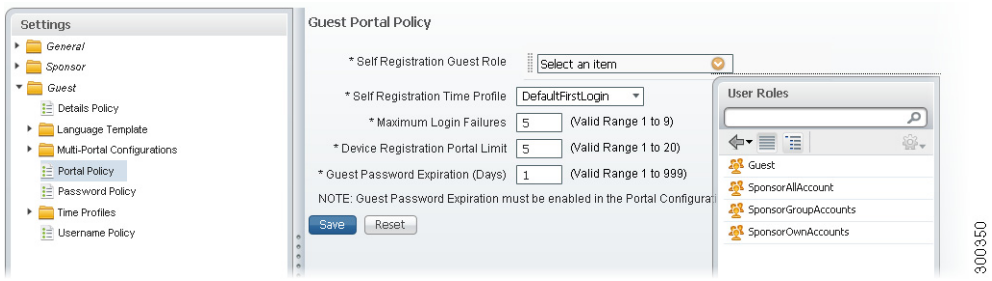
Step 2 In the Settings panel, select **Guest > Portal Policy**.

Step 3 Configure the following options. An example is shown in Figure 21-4.

- **Self Registration Guest Role**—This option is the default guest role assigned to the guest user after self-registration. This role ties the guest user to the associated Identity Group based on the policies defined in the system. For more information on configuring identity groups, see "Configuring User Identity Groups" section on page 4-40.
- **Self Registration Time Profile**—This option is the default time profile assigned to the guest user after self-registration. Only CreateTime and FirstLogin type time profiles are available and both are treated as CreateTime accounts when creating a self-registered guest user account.
- **Maximum Login Failures**—This option is the maximum number of failed login that can occur before a Guest User account is marked as suspended. The default value is five. A user account will be suspended after five failed login attempts. If the user account is suspended, the sponsor will have to re-enable the user account for login. This is a global setting and affects all guest portals.

- **Device Registration Portal Limit**—This option is the maximum number of devices that can be registered for a guest user account. The device registration portal will not allow the guest user to add more devices if the maximum number has been reached. This value can be reduced to a value that is below the maximum number of devices currently registered to a guest account. Lowering the maximum number of registered devices will not affect the existing registered devices and these devices will remain registered.
- **Guest Password Expiration—**This option is the number of days after which the guest password will expire and the guest will have to reset their password. To set this option, Guest Password Expiration must be enabled in the Portal Configuration page.

Figure 21-4 Guest Portal Policy Page



Step 4 Click **Save**.

Related Topics

- Configuring Details Policy, page 21-45
- Multi-Portal Configurations, page 21-49
- Configuring Guest Password Policy, page 21-69
- Time Profiles, page 21-70
- Configuring Guest Username Policy, page 21-73

Configuring Guest Password Policy

The guest password policy determines how the password should be generated for all guest accounts. You can create a password policy based upon a mixture of alphabetic, numeric, or special characters.

To configure a guest password policy, complete the following steps:

Step 1 From the Cisco ISE Administration interface, select **Administration > Guest Management > Settings**.

Step 2 In the Settings panel, select **Guest > Password Policy**.

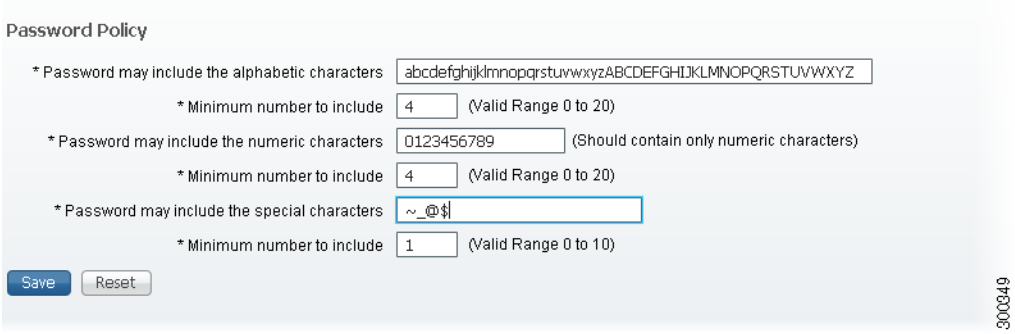
Step 3 Type the characters that will be used to generate the random characters.

Step 4 Enter the minimum number to use from each set of characters.

Step 5 Click **Submit**.

Note Changes to the guest password policy only affect the existing accounts until the guest user passwords have expired and need to be changed.

Figure 21-5 Password Policy Page



Related Topics

- Configuring Details Policy, page 21-45
- Multi-Portal Configurations, page 21-49
- Configuring Guest Portal Policy, page 21-68
- Time Profiles, page 21-70
- Configuring Guest Username Policy, page 21-73

Time Profiles

Time profiles allow a sponsor to assign different levels of access time to a guest account. For example, you can assign a time profile that allows a guest access during a workweek day but not during a weekend day.

After time profiles are created, you must change the sponsor user group to allow sponsors in that group to be able to provision accounts to the appropriate time profiles that are created. You can choose the sponsor user groups that are allowed to assign certain time profiles to guests.

By default, a sponsor user group has the ability to assign guests to the default time profile. Administrators can choose which additional time profiles the sponsor can be assigned, and they can also remove the default time profile from the user group.

Each sponsor user group must have the ability to assign guests to at least one time profile.

If a sponsor user group has only one time profile selected, sponsors will be able to select that time profile alone. If sponsors can choose more than one time profile, they can view a drop-down menu from which they can choose the time profile to be assigned to the account during the account creation.

Related Topics

- Adding, Editing, or Duplicating Time Profiles, page 21-71
- Deleting Time Profiles, page 21-72
- Configuring Details Policy, page 21-45
- Multi-Portal Configurations, page 21-49

- Configuring Guest Portal Policy, page 21-68
- Configuring Guest Password Policy, page 21-69
- Configuring Guest Username Policy, page 21-73

Adding, Editing, or Duplicating Time Profiles

To add or edit a time profile, complete the following steps:

Step 1 From the Cisco ISE Administration interface, select **Administration > Guest Management > Settings**.

Step 2 In the Settings panel, select **Guest > Time Profiles**.

Step 3 Click one of the following:

- **Add**—to create a new time profile
- **Edit**—to edit an existing time profile
- **Duplicate**—to duplicate an existing time profile

Step 4 Enter the name and description of the new time profile.

Step 5 Select a **Time Zone for Restrictions**. Time Restrictions are a set of time periods during which a guest account associated with that time profile would not be granted access to the network or guest portal.

Step 6 From the Account Type drop- down menu, choose one of the predefined options:

- **StartEnd**—allows sponsors to define start and end times for account durations
- **FromFirstLogin**—allows sponsors to define the duration of time that guests can have access after login
- **FromCreation**—allows sponsors to define the duration of time that guest can have access after account creation

Step 7 Set the **Duration** for which the account will be active. The account expires after the duration set here has expired. This option is available only if you select the Account Type as FromFirstLogin or FromCreation.

Step 8 Set the **Restrictions** for the guest access.

These restrictions are composed of a day of the week and a start and end clock time. The Time Zone value specified in the time profile affects the clock times set in any of the Time Restrictions within the time profile. For example, a Time Restriction that specifies Monday 12:00 am to 8:00 am and Monday 6:00 pm to 11:59 pm would only grant system access between 8:00 am and 6:00 pm on Mondays within the time zone of the time profile. Any other day of the week would have no time restriction in this example and system access would be granted at any time.

Step 9 Click **Submit**.

Time profiles do not define the start and end times. This is done during the account creation. The time profile can have restrictions that fall outside the start and end time specified in a Guest account while creation. Only those restrictions that cover the start end time of the account will be applied to the account.

For a wired network the **Termination-Action** must be set to 0 “Default” so that the Session-Timeout is treated as a terminate session. This value must be set on the Authorization Profile as a RADIUS value.

For a WLC the **Allow AAA Override** must be turned on in the WLAN configuration. The RADIUS access-accept will contain a Session-Timeout value in seconds, remaining for the account. When this time has elapsed, NAD will close the connection.

At the time of Guest login the Network Access system will return the remaining time left in the guest account to the NAD that is making the access request. This is so that the NAD can enforce account expiration.

Note For the FromCreation and FromFirstLogin time profiles, the expiration date will be calculated based on the sponsor group duration or time profile duration, whichever is minimum.

Related Topics

- Time Profiles, page 21-70
- Deleting Time Profiles, page 21-72
- Configuring Details Policy, page 21-45
- Multi-Portal Configurations, page 21-49
- Configuring Guest Portal Policy, page 21-68
- Configuring Guest Password Policy, page 21-69
- Configuring Guest Username Policy, page 21-73

Deleting Time Profiles

To delete time profiles, complete these steps:

Step 1 From the Cisco ISE Administration interface, select **Administration > Guest Management > Settings > Guest > Time Profiles**.

Step 2 Select the time profiles to be deleted.

Step 3 Click **Delete**.

Related Topics

- Time Profiles, page 21-70
- Adding, Editing, or Duplicating Time Profiles, page 21-71
- Configuring Details Policy, page 21-45
- Multi-Portal Configurations, page 21-49
- Configuring Guest Portal Policy, page 21-68
- Configuring Guest Password Policy, page 21-69
- Configuring Guest Username Policy, page 21-73

Configuring Guest Username Policy

The Guest Username Policy Configuration page allows the Cisco ISE administrator to specify how the user names will be created for the guest accounts. Username policy configuration can be done in two ways:

- General
- Random

Configuring General Guest Username Policy

You can create a guest username based on the email address or the first and last name of the guest.

To configure general guest username policy, complete the following steps:

Step 1 From the Cisco ISE Administration interface, select **Administration > Guest Management > Settings > Guest > Username Policy**.

Step 2 If necessary, expand the **General** tab.

Step 3 Choose one of the username policy options for creating the username for the guest account:

c. **Create username from email address**—Select this option if you want the guest username to be formed from the guest's email address.

d. **Create username from the first name and last name**—Select this option if you want the guest username to be formed from the first initial of the first name combined with the last name of the guest user.

Step 4 Enter the **Minimum Username length** for the guest user names. Valid range is 1-20.

If the guest user names formed by the email address or by the combination of first and last name are shorter than the minimum length, the username will be appended with *0* (zero) characters and a *1* at the end. If the username is not unique, numeric characters are appended to the name to make it unique.

For example, if there are two guest users named *John Smith*, the first username would be *jsmith* and the second username would be *jsmith1*. Similarly, if the Minimum Username length is set to eight, then the two user names would be generated as *jsmith01* and *jsmith02*.

Step 5 Click **Submit**.

Configuring Random Guest Username Policy

You can create a guest usernames based upon a random mixture of alphabetic, numeric or special characters. The random guest username policy is used when the sponsor creates random accounts.

To configure a random guest username policy, complete the following steps:

Step 1 From the Cisco ISE Administration interface, select **Administration > Guest Management > Settings > Guest > Username Policy**.

Step 2 If necessary, expand the **Random** tab.

Step 3 Type the characters that will be used to generate the random characters.

Step 4 Enter the minimum number to use from each set of characters. Valid range is 0-20 for each character set.

Step 5 Click **Submit**.

Random username length is the combination of the three length fields that is alphabetic, numeric and special other characters. The length of the username defines the total number of unique names that can be created. For example, if 10,000 users are to be created, you will not be able to create enough unique values with a name space that is two characters in length.

Note Changes to the guest username policy do not affect the existing accounts.

Related Topics

- Configuring Details Policy, page 21-45
- Multi-Portal Configurations, page 21-49
- Configuring Guest Portal Policy, page 21-68
- Configuring Guest Password Policy, page 21-69
- Time Profiles, page 21-70

Monitoring Sponsor and Guest Activity

Cisco ISE provides the following ways to view and monitor sponsor and guest activities:

- Metric Meter, page 21-74
- Guest Activity Report, page 21-74
- Guest Accounting, page 21-75
- Guest Sponsor Summary, page 21-75

Metric Meter

Cisco ISE provides an at-a-glance view of active guests in the network in a metric meter that appears on the Cisco ISE dashboard.

Guest Activity Report

This report helps you to view the Guest information for a selected time period. This report displays all the URLs that a guest user visits.

Note For the Guest Activity Report to collect and display the list of URLs visited by the guest user, you must enable guest access syslog configuration on the NAD that inspects guest traffic in your ISE network.

To view this report,

1. Go to **Operations > Reports > Catalog > User**.
2. Click on **Guest Activity**.

Guest Accounting

This report helps you to view the logged in/out information for the particular guest for a selected time period.

To view this report,

1. Go to **Operations > Reports > Catalog > User**.
2. Click on **Guest Accounting**.

Guest Sponsor Summary

This report helps you to view the sponsor information along with a graphical representation for a selected time period.

To view this report,

1. Go to **Operations > Reports > Catalog > User**.
2. Click on **Guest Sponsor Summary**.

For More Information

See Chapter 24, "Reporting," for details on how to configure these reports.

See Chapter 23, "Monitoring and Troubleshooting," for details on monitoring and troubleshooting tools.

Audit Logging

During specific actions within the Guest and Sponsor portals, audit log messages are sent to the underlying audit system. By default, these messages appear in the **/opt/CSCOcpm/logs/localStore/iseLocalStore.log** file.

You can configure these messages to be sent by syslog to the Monitoring and Troubleshooting system and log collector. The monitoring subsystem presents the Sponsor and Guest activity logs.

See Chapter 23, "Monitoring and Troubleshooting," for more information on logging and log collection.

Guest login flow gets logged in the audit logs regardless whether the guest login has passed or failed.



CHAPTER 22

Configuring Cisco Security Group Access Policies

This chapter describes how to configure a Cisco Identity Services Engine (ISE) node as an authentication server, using Cisco security group access policies (SGA). This requires a Cisco SGA solution enabled network.

This chapter covers the following topics:

- Understanding the SGA Architecture, page 22-1
  - SGA Features and Terminology, page 22-2
  - SGA Requirements, page 22-4
- Configuring ISE to Enable the SGA Solution, page 22-5
  - Configuring SGA Settings on the Switches, page 22-6
  - Configuring SGA Devices, page 22-6
  - Configuring Security Group Access Settings, page 22-8
  - Configuring Security Groups, page 22-10
  - Configuring Security Group Access Control Lists, page 22-12
  - Mapping Security Groups to Devices, page 22-14
  - Configuring SGA Policy by Assigning SGTs to Devices, page 22-16
- Assigning Security Groups to Users and End Points, page 22-17
- Egress Policy, page 22-18
- OOB SGA PAC, page 22-31
- SGA CoA, page 22-34

Understanding the SGA Architecture

The Cisco Security Group Access (SGA) solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco SGA cloud is authenticated by its neighbors (peers). Communication between the devices in the SGA cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. The SGA solution uses the device and user identity information that it obtains during authentication to classify, or color, the packets as they enter the network. This packet classification is maintained by tagging packets when they enter

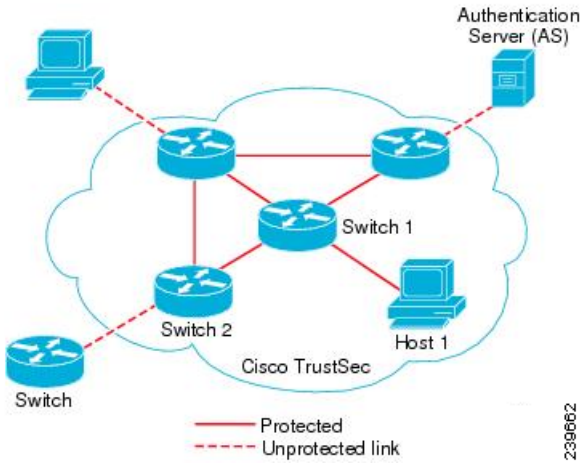
the SGA network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

Note You need an Advanced License Package for ISE to enable SGA services.

For more information on the SGA solution, see http://www.cisco.com/en/US/netsol/ns1051/index.html.

Figure 22-1 shows an example of an SGA network cloud.

Figure 22-1 SGA Architecture



SGA Features and Terminology

The key features of the SGA solution include:

- Network Device Admission Control (NDAC)—In a trusted network, during authentication, each network device (for example ethernet switch) in an SGA cloud is verified for its credential and trustworthiness by its peer device. NDAC uses the IEEE 802.1x port-based authentication and uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as its Extensible Authentication Protocol (EAP) method. Successful authentication and authorization in the NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
- Endpoint Admission Control (EAC)—An authentication process for an endpoint user or a device connecting to the SGA cloud. EAC typically happens at the access level switch. Successful authentication and authorization in EAC process results in SGT assignment to the user or device. EAC access methods for authentication and authorization includes:
  - 802.1X port-based authentication
  - MAC authentication bypass (MAB)
  - Web authentication (WebAuth)
- Security Group (SG)—A grouping of users, endpoint devices, and resources that share access control policies. SGs are defined by the administrator in Cisco ISE. As new users and devices are added to the SGA domain, Cisco ISE assigns these new entities to the appropriate security groups.

- Security Group Tag (SGT)—SGA service assigns to each security group a unique 16-bit security group number whose scope is global within an SGA domain. The number of security groups in the switch is limited to the number of authenticated network entities. You do not have to manually configure security group numbers. They are automatically generated, but you have the option to reserve a range of SGTs for IP-to-SGT mapping.
- Security Group Access Control List (SGACL)—SGACLs allow you to control the access and permissions based on the SGTs that are assigned. The grouping of permissions into a role simplifies the management of security policy. As you add devices, you simply assign one or more security groups, and they immediately receive the appropriate permissions. You can modify the security groups to introduce new privileges or restrict current permissions.
- Security Exchange Protocol (SXP)—SGT Exchange Protocol (SXP) is a protocol developed for SGA service to propagate the IP-to-SGT binding table across network devices that do not have SGT-capable hardware support to hardware that supports SGT/SGACL.
- Environment Data Download—The SGA device obtains its environment data from Cisco ISE when it first joins a trusted network. You can also manually configure some of the data on the device. The device must refresh the environment data before it expires. The SGA device obtains the following environment data from Cisco ISE:
  - Server lists—List of servers that the client can use for future RADIUS requests (for both authentication and authorization)
  - Device SG—Security group to which the device itself belongs
  - Expiry timeout—Interval that controls how often the SGA device should download or refresh its environment data
- SGT Reservation—An enhancement in ISE to reserve a range of SGTs to enable IP to SGT mapping.
- IP-to-SGT Mapping—An enhancement in ISE to bind an endpoint IP to an SGT and provision it to an SGA-capable device.
- Identity-to-Port Mapping—A method for a switch to define the identity on a port to which an endpoint is connected, and to use this identity to look up a particular SGT value in the Cisco ISE server.

Table 22-1 lists some of the common terms that are used in the SGA solution and their meaning in an SGA environment.

Table 22-1 SGA Terminology

Term	Meaning
Supplicant	A device that tries to join a trusted network.
Authentication	The process of verifying the identity of each device before allowing it to be part of the trusted network.
Authorization	The process of deciding the level of access to a device that requests access to a resource on a trusted network based on the authenticated identity of the device.
Access control	The process of applying access control on a per-packet basis based on the SGT that is assigned to each packet.
Secure communication	The process of encryption, integrity, and data-path replay protection for securing the packets that flow over each link in a trusted network.
SGA device	Any of the Cisco Catalyst 6000 Series or Cisco Nexus 7000 Series switches that support the SGA solution.

Table 22-1 SGA Terminology (continued)

Term	Meaning
SGA-capable device	An SGA-capable device will have SGA-capable hardware and software. For example, the Nexus 7000 Series Switches with the Nexus operating system.
SGA seed device	The SGA device that authenticates directly against the ISE server. It acts as both the authenticator and supplicant.
Ingress	When packets first encounter an SGA-capable device that is part of a network where the Cisco SGA solution is enabled, they are tagged with an SGT. This point of entry into the trusted network is called the ingress.
Egress	When packets pass the last SGA-capable device that is part of a network where the Cisco SGA solution is enabled, they are untagged. This point of exit from the trusted network is called the egress.

SGA Requirements

To set up a Cisco ISE network that is enabled with the Cisco SGA solution, you need switches that support the SGA solution and other components. Table 22-2 lists the supported Cisco switch platforms.

Table 22-2 SGA Requirements

Supported Cisco Switch Platforms		
Platform	**Operating System Version**	**Requirement**
Cisco Nexus 7000 Series	Cisco Nexus operating system 5.0.2a. **Note** You would need Advanced Service Package license for Cisco SGA.	Mandatory as enforcement point
Cisco Catalyst 6500E Switch with Supervisor Engine 32 or 720 or Virtual Switching System (VSS) 720	Cisco IOS Software 12.2(33) SXI3 or later	Optional as an access switch
Cisco Catalyst 4900 Series Switch	Cisco IOS Software 12.2(50) SG7 or later	Optional as an access switch
Cisco Catalyst 4500E Switch with Supervisor 6L-E or 6-E	Cisco IOS Software 12.2(50) SG7 or later	Optional as an access switch
Cisco Catalyst 3750-X or 3560-X Series Switches	Cisco IOS Software 12.2(53) SE1 or later	Optional as an access switch
Cisco Catalyst 3750 or 3560 Series Switches	Cisco IOS Software 12.2(53) SE1 or later	Optional as an access switch
Cisco Catalyst Blade Switch 3000 or 3100 Series	Cisco IOS Software 12.2(53) SE1 or later	Optional as an access switch

Apart from the switches listed in Table 22-2 above, you need other components for identity-based user access control using the IEEE 802.1X protocol. These include Microsoft Windows 2003 or 2008 Server running Microsoft Active Directory, Certificate Authority (CA) server, Domain Name System (DNS)

server, and Dynamic Host Configuration Protocol (DHCP) server. An end host running the Microsoft Windows operating system can also be a part of this environment. Table 22-3 lists other components that may be required for your Cisco SGA environment.

Table 22-3 Other Components

Component	Description
User Identity Repository	Although you can use the ISE internal user database, we recommend that you use an external database for identity authentication. ISE supports connections to Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) service
DHCP Service	Any DHCP server that provides DHCP service. For example, Microsoft Windows Server 2008 DHCP server
DNS Service	Any DNS server that provides DNS service. For example, Microsoft Windows Server 2008 DNS server
Certificate Authority Server	Any Certificate Authority server that provides standalone CA service. For example, Microsoft Windows Server 2008 CA server
Target Servers	Servers that provide Internet services such as HTTP, FTP, Secure Shell (SSH), and even file sharing to test the SGACLs
Endpoint PC	SGA is a supplicant-agnostic solution and does not require any specific agent or IEEE 802.1X supplicant running on the endpoint PC. You can use the Cisco Secure Services Client supplicant, Microsoft Windows or another operating system-embedded supplicant, or other third-party supplicant

To enable Cisco ISE to interoperate with SGA deployments, you must configure SGA switch ports on your switches. See "Enable Cisco Security Group Access Switch Ports" section on page C-6 for more information.

Configuring ISE to Enable the SGA Solution

This section describes the tasks that you must perform to enable the SGA solution in your Cisco ISE network.

Note To enable the SGA solution, you need an advanced ISE license. For more information on licensing, see Chapter 12, "Managing Licenses."

This section covers the following tasks:

- Configuring SGA Settings on the Switches, page 22-6
- Configuring SGA Devices, page 22-6
- Configuring Security Group Access Settings, page 22-8
- Configuring Security Group Access AAA Servers, page 22-9
- Configuring Security Groups, page 22-10
- Configuring Security Group Access Control Lists, page 22-12
- Mapping Security Groups to Devices, page 22-14
- Configuring SGA Policy by Assigning SGTs to Devices, page 22-16

Configuring SGA Settings on the Switches

To enable Cisco ISE to interoperate with SGA deployments, you must configure SGA switch ports on your switches. See "Enable Cisco Security Group Access Switch Ports" section on page C-6 for more information.

In addition to configuring SGA settings on Cisco ISE, you must also configure some settings on the SGA devices. These configurations vary for the Catalyst and Nexus switches and are described in the Catalyst and Nexus switch configuration guides that are available at:

- For Catalyst 6500 Series Switches:
  http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html
- For Nexus 7000 Series Switches:

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_5.x.html
- Configuration Example Using Nexus 7000 Series Switches:

  http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/configuration_examples/configuration/guide/Cisco_Nexus_7000_Series_NX-OS_Configuration_Examples_Release_5.x_chapter4.html#con_1191129

Configuring SGA Devices

For Cisco ISE to process requests from SGA-enabled devices, you must define these SGA-enabled devices in Cisco ISE. This section describes how to define SGA-enabled devices in Cisco ISE.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure an SGA device, complete the following steps:

Step 1 Follow the instructions in the "Adding and Editing Devices" section on page 6-3 to add a network device. Table 22-4 describes the SGA-specific settings.

Step 2 Click **Submit** to save the SGA device definition.

Next Step:

Configuring Security Group Access Settings, page 22-8

Network Devices: SGA Attributes

Table 22-4 lists the SGA-specific fields in the Network Devices page and their descriptions.

Table 22-4 Network Devices: SGA Attributes

Field	Description
SGA Attributes	(Required) Check this check box to configure settings that are specific to the SGA solution. SGA devices use these settings to communicate with ISE.
SGA Notifications and Updates	
Use Device ID for SGA Identification	Check this check box if you want the Device Name to be listed as the device identifier in the Device ID field.
Device Id	(Required) Used for identifying the SGA device. By default, this field is empty. If you check the Use Device ID for SGA Identification check box, then the Device Name appears in this field. You can change this ID to a descriptive name of your choice.
Password	(Required) Password to authenticate the SGA device (same password that you have configured on the SGA device command-line interface [CLI]).
Download Environment Data Every	(Required) Specifies the expiry time for environment data. The SGA device downloads its environment information from ISE. You can configure the time interval in seconds, minutes, hours, or days between these downloads. For example, if you enter 60 sec, the device would download its environment data from ISE every minute. The default value is 86,400 seconds or 1 day. Valid range is from 1 to 24850.
Download Peer Authorization Policy Every	(Required) Specifies the expiry time for the peer authorization policy. The SGA device downloads its peer authorization policy from ISE. You can configure the time interval in seconds, minutes, hours, or days between these downloads. For example, if you enter 60 sec, the device would download its peer authorization policy from ISE every minute. The default value is 86,400 seconds or 1 day. Valid range is from 1 to 24850.
Reauthentication Every	(Required) Specifies the 802.1X reauthentication period. In a network that is configured with the SGA solution, after initial authentication, the SGA device reauthenticates itself against ISE. You can configure the time interval in seconds, minutes, hours, or days between these authentications. For example, if you enter 1000 sec, the device would authenticate itself against ISE every 1000 sec. The default value is 86,400 seconds or 1 day. Valid range is from 1 to 24850.
Download SGACL Lists Every	(Required) Specifies the expiry time for SGACL lists. The SGA device downloads the SGACLs from ISE. You can configure the time interval between these downloads. For example, if you enter 3600 sec, the device obtains the SGACL lists from ISE every 3600 sec. The default value is 86,400 seconds or 1 day. Valid range is from 1 to 24850.
Other SGA Devices to Trust This Device (SGA Trusted)	Check this check box if you want all the peer devices to trust this device. If you uncheck this device, the peer devices do not trust it, and all packets that arrive from this device will be colored or tagged accordingly. This option is enabled by default.
Include This Device When Deploying Security Group Tag Mapping Updates	Check this check box if you want this SGA device to obtain the IP-SGT mappings using the Device Configuration credentials.

Table 22-4 Network Devices: SGA Attributes (continued)

Field	Description
Notify this device about SGA configuration changes	Check this check box if you want ISE to send SGA CoA notifications to this SGA device. This option is enabled by default.
Out of Band (OOB) SGA PAC	
Issuing Date[1]	Holds the issuing date of the last SGA PAC that has been generated by ISE for this device.
Expiration Date[1]	Holds the expiration date of the last SGA PAC that has been generated by ISE for this device.
Issued By[1]	Holds the name of the issuer (an SGA administrator) of the last SGA PAC that has been generated by ISE for this device.

1. This field is read only and is always disabled, and empty by default.It is automatically populated with the issuing date, expiration date or issuer of the last SGA PAC that has been generated for this device in ISE. See SGA PAC Provisioning, page 22-31 for details on how to generate SGA PAC.

Configuring Security Group Access Settings

For ISE to function as an SGA server and provide SGA services, you must define some global SGA settings. This section describes how to complete this task.

Prerequisites:

- Before you configure global SGA settings, ensure that you have defined global EAP-FAST settings (choose **Administration > System > Global Options > Protocol Settings > EAP-FAST > EAP-FAST Settings**).

  You must change the Authority Identity Info Description to your Cisco ISE server name. This description is a user-friendly string that describes the ISE server that sends credentials to an endpoint client. The client in a Cisco SGA architecture can be either the endpoint running EAP-FAST as its EAP method for IEEE 802.1X authentication or the supplicant network device performing NDAC. The client can discover this string in the protected access credentials (PAC) type-length-value (TLV) information. The default value is Cisco Identity Services Engine. You should change the value so that the ISE PAC information can be uniquely identified on network devices upon NDAC authentication.

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure general SGA settings, complete the following steps:

Step 1 Choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **Security Group Access**.

The Security Group Access page appears.

Step 3 Enter the values as described:

- Tunnel PAC Time to Live—Specifies the expiry time for the PAC. The tunnel PAC generates a tunnel for the EAP-FAST protocol. You can specify the time in seconds, minutes, hours, days, or weeks. The default value is 90 days. Valid ranges are:
  - 1 to 157680000 seconds
  - 1 to 2628000 minutes
  - 1 to 43800 hours
  - 1 to 1825 days
  - 1 to 260 weeks
- Proactive PAC Update Will Occur After—The proactive PAC update time is configured in this field. ISE proactively provides a new PAC to the client after successful authentication when a configured percentage of the Tunnel PAC TTL remains. The tunnel PAC update is initiated by the server after the first successful authentication that is performed before the PAC expiration. This mechanism allows the client to be always updated with a valid PAC. The default value is 10%. Valid range is from 1 to 100.
- All Tags Automatically Generated by System—Choose this option if you want all the SGTs to be automatically generated by Cisco ISE. See the "Mapping Security Groups to Devices" section on page 22-14 for more information.

Note Cisco recommends that you use this option only if you plan to manually configure specific security groups and policies on the SGA device.

- Reserve a Range—Choose this option if you want to reserve a range of security group tags (SGTs) to be configured on the device manually. If you choose this option, you must also specify a range from 1 to 65535.

  Cisco ISE creates an SGT by default: Unknown, which has takes the value of 0.

Note If you configure a range of SGTs, Cisco ISE will not use the values in this range while generating SGT values.

Step 4 Click **Save** to save the general SGA settings.

Next Step:

Configuring Security Group Access AAA Servers, page 22-9

Configuring Security Group Access AAA Servers

You can configure a list of Cisco ISE servers in your deployment in the AAA server list to allow SGA devices to be authenticated against any of these servers. When you add ISE servers to this list, all these server details are downloaded to the SGA device. When an SGA device tries to authenticate, it would choose any ISE server from this list and, if the first server is down or busy, the SGA device can authenticate itself against any of the other servers from this list. By default, the primary ISE server is an SGA AAA server. We recommend that you configure additional ISE servers in this AAA server list (**Administration > Network Resources > SGA AAA Servers**) so that if one server is busy, another server from this list can handle the SGA request.

This page lists the ISE servers in your deployment that you have configured as your SGA AAA servers.

You can click the **Push** button to initiate an environment CoA notification after you configure multiple SGA AAA servers. This environment CoA notification goes to all SGA network devices and provides an update of all SGA AAA servers that were changed.

Related Topics

Adding and Editing Security Group Access AAA Servers

Adding and Editing Security Group Access AAA Servers

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To add or edit the AAA server list, complete the following steps:

Step 1 Choose **Administration > Network Resources > SGA AAA Servers**.

The AAA Servers page appears.

Step 2 Do one of the following:

- Click **Add** to add an ISE server to this list.
- Check the check box next to the ISE server that you want to edit, and then click **Edit**.

Step 3 Enter the values as described:

- Name—(Required) Name that you want to assign to the ISE server in this AAA Server list. This name can be different from the hostname of the ISE server.
- Description—An optional description.
- IP—(Required) IP address of the ISE server that you are adding to the AAA Server list.
- Port—(Required) Port over which communication between the SGA device and server should take place. The default is 1812.

Step 4 Click **Submit** to save the changes.

Next Step:

Configuring Security Groups, page 22-10

Configuring Security Groups

A security Group (SG) or Security Group Tag (SGT) is an element that is used in SGA policy configuration. SGTs are attached to packets when they move within a trusted network. These packets are tagged when they enter a trusted network (ingress) and untagged when they leave the trusted network (egress).

SGTs are automatically generated in a sequential manner, but you have the option to reserve a range of SGTs for IP to SGT mapping. ISE skips the reserved numbers while generating SGTs.

If you have deleted a particular security group, the SGT assigned to this security group does not get reused until all the succeeding SGTs are deleted.

For example, if you have SGTs 2, 3, and 4 defined and you delete SGT 2, the next SGT that is generated would be SGT 5. If you want SGT 2 to be generated next, you must delete SGTs 3 and 4.

SGA service uses these SGTs to enforce the SGA policy at egress. See the "Configuring SGA Policy by Assigning SGTs to Devices" section on page 22-16.

You can configure security groups from the following ISE administrative user interfaces:

- **Policy > Policy Elements > Results > Security Group Access > Security Groups**. See the "Adding and Editing Security Groups" section on page 22-11 for more information.
- Directly from egress policy page. See Configuring SGT and SGACL from Egress Policy, page 22-27 to configure SGT from egress policy page.
- Clicking the **Generate SGTs** button on the **Policy > Policy Elements > Results > Security Group Access > Security Groups** page. See the "Adding and Editing Security Groups" section on page 22-11 for more information.

You can click the **Push** button to initiate an environment CoA notification after updating multiple SGTs. This environment CoA notification goes to all SGA network devices and provides an update of all SGTs that were changed.

Related Topics

Adding and Editing Security Groups

Adding and Editing Security Groups

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To add or edit a security group, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane on the left, click the **>** button next to Security Group Access and click **Security Groups**.

The Security Groups page appears. There is a default security group in ISE: Unknown. This page provides the name, the SGT in decimal and hexadecimal formats, and an optional description of the security groups.

Step 3 Click **Generate SGTs**.

Step 4 Do one of the following:

- Click **Add** to add a new security group.
- From the navigation pane, click the expand button next to Security Groups and select the security group that you want to edit, or check the check box next to the security group in the list page that you want to edit, and click **Edit**.

Note You cannot edit the predefined unknown security group.

Step 5 Enter the values as described:

- Name—Name of the security group.
- Description—An optional description of the security group.
- Allow System to Automatically Generate Tag—(Visible only if you have chosen the Reserve a Range option in the Security Group Access Settings page) Choose this option if you want ISE to generate an SGT automatically. The tag value will be automatically populated if you choose this option. This option will be visible only if you reserve a range of SGTs while configuring the Global SGA settings. See the "Configuring Security Group Access Settings" section on page 22-8 for more information.
- Select Value from Reserved Range—(Visible only if you have chosen the Reserve a Range option in the Security Group Access Settings page) Choose this option if you want to assign an SGT from the reserved range to a specific IP address. This option will be visible only if you reserve a range of SGTs while configuring the Global SGA settings. See the "Configuring Security Group Access Settings" section on page 22-8 for more information.
- Security Group Tag (Dec/Hex)—ISE assigns this value automatically. This value is sequentially numbered from 0 to 65,535. You can reserve a range of tags for specific security groups and ensure that these numbers are not automatically generated. See the "Configuring Security Group Access Settings" section on page 22-8 for more information.

Step 6 Click **Submit** to save the security group.

Note Each security group in your SGA solution should be assigned a unique SGT. Even though ISE supports 65,535 SGTs, having fewer number of SGTs would enable you to deploy and manage the SGA solution easily. We recommend a maximum of 64000 SGTs.

Next Steps:

- Configuring Security Group Access Control Lists, page 22-12
- Assigning Security Groups to Users and End Points, page 22-17

Configuring Security Group Access Control Lists

Security group access control lists (SGACLs) are permissions that will be assigned after the SGA policy evaluation. SGACLs restrict the operations that a user can perform based on the role of the user instead of the IP address or subnet mask alone. You can configure SGACLs from the ISE administrative user interface (**Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**). You can also configure the security groups ACLs directly from the egress policy page. See Configuring SGT and SGACL from Egress Policy, page 22-27 to configure SGACLs from the egress policy page.

You can click the **Push** button to initiate an environment CoA notification after updating multiple SGACLs. This environment CoA notification goes to all SGA network devices and provides an update of all SGACLs that were changed.

See "Adding and Editing Security Group Access Control Lists" section on page 22-13 for more information.

Adding and Editing Security Group Access Control Lists

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create or edit an SGACL, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane on the left, click the **>** button next to Security Group Access and click **Security Group ACLs**.

The Security Group ACLs page appears with a list of SGACLs and provides the following information:

- Name—Name of the SGACL
- Description—An optional description of the SGACL
- IP Version—IP version that this SGACL supports:
  - IPv4—Supports IP version 4 (IPv4)
  - IPv6—Supports IP version 6 (IPv6)
  - Agnostic—Supports both IPv4 and IPv6

Step 3 Do one of the following:

- Click **Add** to add an SGACL.
- Check the check box next to the SGACL that you want to edit, and then click **Edit** or select the SGACL from the Security Group ACLs object selector.

Step 4 Enter the values as described:

- Name—(Required) Name of the SGACL.
- Description—An optional description of the SGACL.
- IP Version—Specifies which IP version this SGACL supports.
  - IPv4—Supports IPv4
  - IPv6—Supports IPv6
  - Agnostic—Supports both IPv4 and IPv6
- Security Group ACL Content—(Required) Access control list (ACL) commands. For example:

  permit icmp

  deny all

Step 5 Click **Submit** to save the SGACL.

The Nexus 7000 Series with Cisco Nexus operating system 4.2 supports the following access control list entries:

deny all

deny icmp

deny igmp

deny ip

deny tcp [{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

deny udp[{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

permit all

permit icmp

permit igmp

permit ip

permit tcp [{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

permit udp[{***dest*** | ***src***} {{***eq*** | ***gt*** | ***lt*** | ***neq***} port-number | **range** *port-number1 port-number2*}]

For more information on syntax and usage, go to:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/command/reference/sec_cmds_d.html#wp1057446

When you change SGACL ACE, SGACL name, or IP version of an SGACL, all the accumulative changes can be pushed to the SGA network devices by clicking the **Push** button. See Update RBACL Named List CoA, page 22-37 for more details.

Next Step:

Configuring SGA Policy by Assigning SGTs to Devices, page 22-16

Mapping Security Groups to Devices

Cisco ISE allows you to assign an SGT to an SGA device if you know the device hostname or IP address. When a device with the specific hostname or IP address joins the network, ISE will assign the SGT before authenticating it. You can create this mapping from the Security Group Mappings page. Before you perform this action, ensure that you have reserved a range of SGTs. See Reserve a Range option for more information. You can map the security groups to devices from the ISE administrative user interface (**Policy > Policy Elements > Results > Security Group Access > Security Group Mappings**). This page lists the security group mappings that you have configured.

See "Adding and Editing Security Group Mappings" section on page 22-14 for more information.

Adding and Editing Security Group Mappings

Cisco ISE allows you to add and edit security group mappings from the Cisco ISE user interface. This section describes how to complete this task.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create or edit a security group mapping, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane on the left, click the **>** button next to Security Group Access and click **Security Group Mappings**.

The Security Group Mappings page appears.

Step 3 Do one of the following:

- Click **Add** to add a new security group mapping.
- Check the check box next to an existing security group mapping that you want to edit, and then click **Edit**.
- Check the check box next to an existing security group mapping that you want to reassign, and then click **Reassign Groups**. See the "Reassigning SGTs to Devices" section on page 22-15 for more information.
- Check the check box next to an existing security group mapping that you want to deploy, and then click **Deploy**. See the "Deploying SGTs on SGA Devices" section on page 22-15 for more information.
- Check the check box next to an existing security group mapping whose status you want to check, then choose **>>** and click **Check Status**. See the "Checking the Status of Security Group Mapping on Devices" section on page 22-15 for more information.

Step 4 Enter the values as described in Table 22-5.

Table 22-5 Security Group to Host Mappings

Field	Description
Security Group	Click **Select** to choose an SGT to be applied to this device.
Hostname	Enter the hostname of the SGA device.
IP Address	Enter the IP address of the SGA device.

Step 5 Click **Submit** to save the settings.

Step 6 Click the **Security Group Mapping List** link at the top of this screen to go back to the list page.

You can also set filters to view only certain records. You can set a Quick Filter based on a simple condition or an Advanced Filter for an enhanced search. You can also save the advanced custom view.

Deploying SGTs on SGA Devices

You can check the check box next to the security group mapping and click **Deploy** to download the SGT to the SGA device. This option connects to the device through SSH and runs the command to download the SGT on the device. Click **OK** to close this page.

Checking the Status of Security Group Mapping on Devices

You can check the check box next to the security group mapping and click **Check Status** to see if the SGTs have been downloaded on the device. This option allows you to check the status on the SGA device. Click **OK** to close this page.

Reassigning SGTs to Devices

You can check the check box next to the security group mappings and click **Reassign Groups** to assign a different SGT to a set of devices. The Reassign Security Groups page appears:

1. Click **Select** to select the new SGT.

2. Click **OK** to save the changes.

Note You can use the Edit option to edit the SGT mapping for a single device. To change the SGT mapping for multiple devices at the same time, you can use the Reassign Groups option.

Configuring SGA Policy by Assigning SGTs to Devices

Cisco ISE allows you to configure the SGA policy by assigning SGTs to devices. This section describes how to complete this task.

Prerequisites:

- Before you configure an SGA policy, you must create the security groups for use in the policy. See the "Configuring Security Groups" section on page 22-10 for more information.

  You can assign security groups to devices by using the SGA device ID.

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure an SGA policy, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Network Device Authorization**.

The Network Device Authorization page appears. You can define an SGA device policy on this page based on conditions. Cisco ISE supports device attributes for use in policy conditions:

Step 2 Click the action icon in the Default Rule row and click **Insert New Row Above**.

Step 3 Click the drop-down list box to select the status of this rule. The Status can be any one of the following:

- Enable—The policy rule is active.
- Disable—The policy rule is inactive and will not be evaluated.
- Monitor—The policy rule will be evaluated, but the result will not be enforced. You can use this option for testing purposes. You can view the results of this policy condition in the monitoring and report viewer. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in the monitored mode to view the results and then enable it if you are satisfied with the results.

Step 4 Enter the name for this rule in the first text box.

Step 5 Click the plus sign (+) next to Conditions to add a policy condition.

Step 6 Click **Create New Condition (Advance Option)**.

a. From the Expression drop-down list box, choose any one of the following attributes to define the policy condition. For example, Device Type:

- SGAdeviceID
- Device Type
- Location

- Model Name
- Software Version

b. Select the operator from the drop-down list box. You can select EQUALS (is equal to), NOT EQUALS (is not equal to), or MATCHES (is an exact match of).

c. Enter a value for the attribute. For example Nexus 7K.

You can create a compound condition by adding more conditions using the AND or OR operator.

d. To create a compound condition, from within the Conditions popup, click the action icon that appears in the same row as the condition that you have already created, and click **Add Attribute/Value** to add a new row. Repeat the process as described in Step 5a.

Note While creating a compound condition, you can only use AND or OR operator throughout. You cannot use both AND and OR operators in the same compound condition.

For example, you can create a compound condition that checks for all devices in New York and are of the Catalyst 6K model. Your compound condition would appear as follows:

DEVICE:Location EQUALS All Locations:New York

AND

DEVICE:Model Name EQUALS Catalyst 6K

Step 7 Click the minus sign (-) in the popup to close it.

Step 8 From the Security Group drop-down list, select the SGT that you want to assign if this condition evaluates to true.

Step 9 Click the action icon from this row to add additional rules based on device attributes either above or below the current rule. You can repeat this process to create all the rules that you need for the SGA policy. You can drag and drop the rules to reorder them by clicking the icon. You can also duplicate an existing condition, but ensure that you change the policy name.

The first rule that evaluates to true determines the result of the evaluation. If none of the rules match, the default rule will be applied; you can edit the default rule to specify the SGT that must be applied to the device if none of the rules match.

Step 10 Click **Save** to save your SGA policy.

If an SGA device tries to authenticate after you have configured the network device policy, the device will get its SGT and the SGT of its peers and will be able to download all the relevant details.

Assigning Security Groups to Users and End Points

ISE allows you to assign a security group as the result of an authorization policy evaluation. Using this option, you can assign a security group to users and end points.

Prerequisites:

- Read the "Understanding Authorization Policies" section on page 17-1 for information on authorization policies.

- Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To assign security groups to users and endpoints, complete the following steps:

Step 1 Create a new authorization policy as described in "Creating a New Authorization Policy" section on page 17-14.

Step 2 For Permissions, instead of selecting an authorization profile, select a security group.

If the conditions specified in this authorization policy is true for a user or endpoint, then this security group will be assigned to that user or endpoint and all data packets that are sent by this user or endpoint will be tagged with this particular SGT.

Egress Policy

The egress table lists the source and destination SGTs, both reserved and unreserved. This page also allows you to filter the egress table to view specific policies and also to save custom views. When the source SGT tries to reach the destination SGT, the SGA-capable device enforces the SGACLs based on the SGA policy as defined in the Egress Policy. ISE creates and provisions the policy.

After you create the SGTs and SGACLs, which are the basic building blocks required to create an SGA policy, you can establish a relationship between them by assigning SGACLs to source and destination SGTs.

Each combination of a source SGT to a destination SGT is a cell in the egress policy.

Tip Before you create the SGA policy, you can configure security groups and SGACLs. See the "Configuring Security Groups" section on page 22-10 and the "Configuring Security Group Access Control Lists" section on page 22-12 for more information.

This section contains the following:

- Viewing the Egress Policy, page 22-19
- Matrix Operations, page 22-22
- Sorting and Filtering Egress Policy Table, page 22-22
- Configuring Egress Policy Table Cells, page 22-25
- Configuring SGT and SGACL from Egress Policy, page 22-27
- The Unknown Security Group, page 22-30

Viewing the Egress Policy

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have any one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To view the egress policy:

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

The Egress Policy page appears with the following elements:

- **Header**—Shows the Egress Policy and the selected view in parenthesis. That is, Egress Policy (Matrix View) or Egress Policy (Source Tree view) or Egress Policy (Destination view)
- **View tabs**—Allows you to jump among the three views.
- **Toolbar**—Contains buttons and widgets that are common to all views. Table 22-6 lists all the tool bar items.

Table 22-6 Egress Policy Page Options

Option	Description
Edit	Opens the Edit Permissions popup to edit the configuration of the selected mapped cell. This feature is enabled when at least one mapped cell is selected.
Add	Opens the Create Security Group ACL Mapping popup to configure the selected unmapped cells.
Clear Mapping	Deletes the configuration of a selected mapped cell. This feature is enabled when at least one mapped cell is selected. It does not have any impact on the unmapped cells.
Configure	Allows you to create SGTs and SGACLs directly. See Configuring SGT and SGACL from Egress Policy, page 22-27.
Push	Pushes the Egress Policy data to the SGA network devices. See Push Button, page 22-28.
Monitor All	Changes the status of all enabled cells to Monitor mode automatically when this option is selected. See Monitor Mode, page 22-28.
Dimension	Allows you to change the dimension of the matrix cells. This works only in the Matrix view.
Content Area	Displays and manages the Egress Policy data in different views.
Show	Manages the Filters and Preset Filters.
Default Policy	Shows the default policy configuration settings.

You can view the Egress policy in three different ways:

- Source Tree, page 22-20
- Destination Tree, page 22-20

- Matrix View, page 22-20

Source Tree

The Source Tree view lists a compact and organized view of source SGTs in a collapsed state. You can expand any source SGT to see the internal table that lists all information related to that selected source SGT. This view displays only the source SGTs that are mapped to destination SGTs. If you expand a specific source SGT, it lists all destination SGTs that are mapped to this source SGT and their configurations in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Destination Tree

The Destination Tree view lists a compact and organized view of destination SGTs in a collapsed state. You can expand any destination SGTs to see the internal table that lists all information related to that selected destination SGT. This view displays only the destination SGTs that are mapped to source SGTs. If you expand a specific destination SGT, it lists all source SGTs that are mapped to this destination SGT and their configurations in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Matrix View

The Matrix View of the Egress policy looks like a spreadsheet. It contains two axis:

- Source Axis—The vertical axis lists all the source SGTs.
- Destination Axis—The horizontal axis lists all the destination SGTs.

The mapping of a source SGT to a destination SGT is represented as a cell. If a cell contains data, then it represents that there is a mapping between the corresponding source SGT and the destination SGT. There are two types of cells in the matrix view:

- Mapped cells—When a source and destination pair of SGTs is related to a set of ordered SGACLs and has a specified status.
- Unmapped cells—When a source and destination pair of SGTs is not related to any SGACLs and has no specified status.

Table 22-7 lists the fields of the mapped cells and the descriptions.

Table 22-7 Mapped Cell Fields

Field	Description
Source Security Group	Contains the name of the source SGT and its decimal and hexadecimal value in the format Name (Dec/Hex). For example: Employee (75/004B).
Destination Security Group	Contains the name of the destination SGT and its decimal and hexadecimal value in the same format as Source Security Group.
Status	This field shows the status of the mapping. You can configure the following three status: • Enabled—The SGA device downloads the list of SGACLs from the cell and enforce the policy accordingly. • Disabled—The SGA device ignores this cell. It will not download the list of SGACLs from this cell. • Monitored—The SGA device downloads the list of SGACLs from this cell. It will not enforce the policy accordingly. It just monitors the cell by logging a match between packets and the cell. **Note** The default status is Enabled. Only Enabled and Monitored status are available for the default policy.
Description	(Optional). You can add a description to the cell.
Security Group ACLs	(Required) Contains the ordered list of SGACLs. **Note** This is not a mandatory field for default policy. It can be empty.
Final Catch All Rule	(Required) Contains the set of ACEs defined by the SGACLs list. The status can be any one of the following values: • Permit IP • Deny IP • None **Note** The default value is Permit IP. For default policy, only permit IP and Deny IP are available.

The Egress Policy cell displays the source SGT, the destination SGT, and the Final Catch All Rule as a single list under SGACLs, separated by commas. The Final Catch All Rule is not displayed if it is set to None. An empty cell in a matrix represents an unmapped cell.

In the Egress Policy matrix view, you can scroll across the matrix to view the required set of cells. The browser does not load the entire matrix data at once. The browser requests the server for the data that falls in the area you are scrolling in. This prevents memory overflow and performance issues.

See the "Matrix Operations" section on page 22-22 for more information on different actions that you can perform on a matrix cell.

Matrix Operations

The Matrix view in Cisco ISE looks similar to a spreadsheet. It has source SGT as a row title and destination SGT as a column title. A cell is a crossing of source and destination SGTs. The cell in the matrix view contains the configuration information of source and destination pair to SGACLs. The Matrix view does not display all the fields in order to save the cell area.

Navigating through the Matrix

You can navigate through the matrix either by dragging the matrix content area with the cursor or by using horizontal and vertical scroll bars. You can click and hold on a cell to drag it along with the entire matrix content in any direction. The source and destination bar moves along with the cells. The matrix view highlights the cell and the corresponding row (Source SGT) and column (Destination SGT) when a cell is selected. The coordinates (Source SGT and Destination SGT) of the selected cell are displayed below the matrix content area.

Selecting a Cell in the Matrix

To select a cell in the matrix view, click on it. The selected cell is displayed in different color, and the source and destination SGTs are highlighted. You can deselect a cell either by clicking it again or by selecting another cell. Multiple cell selection is not allowed in the matrix view. Double-click the cell to edit the cell configuration. See Adding and Editing the Mapping of Egress Policy Cells, page 22-25, for more information on editing a matrix cell.

Sorting and Filtering Egress Policy Table

Cisco ISE allows you to sort and filter the egress policy tables. By default, no filter is applied to the Egress Policy table. The Egress Policy table is automatically set to default filtering and sorting in the following cases:

- Switching between views
- Refreshing the egress policy page
- After successful submission of an edited cell (default policy excluded)
- After successful submission of a added cell (default policy excluded)
- After deleting a mappings of a cell (default policy excluded)
- Exiting the SGT/SGACL direct create popup

You can sort the Egress policy in either ascending or descending alphabetical order. It is not case sensitive.

Quick Filter

The Quick Filter in Egress Policy works only with Source and Destination Tree views. It is not case sensitive.

Applying Quick Filter to Egress Policy Cells

To perform a quick filter in Source Tree or Destination Tree, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Egress Policy**

The Egress Policy page appears.

Step 2 Select the desired **tree** view.

The selected Tree view of the Egress Policies is displayed.

Step 3 From the **Show** drop-down list, choose **Quick Filter.**

This adds a filter bar at the top of the external table.

Step 4 Select the appropriate Security group from the drop-down lists.

The Tree view gets filtered according to the selected Group.

Step 5 Expand a Security group to see its internal table.

It opens the internal table with the quick filter options. The filter bar contains the Status, Security Group ACLs, and Description fields. You can filter based on any of the fields.

Step 6 Choose the Status from the drop-down list or enter a value in the Security Group ACLs and Description fields.

The application generates a filter based on the input as soon as you enter a value. You can use single or compound filtering conditions.

For example:

- Single condition—If you enter a value *A* in the field Source Security Group, the application generates a filter of Source Security Group that contains *A*.
- Compound condition—If you enter a value *A* in the field Source Security Group and *B* in the Destination Security Group, the application generates a filter with the AND condition. That is, the resulting filter lists the Source SGT that contains *A* and the Destination that contains *B*.

Advanced Filter

The Advanced filter in the Egress Policy is available in all the three views. Using the Advanced Filter option, you can set a filter based on the source and destination security groups, SGACL, and descriptions.

To perform an advanced filter in the Egress table, complete the following steps.

Step 1 Choose **Policy > Security Group Access > Egress Policy** >

Step 2 From the Egress Policy page, choose **>>** and then **Filter**, and click **Quick Filter** to set a simple filter condition or click **Advanced Filter** to set a compound filter condition.

Note The Egress Policy table displays only the source and destination SGTs that have SGACLs assigned.

Step 3 From the **Filter** drop-down list box, select the field on that you want to set the filter condition. For example, Source Security Group (Dec/Hex).

Step 4 From the **Next** drop-down list, select the operator. For example, Contains.

Step 5 In the **Next** text box, enter the name of the source security group. For example, SGT1.

Step 6 You can click the + button to add additional conditions.

Step 7 After you add all the conditions, click **Go** to view the results of your search.

Step 8 Click the **Save** button ( ) to save this custom Egress table to be viewed later.

Note The filter is specific to the view it was created in. For example, a filter saved in the Source Tree would be visible only in the Source Tree view and not in the Destination Tree or the Egress Matrix views.

The advanced filter provides a Match field that usually determines if the logical operator between all conditions defined by the filter is an AND or an OR (named All and Any respectively). The conditions are organized by field. So all the conditions related to the same field are grouped together with the logical operator defined by the Match field. Between these grouped conditions there is an implicit AND.

For example:

Set the advanced filter with the following conditions:

- Match Any (OR)
- Source SGT starts with A+
- Destination SGT starts with B+
- Source SGT starts with C+
- Destination SGT starts with D+

Result:

Mapped Cells where [(Source SGT starts with A) OR (Source SGT starts with C)] AND [(Destination SGT starts with B) OR (Destination SGT starts with D)]

The fields that can be filtered are dependent on the view you use.

Table 22-8 lists all the fields that can be filtered.

Table 22-8 Filterable Fields

	Source SGT	Destination SGT	Status	SGACLs list	Description
Source Tree	Yes	Yes	Yes	Yes	Yes
Destination Tree	Yes	Yes	Yes	Yes	Yes
Matrix	Yes	Yes	No	No	No

The advanced filter operator is explicit and selectable. Table 22-9 lists the list of operators available for each field to enhance your filter.

Table 22-9 Operators to Enhance Advanced Filtering

	Contains	Does not contain	Does not Equal	Ends with	IS Empty	IS exactly (or equal)	IS not empty	Starts with
Source Security Group	Yes	Yes	Yes	Yes	No	Yes	No	Yes
Destination Security Group	Yes	Yes	Yes	Yes	No	Yes	No	Yes
Status	No	No	Yes	No	No	Yes	No	No

Table 22-9 Operators to Enhance Advanced Filtering

	Contains	Does not contain	Does not Equal	Ends with	IS Empty	IS exactly (or equal)	IS not empty	Starts with
Description	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security Group ACLs	Yes	Yes	Yes	Yes	No	Yes	No	Yes

Presetting Filters

Preset Filter is an advanced filter option available in the show drop-down list. This option contains all the saved advanced filter data. The advanced filter prompts for a name when you click **Save**. Choose **Show** menu and select the required filter from the saved filter to open the filter results. Use the **Manage Preset Filters** option to rename or delete the preset filters.

Configuring Egress Policy Table Cells

Cisco ISE allows you to configure cells using various options that are available in the tool bar. ISE does not allow a cell configuration if the selected source and destination SGTs are identical to a mapped cell.

This section contains:

- Adding and Editing the Mapping of Egress Policy Cells, page 22-25
- Editing the Default Policy, page 22-26
- Deleting a Mapping of a Cell, page 22-27

Adding and Editing the Mapping of Egress Policy Cells

To add or edit a mapping, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Egress Policy**

The Egress Policy page is displayed.

Step 2 Click the appropriate view tab to see the matrix cells.

Step 3 To select the matrix cells, do the following:

- In the matrix view, click a cell to select it.
- In the Source and Destination tree view, check the check box of a row in the internal table to select it.

Step 4 Click one of the following:

- **Add** to add a new mapping cell
- **Edit** to edit an existing mapping cell

If you click **Add**, the create Security Group ACL mapping dialog box appears displaying the source and the destination SGTs of the selected cell.

If you click **Edit**, a single cell edit pop up is displayed with the fields Source and Destination Security Groups, Status, Description, Security Group ACLs, and Final Catch All Rule.

The Edit button becomes enabled as soon as you select a cell. You can also double-click a matrix cell to edit.

Step 5 Select appropriate values for:

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule

See Table 22-7 for the description of these fields.

Step 6 Click **Submit** to save the configuration.

You have successfully added a mapping to a cell or edited a mapped cell.

Step 7 Click **Cancel** to delete the configuration changes.

Editing the Default Policy

The default policy is given as a link at the bottom of the content area.

To edit the default policy, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

The Egress Policy page is displayed.

Step 2 Click **Default Policy**.

The default policy edit popup is displayed with the following fields.

- Source and Destination Security Group—Contains a fixed value <ANY,ANY>
- Status—(Required) The default value is Enabled. Only Enabled and Disabled are available for the default policy status.
- Description—(Optional) Enter the description of the selected configuration.
- Security Group ACLs —(Optional)
- Final Catch All Rule—(Required) The default value as Permit IP. Only Permit IP and Deny IP are available for the default policy Final Catch All Rule.

Step 3 Click **Submit** to save the new configuration.

The system displays an appropriate validation error if any of the entry is invalid.

Step 4 Click **Cancel** to delete the configuration changes.

Deleting a Mapping of a Cell

The Clear Mapping feature deletes the configuration of the selected cells. It is enabled only if you select a cell.

To delete a mapping of a cell, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

The Egress Policy page is displayed.

Step 2 Do the following to access different views of the egress policy table:

- Click **Matrix** to access the matrix view.
- Click **Source Tree** to access the source tree view.
- Click **Destination Tree** to access the destination tree view.

Step 3 Select the cells whose mapping you want to delete:

- In Matrix view, click a matrix cell to select it.
- In source and destination view, check the check box of the rows in the internal table whose mapping you want to delete.

Step 4 Click **Clear Mapping**.

The following warning messages are displayed in different views:

- Matrix view:

  Are you sure you want to clear the mappings of the selected cell? OK to continue, Cancel to abort.
- Source and Destination Tree view:

  Are you sure you want to clear the mappings of X cells? OK to continue, Cancel to abort.

Step 5 Click **OK**.

The configurations of the selected cells are deleted.

Configuring SGT and SGACL from Egress Policy

Security groups and Security group ACLs can be created directly from the Egress Policy page.

To create Security Group directly from the Egress Policy page, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

The Egress Policy page is displayed.

Step 2 Choose **Create Security Group** from the Configure option drop-down list.

Step 3 Follow the procedure as explained in Configuring Security Groups, page 22-10 to create a Security Group.

To create Security Group ACLs directly from the Egress Policy page, complete the following steps:

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

The Egress Policy page is displayed.

Step 2 Choose **Create Security Group ACLs** from the Configure option drop-down list.

Step 3 Follow the procedure as explained in Configuring Security Group Access Control Lists, page 22-12 to create a Security Group ACLs.

Push Button

The Push option in the egress policy initiates a CoA notification that calls the SGA devices to immediately request for updates from Cisco ISE regarding the configuration changes in the egress policy. For more information on Egress Policy CoA, see Update SGT Matrix CoA, page 22-38

Monitor Mode

The Monitor All option in the egress policy allows you to change the entire egress policy configuration status to monitor mode with a single click. Check the **Monitor All** check box in the egress policy page to change the egress policy configuration status of all the cells to monitor mode. When you check the Monitor All check box, the following changes take place in the configuration status:

- The cells whose status is Enabled will act as monitored but appears as if they are enabled.
- The cells whose status is Disable will not be affected.
- The cells whose status is Monitor will remain Monitored.

Uncheck the Monitor All check box to restore the original configuration status. It does not change the actual status of the cell in the database. When you deselect Monitor All, each cell in the egress policy regains its original configuration status.

Monitoring the Monitor Mode

The monitoring functionality of the monitor mode helps you to:

- Know how much traffic is filtered but monitored by the monitor mode
- Know that SGT-DGT pair is in monitor mode or enforce mode, and observe if there is any unusual packet drop is happening in the network
- Understand that SGACL drop is actually enforced by enforce mode or permitted by monitor mode
- Create custom reports based on the type of mode (monitor, enforce, or both)
- Identify which SGACL has been applied on NAD and display discrepancy, if any

You can view the monitor mode data from the following reports:

- Top N RBACL Drops by Destination
- Top N RBACL Drops by User
- RBACL Drop Summary

This section describes the process of running each of these reports. For more information on Cisco ISE reports, see Chapter 24, "Reporting."

Top N RBACL Drops by Destination

To run the Top N RBACL Drops by Destination report, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Security Group Access**.

Step 3 In the Reports panel on the right, click the **Top N RBACL Drops by Destination** radio button.

Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last hour
- Last 12 hours
- Today
- Yesterday
- Last 7 days
- Last 30 days

You can use the Run button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters.

Step 5 If you choose Query and Run from the Run drop-down list, you can specify the mode from the Enforcement mode drop-down list as, Enforce, Monitor or Both.

Top N RBACL Drops by User

To run the Top N RBACL Drops by User report, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Security Group Access**.

Step 3 In the Reports panel on the right, click the **Top N RBACL Drops by User** radio button.

Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last hour
- Last 12 hours
- Today
- Yesterday
- Last 7 days
- Last 30 days

You can use the Run button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters.

Step 5 If you choose Query and Run from the Run drop-down list, you can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.

RBACL Drop Summary

To run the RBACL Drop Summary report, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Security Group Access**.

Step 3 In the Reports panel on the right, click the **RBACL Drop Summary** radio button.

Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last hour
- Last 12 hours
- Today
- Yesterday
- Last 7 days
- Last 30 days

The report runs upon choosing the time period. You can see the type of mode under the Enforcement mode column. The default value for this is Both.

Step 5 If you choose Query and Run from the Run drop-down list, you can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.

The Unknown Security Group

The Unknown security group is a pre-configured security group that cannot be modified and represents the ox000 SGT.

The Cisco Security Group network devices request for cells that refer to the unknown SGT when they do not have a SGT of either source or destination. If only the source is unknown, the request applies to the <unknown, Destination SGT> cell. If only the destination is unknown, the request applies to the <source SGT, unknown> cell. If both the source and destination are unknown, the request applies to the <Unknown, Unknown> cell.

Default Policy

Default Policy refers to the <ANY,ANY> cell. Any source SGT is mapped to any destination SGT. Here, the ANY SGT cannot be modified and it is not listed in any source or destination SGTs. The ANY SGT can only be paired with ANY SGT. It cannot be paired with any other SGTs. A SGA network device attaches the default policy to the end of the specific cell policy.

- If a cell is empty, that means it contains the default policy alone.

- If a cell contains some policy, the resulting policy is a combination of the cell specific policy followed by the default policy.

According to ISE, the cell policy and the default policy are two separate sets of SGACLs that the devices get in response to two separate policy queries.

Configuration of the default policy is different from other cells:

- Status can take only two values, Enabled or Monitored.
- Security Group ACLs is an optional field for the default policy, so can be left empty.
- Final Catch All Rule can be either Permit IP or Deny IP. Clearly the None option is not available here because there is no safety net beyond the default policy.

OOB SGA PAC

All SGA network devices possess an SGA PAC as part of the EAP-FAST protocol. This is also utilized by the secure RADIUS protocol where the RADIUS shared secret is derived from parameters carried by the PAC. One of these parameters, Initiator-ID, holds the SGA network device identity, namely the Device ID.

If a device is identified using SGA PAC and there is no match between the Device ID, as configured for that device on Cisco ISE, and the Initiator-ID on the PAC, the authentication fails.

Some SGA devices (for example, Cisco firewall ASA) do not support the EAP-FAST protocol. Therefore, ISE can not provision these devices with SGA PAC over EAP-FAST. Instead, the SGA PAC is generated on ISE and manually copied to the device; hence this is called as the Out of Band (OOB) SGA PAC generation.

When you generate a PAC from Cisco ISE, a PAC file encrypted with the Encryption Key is generated.

This section describes the following:

- SGA PAC Provisioning, page 22-31
- Monitoring SGA PAC, page 22-33

SGA PAC Provisioning

This section describes the following:

- Generating an SGA PAC from the Settings Screen, page 22-31
- Generating an SGA PAC from the Network Devices Screen, page 22-32
- Generating an SGA PAC from the Network Devices List Screen, page 22-33

Generating an SGA PAC from the Settings Screen

To generate an SGA PAC from the Settings screen, complete the following steps:

Step 1 Choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **Protocols**.

Step 3 Choose **EAP-FAST > Generate PAC**.

The Generate PAC page appears.

Step 4 Follow the instructions in the "Generating the PAC for EAP-FAST" section on page 16-11 to generate SGA PAC.

Generating an SGA PAC from the Network Devices Screen

To generate an SGA PAC from the Network Devices screen, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears with a list of configured devices.

Step 3 Click **Add**, or check the check box next to a device and click **Edit** to edit it or click **Duplicate** to create a duplicate entry. You can alternatively click **Add new device** from the action icon on the Network Devices navigation pane or click a device name from the list to edit it.

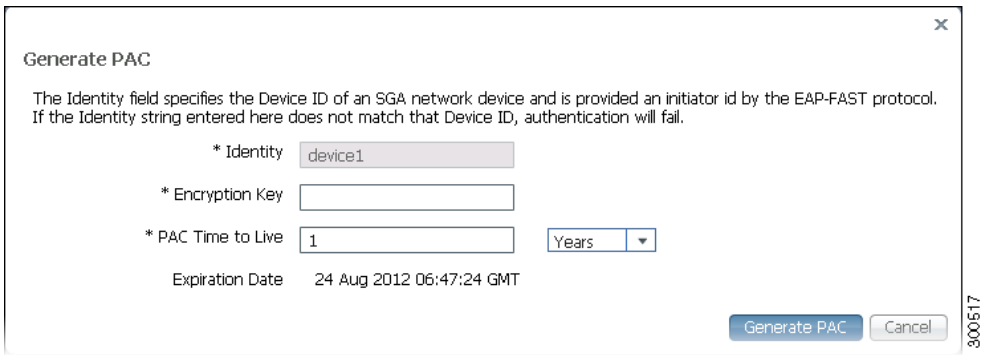
Step 4 If you are adding a new device, provide a device name.

Step 5 Check the Security Group Access (SGA) check box to configure an SGA device.

Step 6 Under the Out of Band (OOB) SGA PAC sub section, click **Generate PAC**.

Step 7 The Generate PAC dialog box is displayed, as shown in Figure 22-2.

Figure 22-2 Generate PAC Dialog Box



Step 8 Provide the following details:

- PAC Time to Live—(Required) Enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is ten years.
- Encryption Key—(Required) Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.

The Encryption Key is used to encrypt the PAC in the file that is generated. This key is also used to decrypt the PAC file on the devices. Therefore, it is recommended that the administrator saves the Encryption Key for later use.

The Identity field specifies the Device ID of an SGA network device and is given an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication will fail.

The expiration date is calculated based on the PAC Time to Live.

Step 9 Click **Generate PAC.**

Generating an SGA PAC from the Network Devices List Screen

To generate an SGA PAC from the Network Devices list screen, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 From the Network Devices navigation pane on the left, click **Network Devices**.

The Network Devices page appears with a list of configured devices.

Step 3 Check the check box next to a device for which you want to generate the SGA PAC and click **Generate PAC**.

The Generate PAC dialog box is displayed, as shown in Figure 22-2.

Step 4 Provide the details as described in Step 8 of the "Generating an SGA PAC from the Network Devices Screen" section on page 22-32.

Step 5 Click **Generate PAC**.

Monitoring SGA PAC

You can view SGA PAC provisioning data in the form of a PAC Provisioning Report.

This section describes the process of running this report. For more information on Cisco ISE reports, see Chapter 24, "Reporting."

PAC Provisioning Report

To view PAC Provisioning data, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Security Group Access**.

Step 3 In the Reports panel on the right, click the **PAC Provisioning** radio button.

Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last hour
- Last 12 hours
- Today
- Yesterday
- Last 7 days
- Last 30 days
- Query and run

You can use the **Run** button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters.

SGA CoA

Cisco ISE supports SGA Change of Authorization (CoA) which allows ISE to notify SGA devices about Security Group changes, so that the devices can reply with requests to get the relevant data.

A CoA notification can trigger a SGA network device to send either an Environment CoA or a Per Policy CoA.

This section contains:

- CoA Supported Network Devices, page 22-34
- Environment CoA, page 22-35
- Per Policy CoA, page 22-37
- SGA CoA Summary, page 22-40
- Monitoring SGA CoA, page 22-40

CoA Supported Network Devices

ISE sends CoA notifications to the following network devices:

- Network device with single IP address (subnets are not supported)
- Network device configured as SGA device
- Network device set as CoA supported

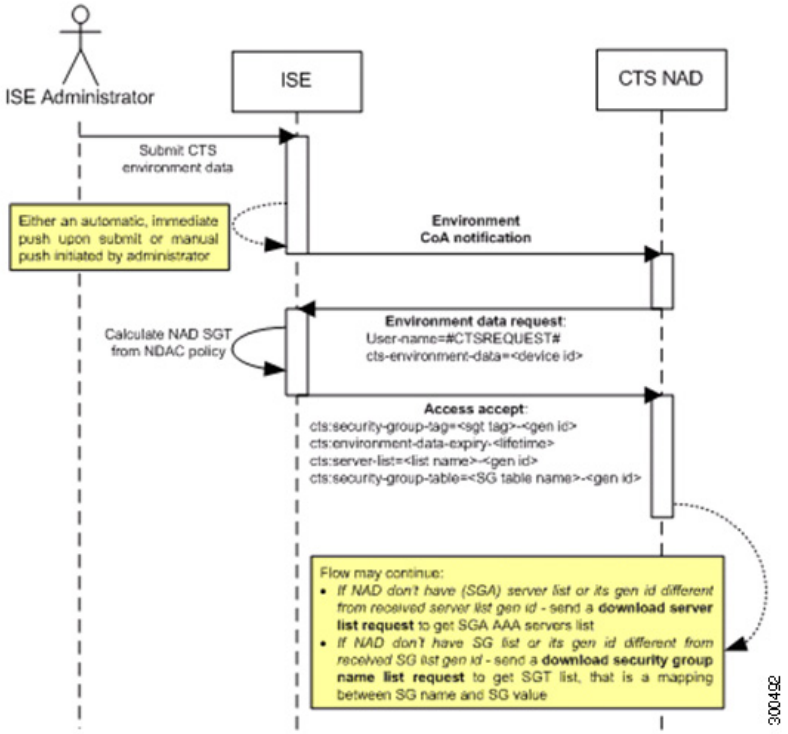
When Cisco ISE is deployed in a distributed environment where there are several secondaries that interoperate with different sets of devices, CoA requests are sent from Cisco ISE primary node to all the network devices. Therefore, SGA network devices need to be configured with the ISE primary node as the CoA client.

The devices return CoA NAK or ACK back to the Cisco ISE primary node. However, the SGA session that follows an SGA CoA is handled by the related Cisco ISE secondary node.

Environment CoA

Figure 22-3 depicts the Environment CoA notification flow.

Figure 22-3 Environment CoA Notification Flow



1. Cisco ISE sends an environment CoA notification to the SGA network device.
2. The device returns an environment request.
3. In response to the environment data request, Cisco ISE returns:
   a. The environment data of the device that sent the request—This includes the SGA device's SGT (as inferred from the NDAC policy) and download environment TTL.
   b. The name and generation ID of the SGA AAA server list.
   c. The names and generation IDs of (potentially multiple) SGT tables—These tables list SGT name versus SGT value, and together these tables hold the full list of SGTs.
4. If the device does not hold an SGA AAA server list, or the generation ID is different from the generation ID that is received, the device sends another request to get the AAA server list content.
5. If the device does not hold an SGT table listed in the response, or the generation ID is different from the generation ID that is received, the device sends another request to get the content of that SGT table.

Initiating Environment CoA

An Environment CoA can be triggered for:

- Network Devices, page 22-36
- Security Groups, page 22-36
- SGA AAA Servers, page 22-36
- NDAC Policy, page 22-37

Network Devices

To trigger an Environment CoA for the Network devices, complete the following steps:

Step 1 Choose **Administration > Network Resources > Network Devices**.

Step 2 Add or edit a network device.

Step 3 Update Security Group parameters under the SGA Attributes section.

Changing the environment TTL is notified only to the specific SGA network device where the change took place.

Since only a single device is impacted, an environmental CoA notification is sent immediately upon submission. The result is a device update of its environment TTL.

Security Groups

To trigger an Environment CoA for the security groups, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane on the left, click the **>** button next to Security Group Access and click **Security Groups**.

Step 3 In the security group page, change the name of an SGT, which will change the name of the mapping value of that SGT. This triggers an environmental change.

Step 4 Click the **Push** button to initiate an environment CoA notification after changing the names of multiple SGTs. This environment CoA notification goes to all SGA network devices and provides an update of all SGTs that were changed.

SGA AAA Servers

To trigger an Environment CoA for the SGA AAA servers, complete the following steps:

Step 1 Choose **Administration > Network Resources > SGA AAA Servers**.

Step 2 In the SGA AAA Servers page create, delete or update the configuration of an SGA AAA server. This triggers an environment change.

Step 3 Click the **Push** button to initiate an environment CoA notification after you configure multiple SGA AAA servers. This environment CoA notification goes to all SGA network devices and provides an update of all SGA AAA servers that were changed.

NDAC Policy

To trigger an Environment CoA for the NDAC Policies, complete the following steps:

In the NDAC policy page you can create, delete, or update rules of the NDAC policy. These environment changes are notified to all network devices.

You can initiate an environment CoA notification by clicking the Push button in the NDAC policy page. This environment CoA notification goes to all SGA network devices and provides an update of network device own SGT, as described in the "Environment CoA" section on page 22-35.

Per Policy CoA

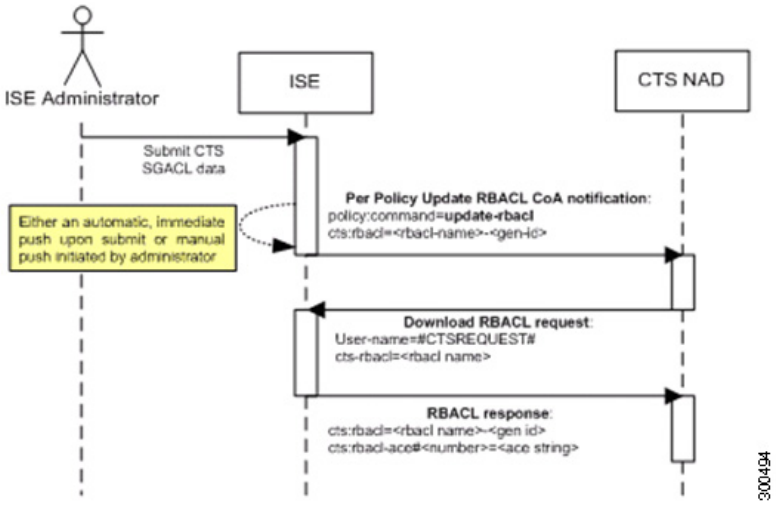
There are three types of Per Policy CoA notification:

- Update RBACL Named List CoA—Triggers a request to download SGACL (RBACL).
- Update SGT Matrix CoA—Triggers a request to download all egress policy cells related to a certain destination SGT (to an egress policy column).
- Policies Update CoA—This is an optimization that allows initiating multiple calls for both RBACL content and egress policy cells with a single CoA notification.

Update RBACL Named List CoA

Figure 22-4 depicts the Update RBACL Named List CoA flow.

Figure 22-4 Update RBACL Named List CoA Notification Flow



1. ISE sends an update RBACL named list CoA notification to a SGA network device. The notification contains the SGACL name and the generation ID.
2. The device may replay with an SGACL (RBACL) data request if both of the following terms are fulfilled:
   a. If the SGACL is part of an egress cell that the device holds. The device holds a subset of the egress policy data, which are the cells related to the SGTs of its neighboring devices and endpoints (egress policy columns of selected destination SGTs).

b. The generation ID in the CoA notification is different from the generation ID that the device holds for this SGACL.

3. In response to the SGACL data request, ISE returns the content of the SGACL (the ACE).

Initiating an Update RBACL Named List CoA

To trigger an Update RBACL Named List CoA, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results**.

Step 2 From the Results navigation pane on the left, click the **>** button next to Security Group Access and click **Security Group ACLs**.

Step 3 Add or edit a SGACL as described in Configuring Security Group Access Control Lists, page 22-12.

After you submit a SGACL, it promotes the generation ID of the SGACL.

Step 4 Click the **Push** button to initiate an Update RBACL Named List CoA notification after you change the content of multiple SGACLs. This notification goes to all SGA network devices, and provides an update of that SGACL content on the relevant devices.

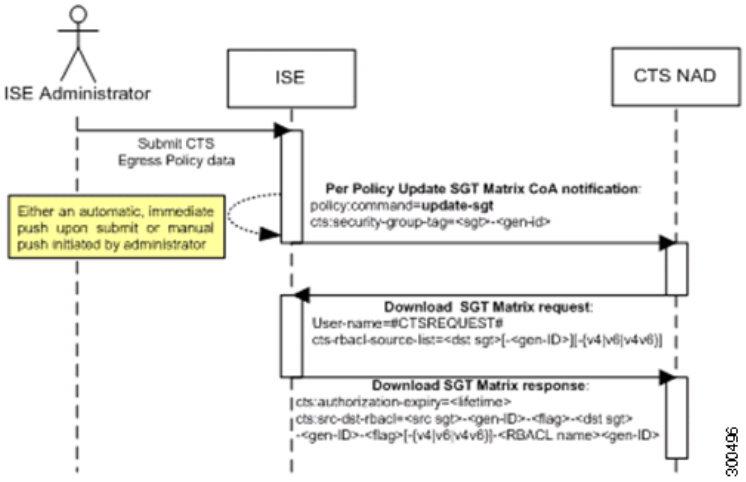
Changing the name or the IP version of an SGACL does not change its generation ID; hence it does not require sending an update RBACL named list CoA notification.

However, changing the name or IP version of an SGACL that is in use in the egress policy indicates a change in the cell that contains that SGACL, and this changes the generation ID of the destination SGT of that cell. See Initiating Update SGT matrix CoA from Egress Policy, page 22-39 that deals with changes in the egress policy.

Update SGT Matrix CoA

Figure 22-5 depicts the Update SGT Matrix CoA flow.

Figure 22-5 Update SGT Matrix CoA flow



1. Cisco ISE sends an updated SGT matrix CoA notification to a SGA network device. The notification contains the SGT value and the generation ID.
2. The device may replay with an SGT data request if both the following terms are fulfilled:
   a. If the SGT is the SGT of a neighboring device or endpoint, the device downloads and hold the cells related to SGTs of neighboring devices and endpoints (a destination SGT).
   b. The generation ID in the CoA notification is different from the generation ID that the device holds for this SGT.
3. In response to the SGT data request, ISE returns the data of all egress cells, such as the source and destination SGTs, the status of the cell, and an ordered list of the SGACL names configured in that cell.

Initiating Update SGT matrix CoA from Egress Policy

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

Step 2 On the Egress Policy page, change the content of a cell (status, SGACLs).

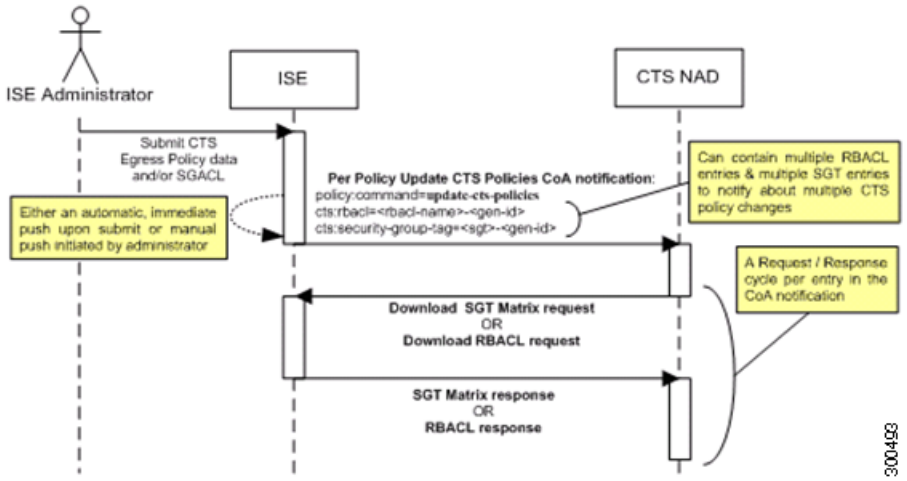
Step 3 After you submit the changes, it promotes the generation ID of the destination SGT of that cell.

Step 4 Click the **Push** button to initiate the Update SGT matrix CoA notification after you change the content of multiple egress cells. This notification goes to all SGA network devices, and provides an update of cells content on the relevant devices.

Policies Update CoA

Figure 22-6 depicts the Policies Update CoA flow.

Figure 22-6 Policies Update CoA flow



1. ISE sends an update policies CoA notification to a SGA network device. The notification may contain multiple SGACL names and their generation IDs, and multiple SGT values and their generation IDs.

2. The device may replay with multiple SGACL data requests and/or multiple SGT data.
3. In response to each SGACL data request or SGT data request, ISE returns the relevant data.

SGA CoA Summary

Table 22-10 summarizes the various scenarios that may require initiating an SGA CoA, the type of CoA used in each scenario, and the related UI pages.

Table 22-10 SGA CoA Summary

UI Page	Operation that triggers CoA	How it is triggered	CoA type	Send to
Network Device	Changing the environment TTL in the SGA section of the page	Upon successful Submit of SGA network device	Environment	The specific network device
SGA AAA Server	Any change in the SGA AAA server (create, update, delete, reorder)	Accumulative changes can be pushed by clicking the Push button on the SGA AAA servers list page.	Environment	All SGA network devices
Security Group	Any change in the SGT (create, rename, delete)	Accumulative changes can be pushed by clicking the Push button on the SGT list page.	Environment	All SGA network devices
NDAC Policy	Any change in the NDAC policy (create, update, delete)	Accumulative changes can be pushed by clicking the Push button on the NDAC policy page.	Environment	All SGA network devices
SGACL	Changing SGACL ACE	Accumulative changes can be pushed by clicking the Push button on the SGACL list page.	Update RBACL named list	All SGA network devices
	Changing SGACL name or IP version	Accumulative changes can be pushed by clicking the Push button on the SGACL list page or the policy push button in the Egress table.	Update SGT matrix	All SGA network devices
Egress Policy	Any operation that changes the generation ID of an SGT	Accumulative changes can be pushed by clicking the Push button on the egress policy page.	Update SGT matrix	All SGA network devices

Monitoring SGA CoA

SGA CoA notifications can be viewed as alarms, logs, and reports.

This section describes how to view the following:

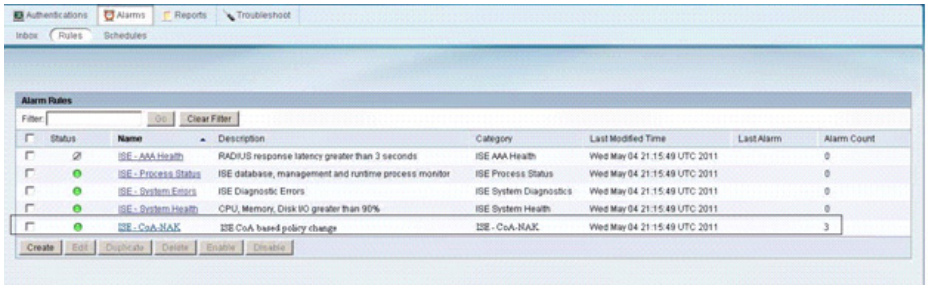
- SGA CoA Alarms, page 22-41
- SGA CoA Report, page 22-41

SGA CoA Alarms

When CoA returns CoA-NAK, an alarm is generated, as shown in Figure 22-7.

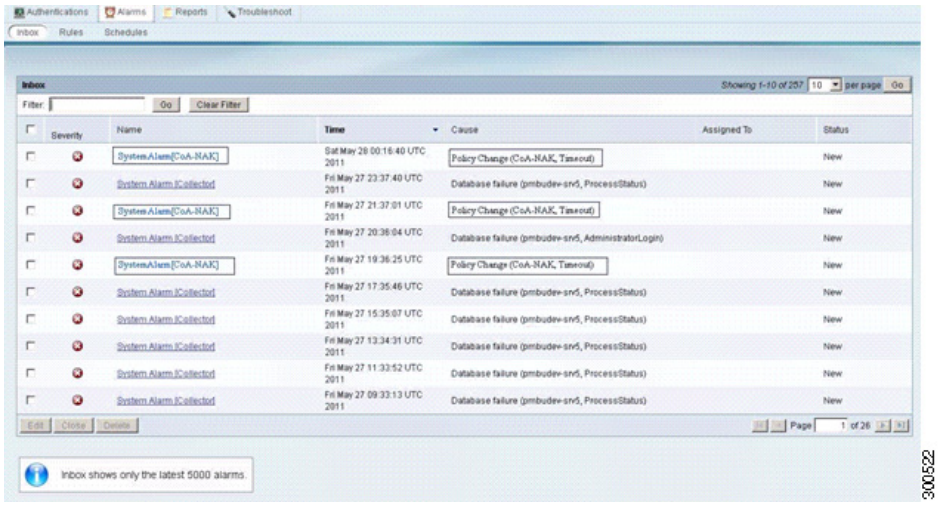
To view SGA CoA alarms, go to **Operations > Alarms > Rules**.

Figure 22-7 SGA CoA Alarms



You can also view the SGA CoA alarms under Live Logs. To view live logs, go to **Operations > Alarms > Inbox** as shown in Figure 22-8**.**

Figure 22-8 SGA CoA Alarms Under Live Logs



SGA CoA Report

To view SGA CoA notification data, complete the following steps:

Step 1 From the ISE Admin dashboard, select **Operations > Reports > Catalog**.

Step 2 In the Reports list, select **Security Group Access**.

Step 3 In the Reports panel on the right, click the **Policy CoA** radio button.

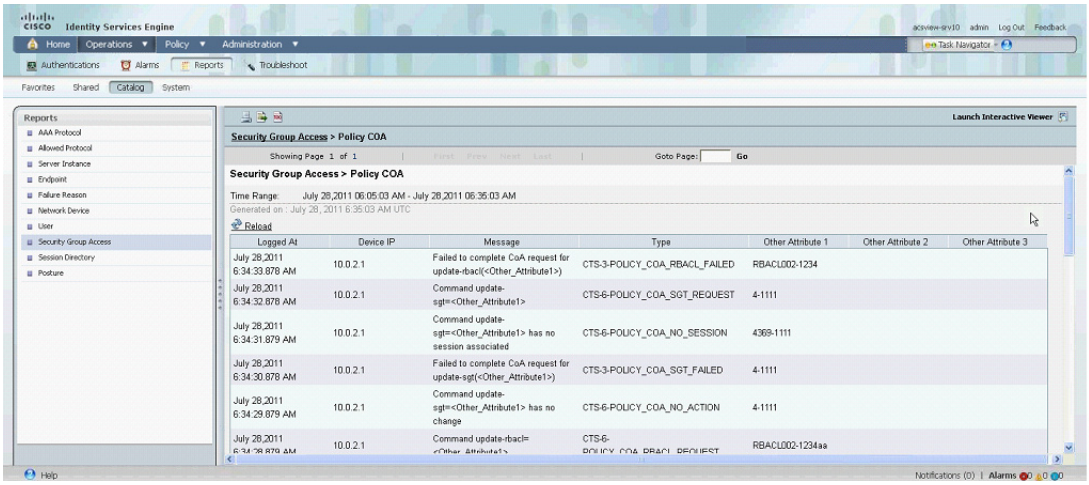
Step 4 From the Run drop-down menu, choose a time period over which the report data will be collected:

- Last hour
- Last 12 hours

- Today
- Yesterday
- Last 7 days
- Last 30 days
- Query and run

You can use the **Run** button to run the report for a specific period, or use the Query and Run option. The Query and Run option allows you to query the output by using various parameters. See Figure 22-9.

Figure 22-9 SGA CoA Report





PART 4

Monitoring and Troubleshooting Cisco ISE



CHAPTER 23

Monitoring and Troubleshooting

The Operations tab on the Cisco Identity Services Engine (ISE) home page, also known as the dashboard, provides integrated monitoring, reporting, alerting, and troubleshooting, all from one centralized location.

This chapter explains monitoring and troubleshooting functions and tasks, and covers the following topics:

- Understanding Monitoring and Troubleshooting, page 23-1
- Configuring Devices for Monitoring, page 23-3
- Cisco ISE Dashboard Monitoring, page 23-3
- Monitoring the Network, page 23-10
- Troubleshooting the Network, page 23-29
- Obtaining Additional Troubleshooting Information, page 23-40
- Monitoring Administration, page 23-45

Note For a list of inherent known issues and workarounds associated with monitoring and troubleshooting, see the *Release Notes for the Cisco Identity Services Engine, Release 1.1*.

Understanding Monitoring and Troubleshooting

Monitoring and troubleshooting is a comprehensive identity solution for all Cisco ISE run-time services, using the following components:

- Monitoring—Provides a real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and effect operational conditions.
- Troubleshooting—Provides contextual guidance for resolving access issues on networks. You can then address user concerns and provide resolution in a timely manner.
- Reporting—Provides a catalog of standard reports that you can use to analyze trends and monitor system performance and network activities. You can customize reports in various ways, and save your changes for future use.

The Cisco ISE dashboard provides visibility into configured policies, authentication and authorization activities, profiled endpoints, postured sessions, and guest activities. Likewise, monitoring and troubleshooting capabilities include the following:

- A real-time summary of system activity and individual services, as well as a comprehensive at-a-glance view of network activity.
- A web-based user interface that simplifies generating and accessing predefined and custom reports.
- Various alert capabilities, including rules and triggers on authentication activity, that allows for early detection of operation or trends.

The data that is gathered by monitoring functionality is accessible from the central administration console, known as the Cisco ISE dashboard. When you log into the administration console, the real-time data, as shown in Figure 23-1.

The dashboard shows the activity on the Network Privilege Framework (NPF), and provides drill-down capabilities for information on the various components. For information on the dashlets and metric meters that comprise the dashboard, see Cisco ISE Dashboard Monitoring, page 23-3.

The NPF is composed of the following three tiers:

Table 23-1 NPF Tiers

Tier	Specifications
1	Access control based on identity using 802.1x, MAC authentication bypass (MAB), the Cisco ISE Profiler service
2	Access control based on identity using 802.1x, MAB, Profiler, guest provisioning of the Network Admission Control (NAC) manager, central web authentication
3	Access control based on identity and posture using 802.1x, MAB, Profiler, guest provisioning of the NAC manager, central web authentication

NPF authentication and authorization generates a flow of events. The events from the different sources are then collected by Cisco ISE monitoring and troubleshooting tools and summarized. You can view the authentication and authorization results on the dashboard, or choose to run any number of reports. For more information, see Chapter 24, "Reporting."

The NPF authentication and authorization event flow uses the following process:

Step 1 NAD performs an authorization or flex authorization.

Step 2 An unknown, agentless identity is profiled with web authorization.

Step 3 RADIUS server authenticates and authorizes the identity.

Step 4 Authorization is provisioned for the identity at the port.

Step 5 Unauthorized endpoint traffic is dropped.

User Roles and Permissions

Monitoring and troubleshooting capabilities are associated with default user roles. The tasks you are allowed to perform are directly related to your assigned user role. For more information on the user roles and their assigned permissions, see Understanding the Impact of Roles and Admin Groups, page 2-19.

Monitoring and Troubleshooting Database

The Cisco ISE monitoring service collects and stores data in a specialized Monitoring database. The rate and amount of data utilized to monitor network functions may require a node dedicated solely to monitoring. If your Cisco ISE network collects logging data at a high rate from Policy Service ISE nodes or network devices, a Cisco ISE node dedicated to monitoring is recommended.

To manage the information stored in the Monitoring database, administrators are required to perform full and incremental backups of the database. This includes purging unwanted data, and then restoring the database. For more information, see Monitoring Administration, page 23-45.

Configuring Devices for Monitoring

The Monitoring ISE node receives and uses data from devices on the network to populate the dashboard display. To enable communication between the Monitoring ISE node and the network devices, switches and network access devices (NADs) must be configured properly.

For information on how to configure these devices, see the following:

- Configure NADs for ISE Monitoring, page D-33

Cisco ISE Dashboard Monitoring

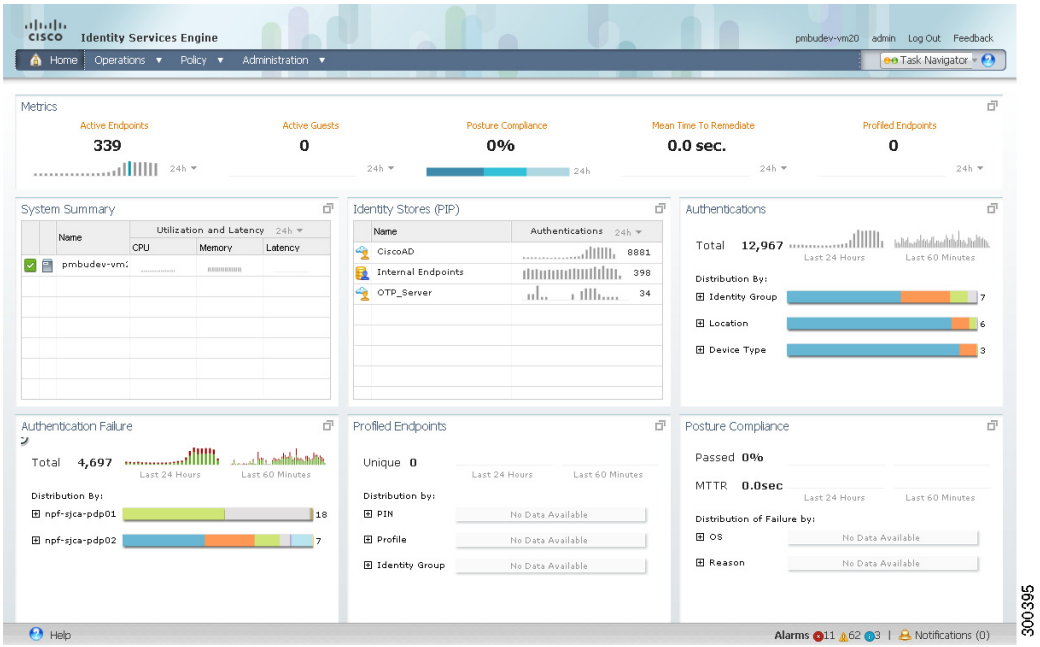
The Cisco ISE dashboard (Home) is the landing page that appears after you log into the Cisco ISE administration console. The dashboard is a centralized management console consisting of metric meters along the top of the window, with dashlets below. This section describes the features functions that comprise the dashboard, as they are represented in the following the graphical user interface elements:

- Dashlets, page 23-4
- Metric Meters, page 23-9

Dashboard real-time data provides an at-a-glance status of the devices and users that are accessing your network, as well as a system health overview.

Note You must have Adobe Flash Player installed on the Administration ISE node to be able to view the dashlets and metric meters on the dashboard.

Figure 23-1 The Cisco ISE Dashboard



The Alarms icon at the bottom right of the Cisco ISE window provides instant access to alarm summaries. Mouse over the Alarms icon to display a pop-up page with a list of recent alarms. You can run filters on the list to view only the alarms of a specific nature. Or, you can drill down for detailed information on individual alarms.

Default alarms include ISE AAA health, ISE process status, ISE system health, and ISE system diagnostics.

For more information:

For information on how to interpret and use the data that is shown on the Cisco ISE dashboard, see the following sections:

- Simplifying Complex Data, page 2-7
- Managing Alarms, page 23-11
- Drilling Down for Details, page 2-15.

Dashlets

Dashlets are individual panels on the dashboard, dashlets summarize important statistics about the devices and users accessing the network. They also provide information about the overall health and security of the network. Each dashlet contains an independent function, and can display the statistical data that is related to its function in various ways. This section explains the purpose and functions of the standard dashlets.

Note You can click a sparkline in a dashlet to generate a report showing relevant logs. Sparklines are a method of visualizing data with vertical lines that depict trends over time. Taller bars mean there was a higher load at a particular time.

Hovering a cursor over the elements of a dashlet brings up a tooltip with detailed information. Tooltip values for a sparkline reflect the specified time interval.

For example, a sparkline with the 24 hour time interval 14 March 3:00 AM, means the sparkline value is calculated based on logs from 3:00 AM to 4:00 AM on that date. Likewise, a sparkline for the 60 minute interval 14 March 3:01:00 AM, means the sparkline value is calculated based on logs from 3:01:00 to 3:02:00 on that date.

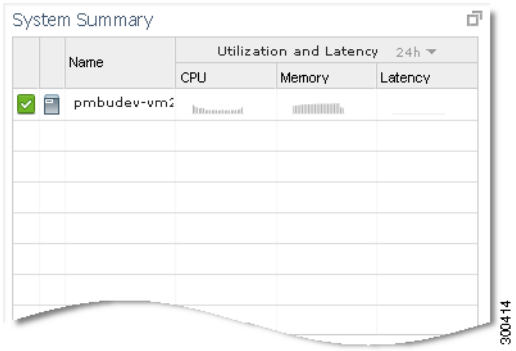
System Summary

The System Summary dashlet focuses on the health of the distributed identity services system deployment. This dashlet provides data for all the nodes on your network, providing an at-a-glance view of node performance, such as CPU, memory, and latency utilization. Sparklines represent a percentage of CPU usage over a specified time increment. For more information, see Sparklines, page 2-14.

The color of the system status icon indicates the health of your system:

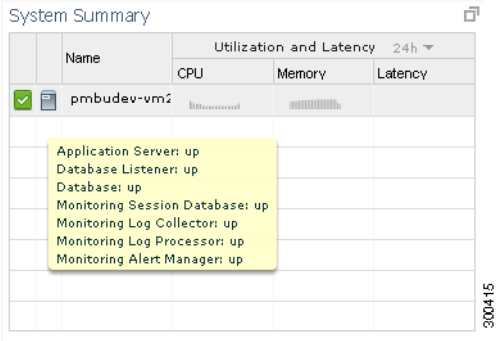
- Healthy = Green
- Warning = Yellow
- Critical = Red
- No information = Gray

Figure 23-2 System Summary Dashlet



When you hover the cursor over the health icon, a quick view dialog appears showing detailed information on system health, as shown in Figure 23-3.

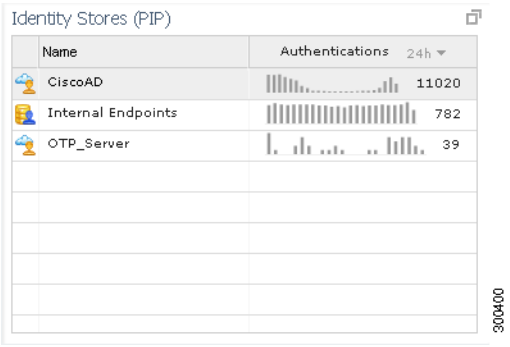
Figure 23-3 System Summary Quick View Display



Identity Stores

The Identity Stores dashlet for policy information points (PIP) focuses on the Microsoft Active Directory infrastructure, providing data on the number of authentications for users and devices, as well as the health of the servers. Internal user attributes and the credential information that was most used to authenticate users and hosts for a given time range is also shown.

Figure 23-4 Identity Stores Dashlet

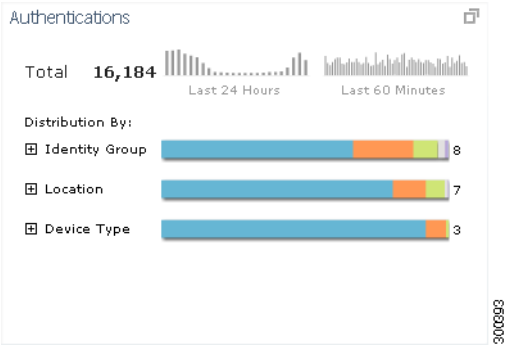


Authentications

The Authentications dashlet shows passed and failed network authentications, providing data on the user or type of device, location, and the identity group to which the user or device belongs. The sparklines along the top of the dashlet represent distribution over the last 24 hours and the last 60 minutes.

When you hover your cursor over a stack bar or sparkline, a tooltip provides detailed information. Figure 23-5 shows data for all authentication attempts that are made on the network, both passed and failed.

Figure 23-5 Authentications Dashlet



Authentication Failure

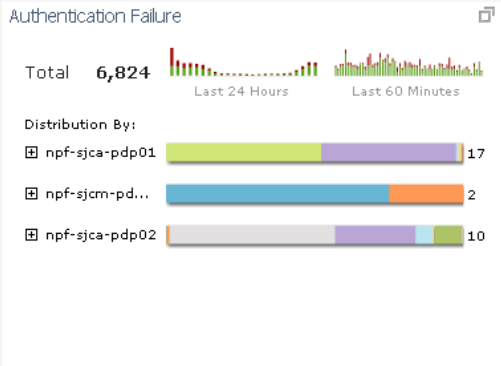
The Authentication Failure dashlet focuses on authentication failures, providing information on the nature of the failures. Total counts are shown across the top, while below is a breakdown of statistics by individual node and individual errors.

When you hover your cursor over a stack bar or sparkline, a tooltip provides detailed information. Sparklines use color to convey passed or failed authentication status at a glance. Green represents passed authentications, and red represents failed authentications.

You can quickly assess the nature of failures that occur on your network with the following information:

- Total count of authentication failures in the last 24 hours
- Authentication trend (60 minutes to 24 hours), marking failures with a different color
- Distribution across all ISE nodes
- Distribution of reasons for failure
- Failure reason trend per Policy Service
- Visual health cues: green = pass, yellow = warning, red = failure

Figure 23-6 Authentication Failure Dashlet



Profiled Endpoints

The Profiled Endpoint dashlet focuses on the endpoints on the network that have matched profiles, providing profile data for each endpoint. For example, the statistics allow you to determine the type of device, its location, and its IP address. The sparklines along the top of the dashlet represent endpoint activity over the last 24 hours and last 60 minutes.

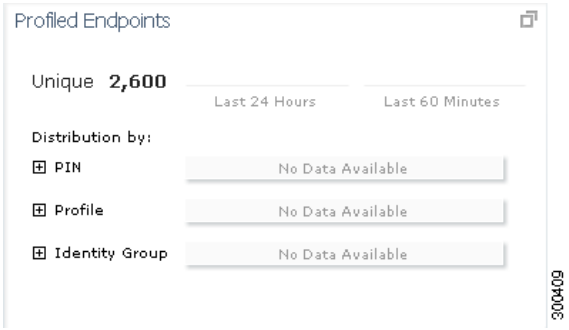
You can expand the following data categories for more information:

- PIN—Place in network
- Profile—Profiler policy
- Identity Group—Includes both user and endpoint identity groups, as applicable

Note The Profiled Endpoint dashlet represents the total number of endpoints that have been profiled on the network for the last 24 hours, including those that are unknown. It is not a representation of how many endpoints are currently active on the network. Sparkline metrics at the top of the dashlet show time specific values for the last 24 hours and 60 minutes.

For information on Profiled Endpoints dashlet, see the "Profiled Endpoints Dashlet" section on page 18-6.

Figure 23-7 Profiled Endpoints Dashlet



Posture Compliance

The Posture Compliance dashlet focuses on the health of the network, providing information on the users who are accessing the network and whether they meet posture compliance. Data is shown on the devices that are currently connected to the network. The stack bars show noncompliance statistics that are arranged according to operating system and other criteria. Sparklines represent the percentage of compliant versus noncompliant posture attempts.

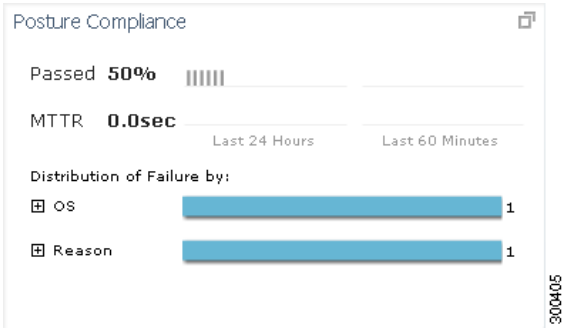
- Passed—Overall average percentage (%) of compliant posture attempts for the last 24 hours and 60 minutes.

Note When you hover a cursor over a sparkline, the tooltip shows the average percentage of compliant posture attempts for a specific time period.

- MTTR—Mean Time To Remediate (MTTR). The time difference between an endpoint moving from a non-compliant to a compliant state is used to determine the mean time to remediate (MTTR). The endpoint MAC address is used as the key to calculate the MTTR.
- OS—Operating system
- Reason—Reason for compliance or noncompliance

For information on Posture Compliance dashlet, see the "Posture Compliance Dashlet" section on page 20-8.

Figure 23-8 Posture Compliance Dashlet



Metric Meters

Metric meters are graphs that appear along the top section of the dashboard. Their data is refreshed every minute to provide real-time at-a-glance information.

Note You can click the main number display in a metric meter to display relevant detailed report data.

Active Endpoints

The Active Endpoints metric meter shows data representing the endpoints connected to the network. The change indicator shows the difference in the number of active endpoints between refreshes.

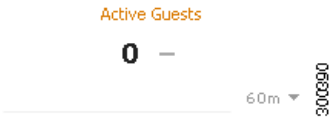
Figure 23-9 Active Endpoints Metric Meter



Active Guests

The Active Guests metric meter shows data representing the current active guests on the network. The change indicator shows the difference in count between the current refresh and the last refresh.

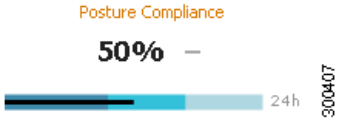
Figure 23-10 Active Guests Metric Meter



Posture Compliance

The Posture Compliance metric meter shows the (average) percentage of hosts that are connected to the system that were compliant with posture rules over the last 24 hours. The black line superimposed on the color-coded bar changes dynamically to show compliancy. The color-coded bar beneath remains static, showing a progression from lowest to highest compliancy.

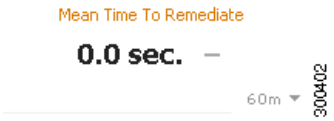
Figure 23-11 Posture Compliance Metric Meter



Mean Time to Remediate

The Mean Time to Remediate metric meter shows the average time that it takes for hosts that are connected to the network to move from a noncompliant state to a compliant state.

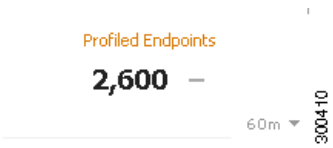
Figure 23-12 Mean Time to Remediate Metric Meter



Profiled Endpoints

The Profile Endpoints metric meter shows data representing the total number endpoints that have been profiled on the network for the last 24 hours, including those that are unknown.

Figure 23-13 Profiled Endpoints Metric Meter



Monitoring the Network

This section discusses the ways in which you can monitor your Cisco ISE network, and covers the following topics:

- Monitoring Network Process Status, page 23-10
- Managing Alarms, page 23-11
- Available Alarm Rules, page 23-18
- Monitoring Live Authentications, page 23-25
- Monitoring Data Collections, page 23-28

Monitoring Network Process Status

You can view process status for the network from the Cisco ISE dashboard using the System Summary dashlet. For example, when processes like the application server or database fail, an alarm is generated and you can view the results using the System Summary dashlet.

To view process status, complete the following steps:

Step 1 Select **System Summary** dashlet. A detailed real-time report appears.

Step 2 Review the following information for the processes that are running on the network:

- Name of the process
- CPU and memory utilization
- Time since process started running

For more information:

See Appendix A, "User Interface Reference."

Troubleshooting Topics

- Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8, page D-11

Managing Alarms

This section introduces Cisco ISE alarms, schedules, and rules which you can configure to effectively monitor your network. You can view them and specify alarms to notify you when critical system conditions occur. Notifications automatically appear in the Operations > Alarms > Inbox, but you can also receive notification of events through email and syslog messages.

This section covers the following topics:

- Understanding Alarms, page 23-11
- Viewing, Editing, and Resolving Alarms, page 23-13
- Viewing and Filtering Alarm Schedules, page 23-14
- Creating, Editing, and Deleting Alarm Schedules, page 23-15
- Creating, Assigning, Disabling, and Deleting Alarm Rules, page 23-16

Understanding Alarms

This section covers the basics of alarms and notifications, and covers alarm categories, schedules and rules (or thresholds), alarm notifications, alarm syslog targets, license enforcement alarms, and RADIUS authentication alerts.

There are two basic categories of alarms: alarm rules and system alarms. See Available Alarm Rules, page 23-18, for descriptions of the standard Cisco ISE alarm rules that you can customize for your network.

Default alarms include ISE AAA health, ISE process status, ISE system health, and ISE system diagnostics.

Alarm Rules

Alarm rules notify you of specified events in log data that is collected from ISE nodes. For example, you can configure alarm rules to notify you about system health, process status, and authentication activity or inactivity.

You define conditions, or rules, on data sets, the time period for applying the alarm rule, the severity of the alarm, and how the notifications should be sent. When alarm rule conditions are met, an alarm is triggered. There are many alarm rule categories that allow you to monitor various types of system behavior.

System Alarms

System alarms notify you of critical conditions that are encountered on the network. They also provide informational status of system activities, such as data purge events. You cannot create or delete system alarms, because they are predefined. However, you can configure how you want to be notified when they occur, or disable them entirely. When you enable system alarms, they are sent to the alarms inbox.

System alarms do not have an associated schedule and are sent immediately after an event occurs. You can only enable or disable system alarms as an entire group, not on an individual basis. For a list of the various types of system alarms and instructions on how to set them, see Configuring System Alarm Settings, page 23-54.

Schedules and Alarm Rules

A schedule consists of one or more continuous or noncontinuous periods you define when you create a alarm rule. For example, you can create a schedule that is active from 8:00 a.m. (0800) to 5:00 p.m. (1700) Monday through Friday. When you assign this schedule to an alarm rule, the rule is evaluated and the alarm is generated only during the specified active period.

Alarm rules are evaluated periodically, with the cycle frequency depending on the number of enabled rules. For example, if there are 1–20 enabled alarm rules, the evaluation cycle might occur every two (2) minutes. For 21–50 enabled rules, the evaluation cycle might occur every three (3) minutes, and 51–100 enabled rules every five (5) minutes.



Note There is a current limitation that restricts the number of rules to a maximum of 100.

When an evaluation cycle begins, each enabled alarm rule is evaluated. If the schedule allows the rule to be executed, the conditions are also evaluated. An alarm is triggered when the conditions of a specified rule are met.

Alarm Notifications

Alarm notifications are generated based on alarm rule conditions, and are evaluated over a specified time period, or schedule. An alarm notification is sent whenever a rule condition is reached or a system alarm is generated.

Alarm notifications are contained in the following locations:

- Alarm inbox—Contains the information that is on the alarm details page. The alarm details usually include one or more links to relevant reports to help you investigate the event that triggered the alarm. You can add comments, and change the status to indicate that it has been acknowledged or closed.

  The alarm inbox can contain up to 5000 alarms, the most recent alarms appearing at the top. Alarms that have been acknowledged or closed are removed from the list.

- Email notification—Contains the information that is on the alarm details page. You can configure a list of recipients, and you can indicate whether you wish to receive notifications in plaintext or HTML format.
- Syslog message—Sent to the Linux or Microsoft Windows machines that you have configured as alarm syslog targets. You can configure up to two alarm syslog targets.
- Alarm summary—Shows a listing of the most recent alarms in a pop-up window when you mouse over the Alarms icon in the right corner of the Global Toolbar at the bottom of the Cisco ISE window. Click an alarm link to view details of the alarm.

For more information, see Specifying Email Settings, page 23-53 and Configuring System Alarm Settings, page 23-54.

Alarm Syslog Targets

Alarm syslog targets are the destinations to which syslog messages are sent. Alarm notifications are sent in the form of syslog messages. You must have a configured syslog server on your network to receive syslog messages. For more information, see Configuring Alarm Syslog Targets, page 23-54.

License Enforcement Alarms

License enforcement alarms count concurrent endpoints or users and verify that number against the total amount that is allowed for a particular license. When the count exceeds the amount that is allowed by a license, a syslog is sent indicating that the license count has been exceeded.

Viewing, Editing, and Resolving Alarms

You can view alarms that met configured alarm rules in the alarms inbox or in the Global Toolbar slide-up window.

The alarm inbox displays a list of recent alarms, which you can select from to view the alarm details. After viewing information for an alarm, you can edit its status, assign the alarm to an administrator, and add notes to track the event.

The Global Toolbar shows the current number of alarms, and the slide-up window displays a read-only list of alarms.

Note Move your cursor over any field on the page to view context-sensitive help for the feature.

Viewing Alarm Summaries

You can view a list of recent alarms from the alarm summary window that you access from the global toolbar. The global toolbar is always available at the bottom of the Cisco ISE window.

To view a list of alarms, complete the following steps:

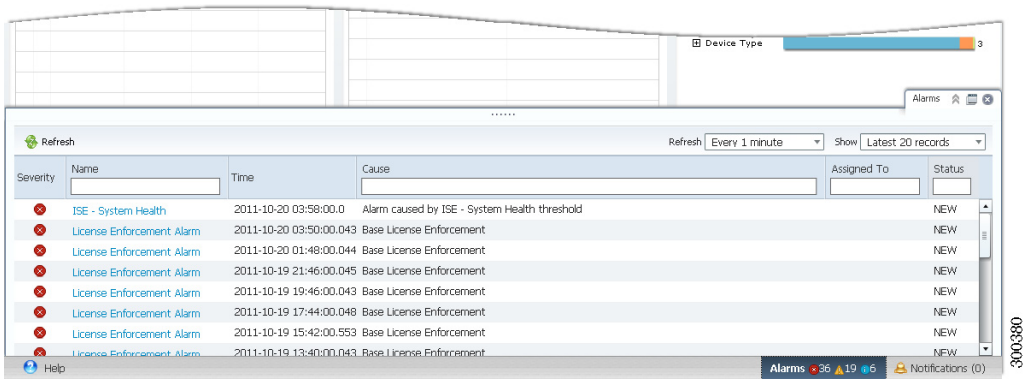
Step 1 Go to the toolbar at the bottom of the Cisco ISE window and move your mouse over the Alarms icon in the far-right corner. A slide-up window appears, showing a list of recent alarms.

Step 2 (Optional) Choose the **Refresh Rate** or **Show** options to modify the window display.

Step 3 (Optional) Choose the **Name**, **Cause**, **Assigned To**, or **Status** option. Enter the required information, and then click the arrow that appears in the right-hand corner of the field.

Step 4 Click the alarm link to view a detailed description of the event that prompted the alarm. A new page appears.

Figure 23-14 Alarm Summary Window



Using the Alarm Box to View, Edit, and Resolve Alarms

The following task shows you how to use the alarm inbox to view and edit alarms.

To view and edit an alarm in the alarm inbox, complete the following steps:

Step 1 Choose **Operations > Alarms > Inbox**. The Alarms Inbox page appears, with a list of the recent alarms.

Step 2 To view and edit an alarm, check the check box to the left of the alarm Name, and click **Edit**.

Step 3 To change the status of the alarm, click the **Status** tab and do the following:

a. Choose the appropriate option from the **Status** pull-down menu: **New**, **Acknowledged**, or **Closed**.

b. Assign the alarm to an administrator by entering a name or email address in the **Assigned** field.

c. Add any comments in the Notes field, and click **Submit**.

You are returned to the alarms inbox.

Step 4 To resolve an alarm, go back to the inbox, select the check box next to the alarm, and do one of the following:

- To close an alarm, click **Close**, enter Closing Notes in the dialog that appears, and click **Close** again.
- To delete an alarm, click **Delete**, and verify the action by clicking **Yes** in the dialog that appears.

Viewing and Filtering Alarm Schedules

You can view a list of all available alarm schedules, and then narrow the results by filtering for specified criteria.

Note Move your cursor over any field on the page to view context-sensitive help for the feature.

To view and filter alarm schedules, complete the following steps:

Step 1 Select **Operations > Alarms > Schedules**. A list of alarm schedules appears.

Step 2 To search for a specific type of alarm, enter the search criteria in the **Filter** field and click **Go**. The results are displayed.

Step 3 To return to the complete list of alarms, click **Clear**.

Creating, Editing, and Deleting Alarm Schedules

You can create alarm schedules to specify when alarm rules are run, and then edit and delete schedules as necessary. Alarm schedules can run at different times of the day throughout a seven-day (week) period. The default alarm schedule is nonstop, monitoring events 24 hours a day, 7 days a week.

Note Move your cursor over any field on the page to view context-sensitive help for the feature.

Creating an Alarm Schedule

The following task shows you how to create and save alarm schedules.

To create an alarm schedule, complete the following steps:

Step 1 Choose **Operations > Alarms > Schedules**.

Step 2 Click **Create**.

Step 3 In the appropriate fields, enter a unique name and a meaningful description to describe the schedule.

Step 4 Define the days and times for the schedule in one of the following ways:

- Click individual squares to select or deselect the hours and days of the alarm schedule. Squares fill with color when they are selected, and they are blank when they are deselected.

  Click **Clear All** or **Undo All** to clear the schedule and start again.
- Click **Select All** to create a nonstop alarm schedule that runs 24 hours a day, 7 days a week.

  Use **Clear All** or **Undo All** to clear the schedule and start again.

Step 5 Click **Submit** to save the schedule, or click **Cancel** to exit without creating a schedule.

If you submitted the schedule, it appears in the list of schedules.

Editing or Deleting an Alarm Schedule

The following task shows you how to edit and delete an alarm schedule.

To edit or delete an alarm schedule, complete the following steps:

Step 1 Select **Operations > Alarms > Schedules**. A list of schedules appears.

Step 2 Check the check box to the left of a schedule name, and do one of the following:

- To remove a selected alarm from the list, click **Delete**, and then click **Yes** to confirm the action.
- To modify a selected alarm, click **Edit**, and then do one of the following:
  - Select and deselect squares to modify the days and times. Squares fill with color when they are selected, and are blank when deselected.
  - Click **Clear All** or **Undo All** to clear the schedule and start again, defining a new schedule.
  - Click **Select All** to create a nonstop alarm schedule that runs 24 hours a day, 7 days a week.

Step 3 Click **Submit** to save your changes, or **Cancel** to exit without saving the changes.

Creating, Assigning, Disabling, and Deleting Alarm Rules

You define alarm rule conditions (also known as rules) on data sets, the time period for (applying) the alarm rule, the severity of the alarm, and how the notifications should be sent. Due to the time element, an alarm rule must be linked to an alarm schedule.

This section shows you how to create an alarm rule and assign it to a schedule. It then shows you how to delete an alarm rule.

Prerequisite

You should have created an alarm schedule, as described in Creating, Editing, and Deleting Alarm Schedules, page 23-15.

Creating and Assigning an Alarm Rule

One of the requirements for creating an alarm rule is that you assign it to a schedule. The following task shows you how to create an alarm rule, and then assign it to a schedule.

The following default alarm rules are shown in the user interface:

- ISE - AAA Health
- ISE - Process Status
- ISE - System Errors
- ISE - System Health

You can create these alarm rules using the following procedure:

- Passed Authentication
- Failed Authentication
- Authentication Inactivity
- Authenticated But No Accounting Start

- Unknown NAD
- External DB Unavailable
- RBACL Drops
- NAD-Reported AA Down

Note Move your cursor over any field on the page to view context-sensitive help for that feature.

To create an alarm rule and assign it to a schedule, complete the following steps:

Step 1 Choose **Operations > Alarms > Rules** and do one of the following:

- To create a copy of an existing alarm rule select the name of the rule, or the check box next to the name, and click **Duplicate**.
- To create a new rule, click **Create** and proceed with the rest of the steps in this task.

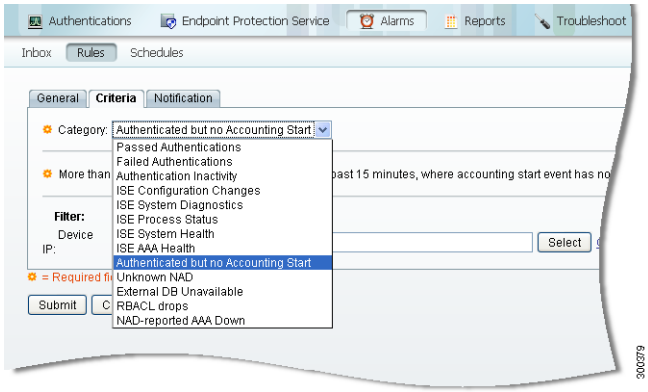
Step 2 On the General tab, enter a name and description for the alarm rule, and select a schedule from the drop-down list.

Step 3 Click the **Criteria** tab and do the following:

a. Select a rule category from the drop-down list.

b. Specify the required details for the category.

c. (*Optional*) Specify any other criteria, as desired.



Step 4 Click the **Notifications** tab and choose a severity level from the drop-down list. Then, specify Email Notification and Syslog Notification, as desired.

Step 5 Click **Submit** to create the rule, or click **Cancel** to quit without creating the rule.

For more information:

See Available Alarm Rules, page 23-18, for descriptions of the standard Cisco ISE alarm rules that you can customize for your network.

Disabling or Deleting an Alarm Rule

You can disable an alarm rule, which turns it off without removing it. Or you can delete the alarm rule entirely.

To disable or delete an alarm rule, complete the following steps:

Step 1 Choose **Operations > Alarms > Rules**.

Step 2 Select the check box next to the alarm rule you want to turn off or remove.

Step 3 To turn off the alarm rule, click **Disable**.

To turn back on a disabled alarm rule, select the check box next to the rule and click **Enable**.

Step 4 To permanently remove the selected alarm rule, click **Delete**. Then click **Yes** in the dialog prompt to finalize the action.

For more information:

See Available Alarm Rules, page 23-18, for descriptions of the standard Cisco ISE alarm rules that you can customize for your network.

Available Alarm Rules

Cisco ISE provides the following standard categories for alarm rules. You can use the following alarm rules in their default form, or customize them to meet your needs:

- Passed Authentication, page 23-19
- Failed Authentication, page 23-19
- Authentication Inactivity, page 23-20
- ISE Configuration Changes, page 23-20
- ISE System Diagnostics, page 23-21
- ISE Process Status, page 23-21
- ISE Health System, page 23-21
- ISE AAA Health, page 23-22
- Authenticated But No Accounting Start, page 23-22
- Unknown NAD, page 23-22
- External DB Unavailable, page 23-23
- RBACL Drops, page 23-24
- NAD-Reported AA Down, page 23-24

Passed Authentication

When Passed Authentication rules are evaluated, passed authentications (such as RADIUS) that occurred during a specified time interval (up to the previous 24 hours) are examined. These authentication records are grouped by a common attribute, such as instance, user, identity group, and so on. The number of records within each of these groups is computed. If the count for any of these groups exceeds the specified rule, an alarm is triggered.

For example, a rule that is configured for passed authentications greater than 1000 in the past 20 minutes for an instance is evaluated. The following table shows the three instances that passed authentications. An alarm was triggered, because at least one instance passed more than 1000 authentications in the past 20 minutes.

Cisco ISE Instance	Passed Authentication Count
New York Cisco ISE	1543
Chicago Cisco ISE	879
Los Angeles Cisco ISE	2096

For example, if you set up another rule for passed authentication less than 3 in the last 20 minutes for a user, the alarm will be generated if the passed authentication is less than 3, provided there was at least one authentication attempt. Zero is not considered as a value for alarm generation.

Note You can specify one or more filters to limit the passed authentications that are considered for rule evaluation. Each filter is associated with a particular attribute in the authentication records, and only the records with a filter value that matches the specified value are counted. If you specify multiple filters, only the records that match all the filter conditions are counted. You can modify the fields in the **Criteria** tab to create a rule with the passed authentication criteria.

For more information:

See Passed Authentications, page A-6 of Appendix A, "User Interface Reference."

Failed Authentication

When the Failed Authentication rule is evaluated, failed authentications (such as RADIUS) that occurred during a specified time interval (up to the previous 24 hours) are examined. These authentication records are grouped by a common attribute, such as Cisco ISE instance, user, identity group, and so on. The number of records within each of these groups is computed. If the count that is computed for any of these groups exceeds the specified rule, an alarm is triggered.

For example, the rule reflected in the table is configured with failed authentications greater than 10 in 2 hours for Device IP. If failed authentications have occurred for four IP addresses in the past two hours, such as shown in the following table, an alarm is triggered. At least one Device IP has greater than 10 failed authentications in the past 2 hours.

Device IP	Failed Authentication Count
a.b.c.d	13
e.f.g.h	8

Device IP	Failed Authentication Count
i.j.k.l	1
m.n.o.p	1

Note You can also modify the fields in the Criteria tab to create a rule with the failed authentication criteria.

You can specify one or more filters to limit the failed authentications that are considered for rule evaluation. Each filter is associated with a particular attribute in the authentication records, and only those records whose filter value matches the value that you specify are counted. If you specify multiple filters, only the records that match all the filter conditions are counted.

For more information:

See Failed Authentications, page A-8 of Appendix A, "User Interface Reference."

Authentication Inactivity

When the Authentication Inactivity rule is evaluated, it examines authentications (such as RADIUS) that occurred during a specified time interval, up to the previous 31 days. If no authentications have occurred, an alarm is triggered. You can specify filters to generate an alarm if no authentications are seen for a particular instance or device IP address during the time interval.

If the specified time interval for authentication inactivity is less than the time taken to complete an aggregation job, then the alarm is suppressed.

Note You can modify the fields in the Criteria tab to define rule criteria based on authentications that are inactive.

For more information:

See Authentication Inactivity, page A-9 of Appendix A, "User Interface Reference."

ISE Configuration Changes

The ISE Configuration Changes alarm is generated when configuration changes, such as adding, updating, or deleting a user or policy, and the like, are made to the server. Cisco ISE then examines the configuration changes made during the interval between the previous and current alarm evaluation cycles. If one or more changes were made, an alarm is triggered. For example, a new user is added, an existing user is updated, and another user is deleted, causing the alarm to be triggered. Installing new software can also trigger a configuration change alarm.

You can specify one or more filters to limit which configuration changes are considered for rule evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

For more information:

See ISE Configuration Changes, page A-9 of Appendix A, "User Interface Reference."

ISE System Diagnostics

When the ISE System Diagnostics rule is evaluated, the system diagnostic records that were generated during the specified interval are examined. If one or more diagnostics were generated at or above the specified security level, an alarm is triggered.

Note Cisco ISE system diagnostics are generated for internal operational diagnostic data, depending on the specified severity level.

You can specify one or more filters to limit which system diagnostic records are considered for rule evaluation. Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

For more information:

See ISE System Diagnostics, page A-10 of Appendix A, "User Interface Reference."

ISE Process Status

When the ISE Process Status rule is evaluated and one or more failures are detected, an alarm is triggered. You can limit the check to particular processes, a particular Cisco ISE instance, or both.

For example, when processes like the application server or database fail, an alarm is generated and you can view the results using the System Summary dashlet.

Note You can modify the fields in the Criteria tab to define rule criteria based on Cisco ISE process status.

For more information:

See ISE Process Status, page A-10 of Appendix A, "User Interface Reference."

ISE Health System

When the ISE Health System rule is evaluated, system health parameters are examined as a result of values exceeding the rule for a specified time interval (up to the previous 60 minutes). These health parameters include percentage of CPU utilization, percentage of memory consumption, and so on. If any parameters exceed the rule, an alarm is triggered. By default, the rule applies to all Cisco ISE instances. However, you can choose to limit the check to just a single Cisco ISE instance.

Note You can modify the fields in the Criteria tab to define rule criteria for Cisco ISE system health.

For more information:

See ISE System Health, page A-11 of Appendix A, "User Interface Reference."

ISE AAA Health

When the ISE AAA Health rule is evaluated, ISE health parameters that exceeded the rule for the specified time interval (up to the previous 60 minutes) are examined. Cisco ISE monitors the following parameters:

- RADIUS throughput
- RADIUS latency

If any of the parameters exceed the rule, an alarm is triggered. By default, the rule applies to all monitored Cisco ISE instances. However, you can choose to limit the check to just a single Cisco ISE instance.

Note You can modify the fields in the Criteria tab as needed.

For more information:

See ISE AAA Health, page A-11 of Appendix A, "User Interface Reference."

Authenticated But No Accounting Start

When the Authenticated But No Accounting Start rule is evaluated, it determines whether a specified number of authenticated sessions have occurred in the past 15 minutes, where an accounting start event has not been received for a device IP.

These events are grouped by device IP address. If the occurrences for a device IP exceeds the specified of the rule, an alarm is triggered. You can set a filter to limit the evaluation to a single device IP.

Note You can modify the fields in the Criteria tab to define rule criteria for authenticated sessions for a device IP.

For more information:

See Authenticated But No Accounting Start, page A-12 of Appendix A, "User Interface Reference."

Unknown NAD

When the Unknown NAD rule is evaluated, the RADIUS failed authentications that occurred during the specified time interval (up to the previous 24 hours) are examined. The failed authentications with the failure reason "unknown NAD" are identified. The unknown NAD authentication records are grouped by a common attribute, such as Cisco ISE instance, user, and so on. A count of the records within each of the groups is computed, and if the records for any group exceed the specified rule, an alarm is triggered.

Take the following rule for example: Unknown NAD count greater than 5 in the past 1 hour for a Device IP

In our example, after one hour, the failed authentications with an "unknown NAD" failure reason occur for two different device IP addresses. An alarm is triggered as a result, because at least one device IP address has a count greater than 5. The following table shows the data for this example.

Device IP	Count of Unknown NAD Authentication Records
a.b.c.d	6
e.f.g.h	1

You can specify one or more filters to limit failed authentications that are considered for rule evaluation. Each filter is associated with an attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Note You can modify the fields in the Criteria tab to define rule criteria based on authentications that have failed because of an unknown NAD.

For more information:

See Unknown NAD, page A-12 of Appendix A, "User Interface Reference."

External DB Unavailable

When the External DB Unavailable rule is evaluated, RADIUS failed authentications that occur during a specified time interval (up to the previous 24 hours) are examined. The failed authentications with the "external DB unavailable" failure reason are then determined. Authentication records with this failure reason are grouped by a common attribute, such as Cisco ISE instance, user, and so on. A count of the records within each of these groups is computed. If the count of records for any group exceeds the rule, an alarm is triggered.

Take the following rule for example: External DB Unavailable count greater than 5 in the past 1 hour for a Device IP

In our example, after one hour, the failed authentications with an "external DB unavailable" failure reason occur for two different device IP addresses. An alarm is triggered, because at least one device IP address has a count greater than 5. The following table shows the data for this example.

Device IP	Count of External DB Unavailable Authentication Records
a.b.c.d	6
e.f.g.h	1

You can specify one or more filters to limit the failed authentications considered for rule evaluation. Each filter is associated with an attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Note You can modify the fields in the Criteria tab to define rule criteria based on an external database to which Cisco ISE is unable to connect.

For more information:

See External DB Unavailable, page A-13 of Appendix A, "User Interface Reference."

RBACL Drops

When the RBACL Drops rule is evaluated, Security Group Access RBACL drops that occurred during a set time interval (up to the previous 24 hours) are examined. The RBACL drop records are grouped by a particular common attribute, such as NAD, SGT, and so on. The number of records for group is computed. If the count for any group exceeds the rule, an alarm is triggered.

Take the following rule for example: RBACL drops greater than 10 in the past 4 hours by an SGT

In our example, RBACL drops occur for two different source group tags in a four-hour period. An alarm is triggered, because at least one SGT has a count greater than 10. The following table shows the data for this example.

SGT	Count of RBACL Drops
1	17
3	14

You can specify one or more filters to limit the RBACL drop records that are considered for rule evaluation. Each filter is associated with a particular attribute in the RBACL drop records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Note You can modify the fields in the Criteria tab to define the RBACL Drops rule.

For more information:

See RBACL Drops, page A-13 of Appendix A, "User Interface Reference."

NAD-Reported AA Down

For the NAD-Reported AAA rule, NAD-reported AAA down events occurring during a specified interval (up to the previous 24 hours) are examined. The AAA down records are then grouped by a particular common attribute, such as device IP address or device group, and a count of records within each group is made. If the count for any group exceeds the specified rule, an alarm is triggered.

Take, for example, the following rule configuration: AAA down count greater than 10 in the past 4 hours by a Device IP

In our example, in the past 4 hours, NAD-reported AAA down events occurred for 3 different device IP addresses, triggering an alarm because at least one device IP address has a count greater than 10. The following table shows the data for this example.

Device IP	Count of NAD-Reported AAA Down Events
a.b.c.d	15
e.f.g.h	3
i.j.k.l	9

You can specify one or more filters to limit the AAA down records, that are considered for rule evaluation. Each filter is associated with a particular attribute in the AAA down records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Note You can modify the fields in the Criteria tab to define rule criteria based on the AAA downtime that a network access device reports.

For more information:

See NAD-Reported AAA Downtime, page A-14 of Appendix A, "User Interface Reference."

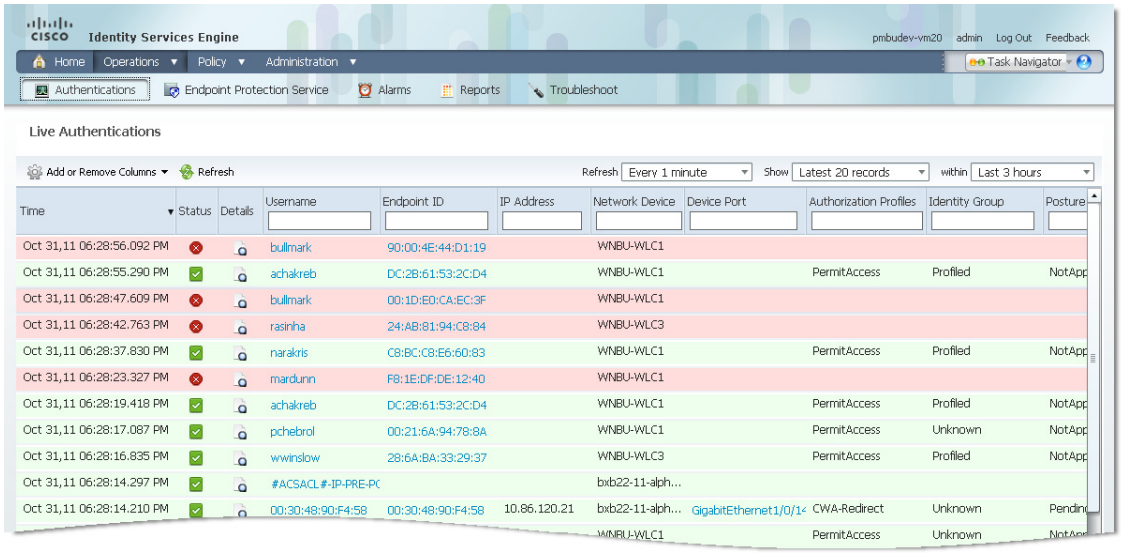
Monitoring Live Authentications

You can monitor recent RADIUS authentications as they happen from the Live Authentications page. The page displays the top 10 RADIUS authentications in the last 24 hours. This section explains the functions of the Live Authentications page.

The Live Authentications page provides a tabular account of recent RADIUS authentications, in the order in which they happen.

Note The Last update shown at the bottom of the Live Authentications page shows the current server date, time, and timezone.

Figure 23-15 Live Authentications Page



The Live Authentication data categories that are shown by default include the following:

- **Time**—Shows the time that the log was received by the collection agent. This column is required and cannot be deselected.
- **Status**—Shows if the authentication was successful or a failure. This column is required and cannot be deselected.
- **Details**—Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more-detailed information on the selected authentication scenario. This column is required and cannot be deselected.
- **Username**—Shows the username that is associated with the authentication.
- **Endpoint ID**—Shows the unique identifier for an endpoint, usually a MAC or IP address.
- **IP Address**—Shows the IP address of the endpoint device.
- **Network Device**—Shows the IP address of the network access device.
- **Device Port**—Shows the port number at which the endpoint is connected.
- **Authorization Profiles**—Shows an authorization profile that was used for authentication.
- **Identity Group**—Shows the identity group that is assigned to the user or endpoint, for which the log was generated.
- **Posture Status**—Shows the status of posture validation and details on the authentication.
- **Event**—Shows the event status.
- **Failure Reason**—Shows a detailed reason for failure, if the authentication failed.

Optionally, you can choose to show the following categories:

- **Auth Method**—Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2), IEE 802.1x or dot1x, and the like.
- **Authentication Protocol**—Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.
- **Security Group**—Shows the group that is identified by the authentication log.
- **Server**—Indicates the Policy Service from which the log was generated.
- **Session ID**—Shows the session ID.

You can choose to view all of the columns, or to display only selected data columns. After selecting the columns that you want to appear, you can save your selections.

To access and modify the Live Authentications display, complete the following steps:

Step 1 Choose **Operations > Authentications**. The Live Authentications page appears.

Step 2 To change the data refresh rate, select a time interval from the drop-down menu.

Step 3 To manually update the data, click the **Refresh** icon on the Live Authentications menu bar.

Step 4 To change the number of records that appear, choose one of the following from the **Show** drop-down menu: Latest 20 Records, Latest 50 Records, Latest 100 Records.

Step 5 To specify a time interval, choose one of the following from the **within** drop-down menu:

- Last 24 hours (the default)
- Last 12 hours
- Last 6 hours
- Last 3 hours
- Last 60 minutes
- Last 30 minutes
- Last 10 minutes
- Last 5 minutes
- Last 60 seconds

Step 6 To change the columns that are shown, click **Add or Remove Columns**, and from the drop-down menu, do any of the following:

- Deselect a check box to remove the column from the display. The check mark disappears.

Note The Time, Status, and Details columns are essential and cannot be deselected.

- Select an empty check box to add the column to the display.
- Select **Restore to Default** to reset the display to the default set of columns.
- Select **Show All Columns** to automatically display all columns. The changes appear automatically.

Step 7 Click **Save** at the bottom of the drop-down menu to save your modifications, or click **Cancel** to discard your changes.

Troubleshooting Topics

- RADIUS Accounting Packets (Attributes) Not Coming from Switch, page D-5
- RADIUS Server Error Message Entries Appearing in Cisco ISE, page D-14
- RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE), page D-15

Monitoring Guest Activity

A guest is a type of user that has limited permissions, such as restricted network access and time duration. For example, a guest might not have access to the company's internal network, and the account expires after eight hours.

You can monitor guests that are currently on the network through the authentications that are generated by these accounts. One way to do this would be to set alarm rules for all users of type guest, and then monitor the live authentications.

To monitor guest activity, complete the following steps:

Step 1 Create an alarm, as described in Creating, Editing, and Deleting Alarm Schedules, page 23-15.

Step 2 Specify a rule for Passed Authentication, page 23-19, Failed Authentication, page 23-19, or Authentication Inactivity, page 23-20 for all users of type guest, as described in Creating and Assigning an Alarm Rule, page 23-16.

Step 3 Calculate guest user activity by Monitoring Live Authentications, page 23-25.

Troubleshooting Topics

- RADIUS Accounting Packets (Attributes) Not Coming from Switch, page D-5
- RADIUS Server Error Message Entries Appearing in Cisco ISE, page D-14
- RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE), page D-15

Monitoring Data Collections

Monitoring functionality collects log and configuration data from nodes on your Cisco ISE network, stores the data in the Monitoring database, and processes it to generate reports and alarms. You can view the details of the logs that are collected from any of the servers in your deployment.

To monitor data collections for system performance and health, complete the following steps:

Step 1 Follow the procedure for Creating, Editing, and Deleting Alarm Schedules, page 23-15.

Step 2 Follow the procedure for Creating, Assigning, Disabling, and Deleting Alarm Rules, page 23-16 using any combination of the following alarm rules:

- ISE System Diagnostics, page 23-21
- ISE Process Status, page 23-21
- ISE Health System, page 23-21
- ISE AAA Health, page 23-22

Step 3 Follow the procedure for Specifying Email Settings, page 23-53.

Step 4 Follow the procedure for Configuring Alarm Syslog Targets, page 23-54.

Step 5 Follow the procedure for Viewing Log Collections, page 23-53.

For more information:

See the Alarms, page A-3 of Appendix A, "User Interface Reference."

Troubleshooting Topics

- RADIUS Accounting Packets (Attributes) Not Coming from Switch, page D-5
- RADIUS Server Error Message Entries Appearing in Cisco ISE, page D-14
- RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE), page D-15

Troubleshooting the Network

This section covers the following topics:

- Viewing and Editing Failure Reasons, page 23-29
- Troubleshooting Network Access, page 23-29
- Performing Connectivity Tests, page 23-30
- Using Diagnostic Troubleshooting Tools, page 23-31

Viewing and Editing Failure Reasons

The Failure Reason Editor allows you to view and edit the description of a failure reason, as well as providing instructions on how to resolve the problem.

To view and edit failure reasons, complete the following steps:

Step 1 Choose **Administration > System > Settings.**

Step 2 In the navigation panel on the left, expand **Monitoring** and select **Failure Reason Editor**. A list of failure reasons appears in the right panel.

Step 3 To view a failure reason, do one of the following:

- Select a radio button or name link for a failure reason from the list.
- Enter a text string in the Filter text box, click **Filter**, and select a failure from the results.

Step 4 To edit a failure reason, do the following:

a. Click the radio button to the left of the name. The button turns green when selected.

b. Click **Edit**.

c. In the appropriate field, enter or modify a description, then enter or modify resolution steps.

d. Click **Submit** to save your changes, or click **Cancel** to quit without saving any changes.

For more information:

See Troubleshoot, page A-40 of Appendix A, "User Interface Reference."

Troubleshooting Network Access

You can troubleshoot network access for a specific user, device, or search criteria based on attributes that are related to the authentication requests. You do this by running an Authentication Failure Code Lookup report.

Note If the MAC address value that you provide is not in the prescribed format, it is assumed to be a username, and a user authentication summary report is run for the chosen time range and protocol.

To troubleshoot network access based on authentication requests, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog**.

Step 2 In the Reports list panel on the left, choose **Failure Reason**.

Step 3 In the panel on the right, click the radio button next to **Authentication Failure Code Lookup**.

Step 4 Follow the instructions described in Running, Viewing, and Navigating Reports, page 24-3, and consider the following:

- If you provide the Username or MAC Address value in the format aa-bb-cc-dd-ee-ff, the report is run for this MAC address.
- If you provide the Username or MAC Address value in any other format, the value is considered a username, and the report is run for that user.
- If you leave the Username or MAC Address field empty, a report using the default parameters is run for the chosen protocol and time range (similar to running a RADIUS authentication report in the catalog pages).
- If you provide a valid MAC address value for the Username or MAC Address field and choose the Summary View option, an endpoint summary report is run. Irrespective of the protocol that you choose, an endpoint summary report is always run for the RADIUS protocol.

Step 5 Review the report data to troubleshoot your network access problem.

For more information:

See Troubleshooting RADIUS Authentications, page 23-31.

Performing Connectivity Tests

Failed authentications can be caused by connection problems. Troubleshooting tools functionality allows you to perform connectivity tests to check for connectivity issues. You can enter the hostname or the IP address of the network device with which you are trying to connect and execute the following commands from the web interface: **ping**, **traceroute**, and **nslookup**. The output is displayed in the dashboard window.

To perform connectivity tests, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel on the left, select **General Tools > Connectivity Tests**.

Step 3 In the appropriate field, enter the hostname or IP address for a connection that you want to test.

Step 4 Do any of the following:

- Click **Ping** to view the packets sent and received, packet loss (if any), and the time it takes for the test to complete.
- Click **Traceroute** to view the intermediary IP addresses (hops) between the Cisco ISE node and the specified hostname or IP address, and the time it takes for each hop to complete.

- Click **Nslookup** to view the server and IP address of your tested domain name server hostname or IP address.

For more information:

See Policy, page A-54 of Appendix A, "User Interface Reference."

Using Diagnostic Troubleshooting Tools

Diagnostic Tools help you to diagnose and troubleshoot problems on an Cisco ISE network. Detailed instructions on how to resolve the problem is also provided. You can use these tools to evaluate the configuration of any network device on your network, including Security Group Access devices, and troubleshoot passed and failed authentications.

This section covers the following diagnostic procedures:

- Troubleshooting RADIUS Authentications, page 23-31
- Executing a Network Device Command, page 23-33
- Evaluating a Network Device Configuration, page 23-33
- Troubleshooting Posture Data, page 23-34
- Troubleshooting with TCP Dump, page 23-35
- Comparing SGACL Policies, page 23-37
- Comparing SXP-IP Mappings, page 23-38
- Comparing IP-SGT Pairs, page 23-38
- Comparing SGT Devices, page 23-39

Troubleshooting RADIUS Authentications

Use the RADIUS Authentication diagnostic tool to troubleshoot RADIUS authentications issues.

To search and select a RADIUS authentication for troubleshooting, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel at the left, select then select **General Tools > RADIUS Authentication Troubleshooting**.

Step 3 Specify the following information:

- Username—Enter the username of the user whose authentication you want to troubleshoot, or click **Select** to choose the username from a list.
- MAC address—Enter the MAC address of the device that you want to troubleshoot, or click **Select** to choose the MAC address from a list.
- Audit Session ID—Enter the audit session ID that you want to troubleshoot.
- NAS IP—Enter the NAS IP address, or click **Select** to choose the NAS IP address from a list.
- NAS Port—Enter the NAS port number, or click **Select** to choose a NAS port number from a list.

- Authentication Status—Choose the status of your RADIUS authentication from the Authentication Status drop-down list. The available options are as follows:
  - Pass or Fail
  - Pass
  - Fail
- Time Range—Select a time range from the drop-down list.

Note If you selected a Custom time range, specify the Start Date-Time and End Date-Time.

- Failure Reason—View and edit the description of a failure reason.
- Fetch Number of Records—Choose the number of records that you want to fetch from the drop-down list: 10, 20, 50, 100, 200, or 500.

Step 4 Click **Search** to display the RADIUS authentications that match your search criteria.

The Search Result table is populated with the results of your search. The following fields appear in the table: Time, Status, Username, MAC Address, Audit Session ID, Network Device IP, Failure Reason, and Allowed Protocol.

Step 5 Select a RADIUS authentication record from the table and click **Troubleshoot**.

The Expert Troubleshooter begins to troubleshoot your RADIUS authentication. You are prompted for additional input, if required.

Step 6 Click **User Input Required**, modify the fields as needed, and then click **Submit**.

The Progress Details page appears, providing a summary. You may be prompted for additional input, if required. If additional input is required, click **User Input Required** and enter the necessary information.

Step 7 Click **Done**.

The Progress Details page refreshes periodically, displaying tasks that are performed as troubleshooting progresses.

Step 8 After the troubleshooting is complete, click **Show Results Summary**.

Step 9 Click **Done** to return to view a diagnosis, steps to resolve the problem, and troubleshooting summary.

For more information:

See RADIUS Authentication Troubleshooting—Progress Details, page A-42 of Appendix A, "User Interface Reference."

Troubleshooting Topics

- RADIUS Accounting Packets (Attributes) Not Coming from Switch, page D-5
- RADIUS Server Error Message Entries Appearing in Cisco ISE, page D-14
- RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE), page D-15

Executing a Network Device Command

The Execute Network Device Command diagnostic tool allows you to run the **show** command on any network device from the centralized Cisco ISE dashboard. The results are exactly what you would see on a console, and can be used to identify problems in the configuration of the device.

To run the show command on any network device, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel on the left, choose **General Tools > Execute Network Device Command**.

Step 3 Enter the following information in the appropriate fields:

- Network Device IP—The IP address of the network device
- Command—A **show** command, such as **show run** or **show vlan**

Step 4 Click **Run** to execute the command on the specified network device. The Progress Details page appears, prompting you for additional input.

Step 5 Click **User Input Required**, and modify the fields as necessary.

Step 6 Click **Submit** to run the command on the network device, and view the output.

For more information:

See Progress Details, page A-44 of Appendix A, "User Interface Reference."

Evaluating a Network Device Configuration

You can use this diagnostic tool to evaluate the configuration of a network device and identify any configuration problems. The Expert Troubleshooter compares the configuration of the device with the standard configuration.

To evaluate the configuration of a network device, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel on the left, choose **General Tools > Evaluate Configuration Validator**.

Step 3 Enter the Network Device IP address of the device whose configuration you want to evaluate, and specify other fields as necessary.

Step 4 Select configuration options to compare against the recommended template. A green check mark means the option is selected. Click the option again to deselect. Choose from the following:

- Web Authentication—Check this check box to compare the web authentication configuration.
- Profiler Configuration—Check this check box to compare the Profiler configuration.
- CTS—Check this check box if you want to compare Security Group Access configuration.
- 802.1X—Check this check box if you want to compare the 802.1X configuration, and choose one of the following options:
  - Open Mode
  - Low Impact Mode (Open Mode + ACL)

- High Security Mode (Closed Mode)

Step 5 Click **Run**. The Progress Details page appears, prompting you for additional input.

Step 6 Click **User Input Required**, and modify the fields as necessary.

A new window appears, prompting you to select the interfaces for the configuration analysis.

Step 7 Check the check boxes next to the interfaces that you want to analyze, and click **Submit**. The Progress Details page appears.

Step 8 Click **Show Results Summary**.

For more information:

See Progress Details, page A-44 of Appendix A, "User Interface Reference."

Troubleshooting Posture Data

The Posture Troubleshooting tool helps you find the cause of a posture check failure to identify the following:

- Which endpoints were successful in posture and which were not.
- If an endpoint failed in posture, what steps failed in the posture process.
- Which mandatory and optional checks passed and failed.

You determine this information by filtering requests based on parameters, such as username, MAC address, posture status, and so on.

To troubleshoot posture incidents, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel on the left, choose **General Tools > Posture Troubleshooting**.

Step 3 Specify the following parameters:

- Username—Enter the username to filter on.
- MAC Address—Enter the MAC address to filter on, using format: xx-xx-xx-xx-xx-xx
- Posture Status—Select one of the following authentication status filters:
  - Any
  - Compliant
  - Noncompliant
  - Unknown
- Failure Reason—Enter the failure reason, or click **Select** to choose a failure reason from a list.
- Time Range—Select a time range filter from the drop-down list.

Note If you selected a Custom time range, specify the Start Date-Time and End Date-Time.

- Fetch Number of Records—Select the number of records you want displayed at one time from the drop-down list: 10, 20, 50, 100, 200, or 500.

Step 4 Click **Search**.

The search results appear in the window, displaying time, status, username, MAC address, and failure reason for each event.

Step 5 To find an explanation and determine a resolution for an event, select the event in the list and click **Troubleshoot**.

For more information:

See Egress SGACL Policy, page A-48 of Appendix A, "User Interface Reference."

Troubleshooting with TCP Dump

The tcpdump utility monitors the contents of packets on a network interface that match a given boolean expression. You can use the tcpdump utility to troubleshoot problems on your network. Cisco ISE troubleshooting diagnostic tools provide an intuitive user interface for this utility.

This section shows you how to use the TCP Dump feature directly from the Cisco ISE dashboard, and covers the following topics:

- Monitoring and Saving Packets, page 23-35
- Saving a Dump File, page 23-36

Warning **Starting a TCP Dump automatically deletes a previous dump file. To save a previous dump file, perform the Saving a Dump File, page 23-36 before you begin a new TCP Dump session.**

Monitoring and Saving Packets

This procedure shows you how to configure TCP Dump options and then collect data from the network traffic to help you troubleshooting a network issue.

To monitor packets on the network, complete the following steps:

Step 1 Select **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the left-hand navigation pane, select **General Tools > TCP Dump**.

Step 3 Select a **Network Interface** to monitor from the drop-down menu.

This is the interface upon which the network traffic is monitored, or sniffed.

Step 4 Set Promiscuous Mode to **On** or **Off** by clicking the radio button. The default is On.

Promiscuous mode is the default packet sniffing mode. It is recommended that you leave it set to On. In this mode the network interface is passing all traffic to the system's CPU.

Step 5 In the Filter field, enter a boolean expression on which to filter.

Standard tcpdump filter expressions are supported, such as the following:

host 10.0.2.1 and port 1812

Step 6 Click **Start** to begin monitoring the network.

Note An In Progress status appears when you start the utility. You can navigate to another page in the user interface and later return. The In Progress status displays how many bytes generated so far, and is updated every 30 seconds until the process ends or you manually stop the process.

The date, time, format, and size of the file are shown at the bottom of the pane.

Step 7 Click **Stop** when you have collected a sufficient amount of data, or wait for the process to conclude automatically after accumulating the maximum number of packets (500,000).

Note You must have Adobe Flash Player installed on the Administration ISE node to be able to view the tcpdump.

Next Step

- Saving a Dump File, page 23-36

Troubleshooting Topics

- Policy Service ISE Node Not Passing Traffic, page D-6

Saving a Dump File

This procedure shows you how to save a dump file that you can use for troubleshooting purposes.

Prerequisite

You should have successfully completed Monitoring and Saving Packets, page 23-35.

To download a previous dump file, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

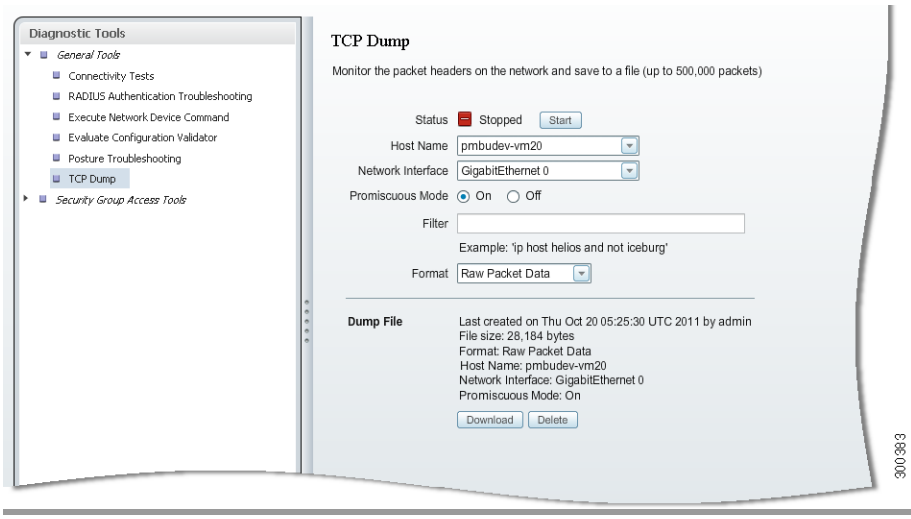
Step 2 In the left-hand navigation pane, select **General Tools > TCP Dump**.

Step 3 Select a Format from the drop-down menu. Human Readable is the default.

Step 4 Click **Download**, navigate to the desired location and then click **Save**.

Step 5 To get rid of the previous dump file without saving it first, click **Delete**.

Figure 23-16 TCP Dump



Note You can also access tcpdump through the Cisco ISE command line interface (CLI). For more information, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

Comparing SGACL Policies

For devices that are enabled with the Security Group Access solution, an SGACL is assigned for every source and destination SGT pair based on the egress policy matrix that is configured in Cisco ISE. The egress policy diagnostic tool uses the following process for its comparison:

1. Connects to the device with IP address that you provided, and obtains the access control lists (ACLs) for each source and destination SGT pair.
2. Checks the egress policy that is configured in Cisco ISE and obtains the ACLs for each source and destination SGT pair.
3. Compares the SGACL policy that is obtained from the network device with the SGACL policy that is obtained from Cisco ISE.
4. Displays the source and destination SGT pair if there is a mismatch. Also, displays the matching entries as additional information.

To compare SGACL policies using the Egress (SGACL) Policy tool, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel on the left, select **Security Group Access Tools > Egress (SGACL) Policy**.

Step 3 Enter the **Network Device IP** address of the Security Group Access device whose SGACL policy you want to compare.

Step 4 Click **Run**. The Progress Details page appears, prompting you for additional input.

Step 5 Click **User Input Required** and modify the fields as necessary.

Step 6 Click **Submit**. The Progress Details page appears with a brief summary of the results.

Step 7 Click **Show Results Summary** to view the diagnosis and suggested resolution steps.

For more information:

See Egress SGACL Policy, page A-48 of Appendix A, "User Interface Reference."

Comparing SXP-IP Mappings

Security Group Access devices communicate with their peers and learn their SGT values. The Security Exchange Protocol (SXP)-IP Mappings diagnostic tool connects to the device whose IP address you provide and lists the IP addresses of the peer devices and SGT values. You must select one or more of the device peers. This tool connects to each of the peers that you select, and it obtains their SGT values to verify that these values are the same as the values that it learned earlier.

To compare SXP-IP mappings between a device and its peers, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel on the left, choose **Security Group Access Tools > SXP-IP Mappings**.

Step 3 Enter the network device IP address of the network device, and click **Select**.

Step 4 Click **Run**, and then click **User Input Required** and modify the necessary fields.

The Expert Troubleshooter retrieves Security Group Access SXP connections from the network device and again prompts you to select the peer SXP devices.

Step 5 Click **User Input Required**, and enter the necessary information.

Step 6 Check the check box of the peer SXP devices for which you want to compare SXP mappings, and enter the common connection parameters.

Step 7 Click **Submit**. The Progress Details page appears with a brief summary of the results.

Step 8 Click **Show Results Summary** to view the diagnosis and resolution steps. The Results Summary page appears.

For more information:

See SXP-IP Mappings, page A-49 of Appendix A, "User Interface Reference."

Comparing IP-SGT Pairs

For devices that are enabled with the Security Group Access solution, each user is assigned an SGT value through RADIUS authentication. The IP User SGT diagnostic tool connects to the network device (whose IP address you provide) and performs the following tasks:

1. Obtains a list of all IP-SGT assignments on the network device.
2. Checks the RADIUS authentication and accounting records for each IP-SGT pair to find out the IP-SGT-User value that assigned most recently.
3. Displays the IP-SGT pairs in a tabular format, and identifies whether the SGT values that were most recently assigned and those that are on the device are the same or different.

To compare IP-SGT values on a device with the most assigned SGT, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel on the left, select **Security Group Access Tools > IP User SGT**.

Step 3 Specify the following:

- **Network Device IP**—Enter the IP address of the network device.
- **Username**—Enter the username of the user whose records you want to troubleshoot.
- **User IP Address**—Enter the IP address of the user whose records you want to troubleshoot.
- **SGT**—Enter the user SGT value.

Step 4 Click **Run**. You are prompted for additional input.

Step 5 Click **User Input Required**, and modify the fields as necessary, and then click **Submit**.

Step 6 Click **Show Results Summary** to view the diagnosis and resolution steps.

For more information:

See IP User SGT, page A-51 of Appendix A, "User Interface Reference."

Comparing SGT Devices

For devices that are enabled with the Security Group Access solution, each network device is assigned an SGT value through RADIUS authentication. The Device SGT diagnostic tool connects to the network device (whose IP address you provide) and performs the following tasks:

1. Obtains the network device SGT value.
2. Checks the RADIUS authentication records to determine the SGT value that was assigned most recently.
3. Displays the Device-SGT pairs in a tabular format, and identifies whether the SGT values are the same or different.

To compare the device SGT with the recently assigned SGT value, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Diagnostic Tools**.

Step 2 In the panel on the left, choose **Security Group Access Tools > Device SGT**.

Step 3 Specify the following:

- Network Device IPs—Enter the network device IP addresses (whose device SGT you want to compare with a Cisco ISE-assigned device SGT) separated by commas.
- Use Common Connection Parameters—Select this check box to use the following common connection parameters for comparison:
  - Username—Enter the username of the network device.
  - Password—Enter the password.
  - Protocol—Choose the protocol from the Protocol drop-down list box. Valid options are: Telnet and SSHv2. Telnet is the default option. If you choose SSHv2, SSH connections must be enabled on the network device.
  - Port—Enter the port number. The default port number for Telnet is 23 and SSH is 22.
- Enable Password—Enter the enable password if it is different from your login password.
- Same as login password—Select this check box if your enable password is the same as your login password.

Step 4 Click **Run**.

Step 5 Click **Show Results Summary** to view the results of the device SGT comparison.

The Results Summary page appears with the diagnosis, resolution, and troubleshooting summary.

For more information:

See Device SGT, page A-53 of Appendix A, "User Interface Reference."

Obtaining Additional Troubleshooting Information

Cisco ISE allows you to download support and troubleshooting information from the administrative user interface. You can use the support bundle to prepare diagnostic information for the Cisco Technical Assistance Center (TAC) to troubleshoot problems with Cisco ISE.

Note The support bundles and debug logs provide advanced troubleshooting information for Cisco TAC and are difficult to interpret. You can use the various reports and troubleshooting tools that Cisco ISE provides to diagnose and troubleshoot issues that you are facing in your network. See "Troubleshooting the Network" section on page 23-29 for more information.

This section contains the following topics:

- Downloading Support Bundles, page 23-40
- Downloading Debug Logs, page 23-43

Downloading Support Bundles

You can download the support bundle to your local computer as a simple tar.gz file. The support bundle will be named with the date and time stamps in the format ise-support-bundle-*mm-dd-yyyy-hh-mm.tar.gz*. The browser prompts you to save the support bundle to an appropriate location.

You can configure the logs that you want to be part of your support bundle. For example, you can configure logs from a particular service to be part of your debug logs. See the "Understanding Debug Log Configuration" section on page 14-8 for more information.

The logs that you can download are categorized as follows:

- Full configuration database—The Cisco ISE configuration database is downloaded in a human readable XML format. When you are trying to troubleshoot issues, you can import this database configuration in another Cisco ISE node to recreate the scenario.
- Debug logs—Captures bootstrap, application configuration, run time, deployment, monitoring and reporting, and public key infrastructure (PKI) information.

  Debug logs provide troubleshooting information for specific ISE components. See the "Downloading Debug Logs" section on page 23-43 for more information. To enable debug logs, see Chapter 14, "Logging". If you do not enable the debug logs, all the informational messages (INFO) will be included in the support bundle.
- Local logs—Contains syslog messages from the various processes that run on Cisco ISE.
- Core files—Contains critical information that would help identify the cause of a crash. These logs are created when the application crashes and includes heap dumps.
- Monitoring and reporting logs—Contains information about the alerts and reports.
- System logs—Contains Cisco Application Deployment Engine (ADE)-related information.

You can download these logs from the Cisco ISE CLI by using the **backup-logs** command. For more information, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.*

Note For Inline Posture nodes, you cannot download the support bundle from the Cisco ISE user interface. You must use the **backup-logs** command from the Cisco ISE CLI to download logs for Inline Posture nodes.

If you choose to download these logs from the administrative user interface, you can do the following:

- Download only a subset of logs based on the log type such as debug logs or system logs.
- Download only the latest "*n*" number of files for the selected log type. This option allows you to control the size of the support bundle and the time taken for download.

Monitoring logs provide information about the monitoring, reporting, and troubleshooting features.

Prerequisite:

To perform the operations that are described in the following procedure, you must have Super Admin or System Admin privileges. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges that are associated with each of them.

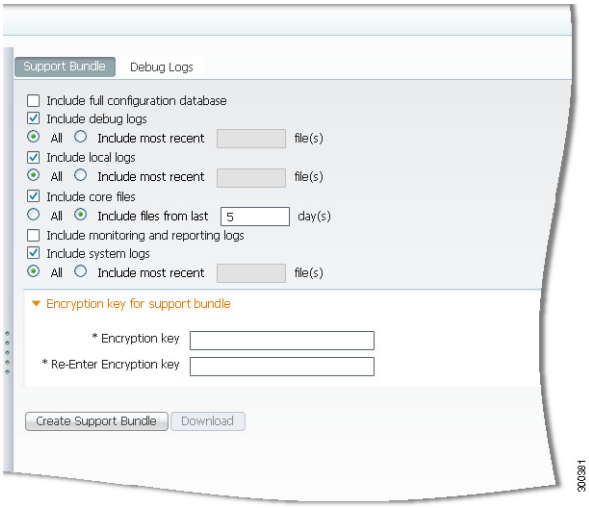
To download support bundles, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Download Logs**.

Step 2 From the Appliance node list navigation pane on the left, choose the node from which you want to download the support bundles.

The Support Bundle page appears, as shown in Figure 23-17 appears. Your support bundle is populated with the parameters that you choose. For specific instructions on Debug Logs, see "Downloading Debug Logs" section on page 23-43.

Figure 23-17 Download Logs Parameters



Step 3 Check the check boxes next to the logs that you want to download, and then specify one of the following, as appropriate:

- **All** to include all the selected log files
- **Include most recent** and enter the number of files to include
- **Include files from last** and enter the number of days

If you include all the logs, your support bundle will be excessively large and the download will take a lot of time. To optimize the download process, choose to download only the most recent *n* number of files.

Step 4 Enter the encryption key for the support bundle, and then re-enter the encryption key.

Step 5 Click **Create Support Bundle**.

Step 6 Click **Download** to download the newly created support bundle.

The support bundle is a zip file that is downloaded to the client system that is running your application browser. You must extract the contents of the zip file and untar the tar.gz file to view the logs.

Next Step:

See "Downloading Debug Logs" procedure on page 23-43 for information on how to obtain debug logs for specific components.

Downloading Debug Logs

Debug logs provide troubleshooting information for various Cisco ISE components. While reporting problems, you might be asked to enable these debug logs on ISE and send these logs for diagnosis and resolution of your problems.

Obtaining debug logs is a two-step process:

1. Configure the components for which you want to obtain the debug logs on the Debug Log Configuration page. To configure debug logs for various components, see "Understanding Debug Log Configuration" section on page 14-8 and "Configuring Debug Log Level" section on page 14-9.

   Table 23-2 provides a list of components and the corresponding debug logs that it generates.

2. Download the debug logs.

Table 23-2 Debug Log Configuration: Components and the Corresponding Debug Logs

Component	Debug Log
runtime-AAA	*prrt.log*
runtime-config	*prrt.log*
runtime-logging	*prrt.log*
NotificationTracker	*ise-tracking.log*
ReplicationTracker	*ise-tracking.log*
CacheTracker	*ise-tracking.log*
pep-auth-manager-test	*ise-psc.log*
net-securent	*ise-psc.log*
posture	*ise-psc.log*
provisioning	*ise-psc.log*
swiss	*ise-psc.log*
client	*ise-psc.log*
prrt-JNI	*ise-prrt.log*
profiler	*profiler.log*
cisco-mnt	*ise-psc.log*
guest	*ise-psc.log*
guestportal	*ise-psc.log*
sponsorportal	*ise-psc.log*
guestauth	*ise-psc.log*
epm-pap	*ise-psc.log*
epm-pdp	*ise-psc.log*
epm-pip	*ise-psc.log*
epm-pap-api.services	*ise-psc.log*
org-apache	*ise-psc.log*
org-apache-digester	*ise-psc.log*
org-displaytag	*ise-psc.log*

Table 23-2 Debug Log Configuration: Components and the Corresponding Debug Logs

Component	Debug Log
org-apache-cxf	*ise-psc.log*
identity-store-AD	*ise-psc.log*
mnt-collector	*mnt-collector.log*
mnt-alert	*mnt-alert.log*

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations that are described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges that are associated with each of them.

To download debug logs, complete the following steps:

Step 1 Choose **Operations > Troubleshoot > Download Logs**.

Step 2 From the Appliance node list navigation pane on the left, choose the node from which you want to download the debug logs.

The Support Bundle and Debug Logs page appears.

Step 3 Click the **Debug Logs** tab.

A list of debug log types and debug logs is displayed. This list is based on your debug log configuration. See "Understanding Debug Log Configuration" section on page 14-8 for more information.

Step 4 Click the log file that you want to download and save it to the system that is running your client browser.

You can repeat this process to download other log files, as needed. The following are additional debug logs that you can download from the Debug Logs page:

- isebootstrap.log—Provides bootstrapping log messages
- monit.log—Provides watchdog messages
- pki.log—Provides the third-party crypto library logs
- iseLocalStore.log—Provides logs about the local store files
- ad_agent.log—Provides Microsoft Active Directory third-party library logs
- catalina.log—Provides third-party logs

Monitoring Administration

The rate and amount of data that is utilized by Monitoring functions requires a separate database on a dedicated node that is used for these purposes.

Like Policy Service, Monitoring has a dedicated database that requires administrators to perform maintenance tasks, such as the topics covered in this section:

- Backing Up and Restoring the Monitoring Database, page 23-45
- Viewing Log Collections, page 23-53
- Specifying Email Settings, page 23-53
- Configuring System Alarm Settings, page 23-54
- Configuring Alarm Syslog Targets, page 23-54

Backing Up and Restoring the Monitoring Database

Monitoring functionality handles large volumes of data. Over time, the performance and efficiency of the node depends on how well you manage that data. To increase efficiency, it is recommended that you back up the data and transfer it to a remote repository on a regular basis. You can automate this task by scheduling automatic backups.

Note If you register a secondary Monitoring ISE node, it is recommended that you first back up the primary Monitoring ISE node and then restore the data to the new secondary Monitoring ISE node. This ensures that the history of the primary Monitoring ISE node is in sync with the new secondary node as new changes are replicated. For more information, see Performing On-Demand Backups, page 23-50 and Restoring the Monitoring Database, page 23-51.

Due to the size of the Monitoring database, the backup process can take a while to complete. To save time, you can perform incremental backups, after first completing an initial full database backup. A recommended step, purging unwanted data during the backup process permanently deletes data from the database, and can be configured as an automatic process.

You cannot back up or restore (on-demand and scheduled) the monitoring database for 1.5 hours before or after the purge process. The purge process begins at 4 a.m. (0400). and you cannot back up or restore the monitoring database between 2:30 a.m. (0230) and 5:30 a.m. (0530).

Warning **For scheduled backup and purge to work properly for a redundant Monitoring ISE node pair, you must create and specify the same repository, or repositories, for both the primary and secondary nodes. The repository is not automatically synced between the primary and nodes. For more information, see Configuring Repositories, page 15-3.**

This section shows you how to effectively manage the Monitoring database and optimize disk space through the following tasks:

- Configuring Data Purging, page 23-46
- Scheduling Full and Incremental Backups, page 23-48
- Performing On-Demand Backups, page 23-50
- Restoring the Monitoring Database, page 23-51

Note Every administrator account is assigned one or more administrative roles. Depending upon the roles that are assigned to your account, you may not be able to see or perform the options or perform the procedures that are described in this section. For more information, see Understanding the Impact of Roles and Admin Groups, page 2-19.

Configuring Data Purging

The purging process allows you to manage the size of the Monitoring database by configuring the following options:

- Percentage of Disk Space—Specifies a usage threshold for the Monitoring database as a percentage (%) of total used disk space. The default for the user-configurable option is 80 percent. The maximum value allowed is 100 percent.

  When a purge operation triggers, if the actual used database disk space is greater than the configured threshold, the purge operation removes all data from the Monitoring database tables prior to the data retention window (as specified in the Maximum Stored data period field described below).

- Maximum Stored Data Period—Specifies the number of months to retain data during a purge. The default is three (3) months. This value is utilized when the disk space usage threshold for purging (Percentage of Disk Space) is met.

  Note For this option, each month consists of 30 days. The default of three months equals 90 days.

- Data Repository—Specifies the repository in which to backup data prior to purging. You select the repository from the drop-down menu. If a repository is not specified, the data is purged without prior backup. For information on how to specify a repository, see Configuring Repositories, page 15-3.

Conditions and Rules for Monitoring database Purging

- The purge process executes once every 24 hours at 4 AM.

  Purging is always based on the database consumed disk space percentage. Only when the used database space is equal to or exceeds the user specified allowed percentage (by default 80%, which is user configurable), does the purging process begin purging the tables. Otherwise, the purging process is skipped.

- If the Monitoring database disk usage is greater than 95 percent of the threshold setting, an information (INFO) alarm is generated indicating that the database size is too large.

- If the Monitoring database disk usage is greater than 100 percent or above the threshold setting, a backup runs. Monitoring data that is older than the data retention window setting (the default is three months, or 90 days, as each month consists of 30 days) is removed from the database. An information (INFO) alarm is generated after the purge completes.

  A purge process runs, creating a status history report that you can view by going to **Operations > Reports > System > Data Management > Monitoring Node > Purging History**. An information (INFO) alarm is generated when the purge completes.

  Note If you have not specified a repository, the data is not backed up.

- If the Monitoring database disk usage is greater than 125 percent of the threshold setting, a backup is not performed. Data that is older than the data retention window setting is automatically removed from the database.

  A purge process runs, creating a status history report that you can view by going to **Operations > Reports > System > Data Management > Monitoring Node > Purging History**. An information (INFO) alarm is generated when the purge completes.

- You must configure repositories for backup and data purging on both the primary and secondary Monitoring ISE nodes, using the same repositories for each. This is important for the backup and purging features to work properly. Purging takes place on both the primary and secondary nodes of a redundant pair, and the repository is not automatically synced between the nodes.

  For example, if the primary node uses two repositories for backup and purging, you must specify the same repositories for the secondary node. For more information, see Configuring Repositories, page 15-3 and Backing Up and Restoring the Monitoring Database, page 23-45.

- If the Cisco ISE node has Administration and Monitor personas (standalone or distributed deployment), a scheduled backup and restore pertains to both Administration and Monitoring data.

- In a distributed environment with a dedicate Monitor ISE node, a scheduled backup includes both Monitor and Administration content. However, since the Administration ISE node is remote on the network, the Administration data that is backed up from the Monitor ISE node might be out of date.

  For this reason, it is recommended that you sync the dedicated Monitor ISE node with the Administration ISE node, after the Monitor ISE node restore is complete.

- An on-demand backup only backs up monitoring data.

- You cannot run an on-demand or scheduled backup for 1.5 hours before or after the purge process.

Purging Unwanted Data

Purging is based on the percentage of consumed disk space for the database. When the consumed disk space for the database is equal to or exceeds the threshold (default 80 percent), the purging process starts. Purging always checks the Monitoring database disk space limit before proceeding.

The maximum stored data period is based on 30-day months, not calendar months. For example, if the server date is April 16, 2011 and the maximum stored data period is set to 1 month, a purge triggered on April 16, 2011 retains data from March 17, 2011 through April 15, 2011.

The purging process triggers once a day at 4:00 AM (a non-configurable default). If disk space usage is met or over the specified limit, the purge executes and runs in the background. If the limit has not been reached, purging is skipped.



Warning **For scheduled backup and purge to work properly on the nodes of a Monitoring redundant pair, you must configure the same repository, or repositories, on both the primary and secondary nodes using the CLI. The repositories are not automatically synced between the two nodes.**

Prerequisite

Configure a data repository where data is backed up prior to purging. You can configure a data repository for a Monitoring ISE node using the **repository** command in the system command line interface (CLI). For more information on CLI commands, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

To configure data purging, complete the following steps:

Step 1 Choose **Administration > System > Maintenance.**

Step 2 In the left-hand Maintenance panel, choose **Data Management**, expand the **Monitoring Node,** and select **Data Purging**.

Step 3 In the Data Purging panel, do the following:

a. Enter a numerical percentage value for allowed disk space usage. This threshold triggers a purge when disk space usage meets or exceeds Conditions and Rules for Monitoring database Purging, page 23-46.

b. Choose a data repository from the drop-down list. If no repository is specified, a backup does not occur.

c. Choose the maximum stored data period (in months) from the drop-down list. The default is three months.

Note For this option, each month consists of 30 days. The default of three months equals 90 days.

Step 4 Click **Submit**.

Step 5 Verify the success of the data purge by viewing the Purging History report. For more information, see System Reports, page 24-11.

Next Steps

Proceed with one of the of the following tasks:

- Scheduling Full and Incremental Backups, page 23-48
- Performing On-Demand Backups, page 23-50

Scheduling Full and Incremental Backups

You can schedule full-backups to run automatically at a specified day and time. You need to perform a full database backup before you begin scheduling incremental backups. Incremental backups backup only the data that has changed since the last backup, allowing you to save time and disk space.

Note You cannot schedule a full or incremental backup for 1.5 hours before or after the purge process (between 2:30 a.m. (0230) and 5.30 a.m. (0530). Also, full and incremental backups must be scheduled two hours apart.

Prerequisite

Before you begin either procedure you should have successfully set purging options, as described in Configuring Data Purging, page 23-46.

Scheduling Full Backups

By default, scheduled monthly backups occur on last day of month, scheduled weekly backups occur last day of week, and scheduled daily backups occur at the time specified.

To configure a full database backup, complete the following steps:

Step 1 Choose **Administration > System > Maintenance**.

Step 2 In the left-hand Maintenance panel, choose **Data Management**, expand the **Monitoring Node,** and select **Scheduled Backup**.

Step 3 Enter an **Encryption Key**. This key is used to encrypt and decrypt the backup file.

Step 4 Make sure that the **Incremental Backup** radio button is set to **On**. If it is set to **Off**, the full database backup will not start.

Step 5 Specify **Configure Full Monitoring Database Backup** options as follows:

a. Select a data repository from the drop-down list.

For information on how to specify a repository, see Configuring Repositories, page 15-3.

b. Schedule the time that the backup will be performed by selecting hours, minutes, and AM or PM from the drop-down lists.

c. Select the frequency of the backup from the drop-down list. Determine if it will be daily, weekly, or monthly.

Step 6 Click **Submit**.

Step 7 Verify the success of the backup by viewing the Backup History report. For more information, see System Reports, page 24-11.

Step 8 If the backup fails, check the following:

- Make sure that no other job or backup is running in parallel.
- Check the available disk space for the configured repository.
  - If the database disk usage is greater than 120 GB, but less than 150 GB (125 percent of the total database size of 120 GB), monitoring functions may wait until another purge is performed before continuing with the backup.
  - If the database disk usage is greater than 150 GB, a purge occurs whether or not a backup has occurred, to reduce the database disk usage is below 120 GB.
- Verify whether the repository is configured.

Next Step

- Restoring the Monitoring Database, page 23-51

Scheduling Incremental Backups

Incremental backups save time and disk space, and allow you to configure the frequency and time backups occur. Incremental backups store data updates in a separate location, so it is important that you perform an initial full backup before starting incremental backups.

Note Perform a full database backup before scheduling incremental backups. If you disable the incremental backup feature, run a full backup before returning to incremental backups. This precaution will ensure that all your data is complete and current.

Prerequisites

You should have successfully run a full backup of the Monitoring database, before you attempt to perform an incremental backup. For more information, see Scheduling Full Backups, page 23-48 or Performing On-Demand Backups, page 23-50.

To schedule incremental backups, complete the following steps:

Step 1 Choose **Administration > System > Maintenance.**

Step 2 In the left-hand Maintenance panel, choose **Data Management**, expand the **Monitoring Node,** and select **Scheduled Backup**.

Step 3 Enter an **Encryption Key**. This key is used to encrypt and decrypt the backup file.

Step 4 Make sure that the **Incremental Backup** radio button is set to **On**. If it is set to **Off**, the incremental backup will not start.

Step 5 Specify **Configure Incremental Monitoring Database Backup** options as follows:

a. Select a data repository from the drop-down list.

For information on how to specify a repository, see Configuring Repositories, page 15-3.

b. Schedule the time that the backup will be performed by selecting hours, minutes, and AM or PM from the drop-down lists.

c. Select the frequency of the backup from the drop-down list. Determine if it will be daily, weekly, or monthly.

Scheduled monthly backups occur on last day of month; scheduled weekly backups occur last day of week; and scheduled daily backups occur at the time specified.

Step 6 Click **Submit**.

Step 7 Verify the success of the backups by viewing the Backup History report. For more information, see System Reports, page 24-11.

Next Steps

Restore data from an incremental backup, start with the initial full backup and continue through the latest incremental backup. For more information on restoring data, see Restoring the Monitoring Database, page 23-51.

Performing On-Demand Backups

You can perform an immediate full backup of the Monitoring database at any time, as long as no other backup is already in progress. If another backup process is running, you must wait for it to complete before you can start an on-demand backup.

Note An on-demand backup only backs up monitoring data.

Note You cannot perform an on-demand backup for 1.5 hours before or after the purge process (between 2:30 a.m. (0230) and 5:30 a.m. (0530)).

Prerequisite

You should have configured data purging, as described in Purging Unwanted Data, page 23-47.

To generate a full backup immediately, complete the following steps:

Step 1 Choose **Administration > System > Maintenance.**

Step 2 In the left-hand Maintenance panel, choose **Data Management**, expand the **Monitoring Node,** and select **Full Backup On Demand**.

Step 3 Select a data repository from the drop-down list.

If no repository is specified, the data will be purged and no backup occurs. For information on how to specify a repository, see Configuring Repositories, page 15-3.

Enter an **Encryption Key**. This key is used to encrypt and decrypt the backup file.

Step 4 Click **Backup Now**.

Step 5 Verify the success of the backup by viewing the Backup History report. For more information, see System Reports, page 24-11.

Next Step

- Restoring the Monitoring Database, page 23-51

Restoring the Monitoring Database

You can restore data from an incremental or full backup using the Data Restore feature. If you choose to restore incremental backup data, the full data backup is restored first, followed by all subsequent incremental backups in sequential order.

The process for restoring the Monitoring database is different depending on the type of deployment. The following sections explain how to restore the Monitoring database in a standalone deployment and distributed deployments.

Standalone Deployment Restore

In a standalone deployment where Administration and Monitoring personas are both running on the Cisco ISE node, restoring a Monitoring database backup also restores the Administration database. For more information, see Restoring a Monitor backup in a Standalone Environment, page 23-52.

Distributed Deployment Restore

There are two possible scenarios for restoring a Monitoring backup:

- Restoring a Monitoring backup to a Cisco ISE node with Administration and Monitoring personas.
- Restoring a Monitoring backup to a Cisco ISE node with only a Monitoring persona.

For more information, see Restoring a Monitor Backup in a Distributed Environment, page 23-52.

Warning **If you attempt to restore data to a node other than the one from which the data was taken, you must configure the logging target settings to point to the new node. This ensures that the monitoring syslogs are sent to the correct node. For more information, see Configuring Alarm Syslog Targets, page 8-22.**

Restoring a Monitor backup in a Standalone Environment

Use the following procedure to restore the Monitoring database to a standalone node.

Prerequisites

You should have successfully performed the following procedures:

- Configuring Data Purging, page 23-46
- Scheduling Full and Incremental Backups, page 23-48 or Performing On-Demand Backups, page 23-50.

To restore incremental and full backup data, complete the following steps:

Step 1 Choose **Administration > System > Maintenance.**

Step 2 In the left-hand Maintenance panel, choose **Data Management**, expand the **Monitoring Node,** and select **Data Restore**.

Step 3 Select the name of an incremental or full backup from the list.

If an incremental backup file is selected, all previous incremental backups are shown, along with the initial full backup.

Enter the **Encryption Key** used during the backup.

Step 4 Click **Restore**.

Restoring a Monitor Backup in a Distributed Environment

Use the procedures outlined in this section to restore a Monitor backup in a distributed environment.

Prerequisites

You should have successfully performed the following procedures:

- Configuring Data Purging, page 23-46
- Scheduling Full and Incremental Backups, page 23-48 or Performing On-Demand Backups, page 23-50.

To restore a Monitor backup to a Cisco ISE node with Administration and Monitor personas:

Step 1 Prepare to promote another Cisco ISE node as the primary Administration ISE node, by syncing the node with the existing primary node you want to backup. For more information, see Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 15-12.

This ensures that the configuration of the Cisco ISE node you are going to promote is up to date

Step 2 Promote the newly synced Administration ISE node to primary status. For more information, see Configuring a Primary Administration Cisco ISE Node, page 9-11.

Step 3 Prepare to deregister the node to be backed up by assigning the Monitor persona to another node in the deployment. For more information, see Changing Node Personas and Services, page 9-23.

Note A deployment must have at least one functioning Monitor ISE node.

Step 4 Deregister the node to be backed up. For more information, see Removing a Node from Deployment, page 9-26.

Step 5 Restore the Monitor backup to the newly deregistered node, as described in Restoring a Monitor backup in a Standalone Environment, page 23-52.

Step 6 Register the newly restored node with the current Administration ISE node. For more information, see Registering and Configuring a Secondary Node, page 9-13.

Step 7 Promote the newly restored and registered node as the primary Administration ISE node. For more information, see Configuring a Primary Administration Cisco ISE Node, page 9-11.

To restore a Monitor backup to a Cisco ISE node with only a Monitor persona:

Step 1 Prepare to deregister the node to be restored by assigning the Monitor persona to another node in the deployment. For more information, see Changing Node Personas and Services, page 9-23.

Note A deployment must have at least one functioning Monitor ISE node.

Step 2 Deregister the node to be restored. For more information, see Removing a Node from Deployment, page 9-26.

Note Wait until the deregistration is complete before proceeding with the restore. The node must be in a standalone state before you can continue with the restore.

Step 3 Restore the Monitoring backup to the newly deregistered node, as described in Restoring a Monitor backup in a Standalone Environment, page 23-52.

Step 4 Register the newly restored node with the current Administration ISE node. For more information, see Registering and Configuring a Secondary Node, page 9-13.

Step 5 Promote the newly restored and registered node as the primary Administration ISE node. For more information, see Configuring a Primary Administration Cisco ISE Node, page 9-11.

Viewing Log Collections

Monitoring functions collects log and configuration data, stores the data, and then processes the collected data to generate reports and alarms. You can view the details of the logs that are collected from any of the servers in your deployment. For more information, see Chapter 14, "Logging."

Specifying Email Settings

For use with monitoring log messages, you can specify the email server email address and the name that is displayed for this address. For more information, see Configuring Email Settings, page 8-20.

Note Depending upon the roles that are assigned to your account, you may or may not be able to perform the operations or see the options that are described in the following procedure. For more information, see Understanding the Impact of Roles and Admin Groups, page 2-19.

Configuring System Alarm Settings

System alarms notify you of critical conditions that are encountered. System alarms are standard and cannot be created or deleted. You can enable and disable system alarms, and you can configure how you receive notification. You can choose to send alarm notifications through email and as syslog messages.

For instructions on how to set system alarms, see Configuring System Alarm Settings, page 8-21.

Note To send syslog messages successfully, you must configure alarm syslog targets, which are syslog message destinations. See Configuring Alarm Syslog Targets, page 8-22.

For more information:

See System Alarm Settings, page A-60 of Appendix A, "User Interface Reference."

Configuring Alarm Syslog Targets

If you configure monitoring functions to send system alarm notifications as syslog messages, you need a syslog target to receive the notification. Alarm syslog targets are the destinations where alarm syslog messages are sent.

You must also have a system that is configured as a syslog server to be able to receive syslog messages. You can create, edit, and delete alarm syslog targets. For more information, see Configuring Alarm Syslog Targets, page 8-22.

Warning **Cisco ISE monitoring requires that the logging source-interface configuration use the network access server (NAS) IP address. For information on how to configure a switch for Cisco ISE monitoring, see Configure NADs for ISE Monitoring, page D-33.**

For more information:

See Alarm Syslog Targets, page A-59 of Appendix A, "User Interface Reference."



CHAPTER 24

Reporting

Cisco Identity Services Engine (ISE) reports are used with monitoring and troubleshooting features to analyze trends, monitor system performance and network activities from a central location. For more information, see Chapter 23, "Monitoring and Troubleshooting."

This chapter explains the types of reports that are available in ISE. It also discusses the various ways that you can use report data, and how you can organize data for more effective use.

This chapter covers the following topics:

- Report Basics, page 24-1
- Catalog Reports, page 24-6
- Favorite Reports, page 24-8
- Shared Reports, page 24-10
- System Reports, page 24-11
- Organizing and Formatting Report Data, page 24-12
- Working with Active RADIUS Sessions, page 24-39
- Available Reports, page 24-42

Report Basics

ISE collects log and configuration data from across your network, and it then aggregates the data into reports for you to view and analyze. ISE provides a standard set of predefined reports that you can use and customize to fit your needs.

The reports are grouped into logical categories for information related to authentication, session traffic, device administration, configuration and administration, and troubleshooting. For a complete list of ISE reports, see Available Reports, page 24-42.

Note All the reports except Favorite and Shared reports will be deleted after upgrade.

This section covers the following topics:

- Understanding Reports View and Interactive Viewer, page 24-2
- Running, Viewing, and Navigating Reports, page 24-3
- Exporting and Printing Reports, page 24-4

- Deleting Reports, page 24-5

Understanding Reports View and Interactive Viewer

You can view, run, and customize report data using Reports View and Interactive Viewer for all types of reports.

Note Cisco does not recommend using Interactive Viewer in the following version 8 releases of Windows Internet Explorer running in a Microsoft Windows XP operating system environment:

- Version 8.0.6001.18702
- Version 8.0.6001.18702IC

About Reports View

The Reports View displays lists of catalog or favorites reports, allows you to run reports, view results, export data, and print information. Reports View displays automatically when you select **Operations > Reports > Catalog** or **Favorites**.

- **Catalog reports** are preconfigured system reports that are standard in ISE. For more information, see Catalog Reports, page 24-6.
- **Favorites reports** are frequently used reports that you add to your Favorites page to make them easier to find. For more information, see Favorite Reports, page 24-8.
- **Shared reports** are reports that you make them available for all users by placing them in a shared folder.

About Interactive Viewer

Interactive Viewer allows you to organize and format report data into tables, graphs, or charts. It also allows you to drill down for finer details, filter report data, customize your reports, and then save custom report designs for later use.

You access Interactive Viewer by clicking the **Launch Interactive Viewer** link on the toolbar that appears at the top of the window after you run a report.

Figure 24-1 Launch Interactive Viewer Icon



The Interactive Viewer toolbar appears, providing the tools for Organizing and Formatting Report Data, page 24-12. For specific information, see Working with the Interactive Viewer Toolbar, page 24-12.

Figure 24-2 Interactive Viewer Toolbar



Using Context Menu Shortcuts

Context menus provide shortcuts for performing formatting and organizing tasks, and they appear when you right-click a report item. Each context menu is specific to the item you right-click. For example, when you right-click a label, the context menu that appears supports formatting the label.

For more information:

See the Troubleshoot, page A-40 of Appendix A, "User Interface Reference," for details on the fields.

Running, Viewing, and Navigating Reports

This section describes how to run, view, and navigate reports using Reports View. You can specify time increments over which to display data in a report. Available time durations include the last 30 minutes, the last hour, the last 12 hours, yesterday, the last 7 days, or the last 30 days.

Prerequisite

You should have reviewed Understanding Reports View and Interactive Viewer, page 24-2.

To run, view, and navigate reports using the Reports View, complete the following steps:

Step 1 Choose **Operations > Reports** and **Catalog** or **Favorites.** This example uses catalog.

Step 2 Choose a **Report** category from the list in the left-hand navigation pane.

Note Move your cursor over a report name to view a context-sensitive description for the report, along with its logging category, when applicable.

A list of available reports for that category appears in the main window.

Step 3 Run a report in one of the following ways:

- Click the radio button to the left of the report name, and then select a time duration for the report from the Run drop-down menu.
- Click the **Report Name** link to run the report for today only.

Report data is shown in the main window.

Step 4 Enter report criteria for the selected report as needed, and then click **Run**. To reload the report data click the **Reload** link.

Step 5 Scroll down to view report results, expanding topic headings for more details.

Step 6 To move forward or back through the report, click the **First**, **Prev**, **Next**, or **Last** links in the toolbar. Or, jump directly to a specific page by entering the page number in the **Go to Page** field, and then clicking **Go**.

Step 7 To view a table of contents, click the **Toggle TOC** icon on the toolbar, then select a link in the left-hand navigation pane. Click the plus (+) icon in the right-hand window to expand and view the contents.

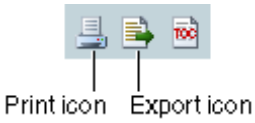
For more information:

- Catalog Reports, page 24-6
- Favorite Reports, page 24-8
- Shared Reports, page 24-10
- System Reports, page 24-11
- Available Reports, page 24-42
- Reports, page A-15 for information on individual fields

Exporting and Printing Reports

After you have run a report, you can export the data to a spreadsheet or print the data as is. You perform these tasks using the Print and Export icons on the toolbar.

Figure 24-3 Print and Export Icons



Exporting Report Data

You can export report data to an Excel spreadsheet as a comma-separated values (.csv) file, pipe-separated values (.psv) file, or a tab-separated values (.tsv) file.

Note Exported report records have a 5k size limit. Check the size of the data prior to exporting, and export in bundles of 5k or less.

Spreadsheet data is formatted like the data in the information object or the template. If you edit column headers or format numeric data in the report design, the spreadsheet does not reflect your edits. For more information, see Organizing and Formatting Report Data, page 24-12.

Prerequisite

Check the size of the report data you want to export. The data must be 5k or less.

To export report data, complete the following steps:

Step 1 Run a report, as described in Running, Viewing, and Navigating Reports, page 24-3.

Step 2 In the top left-hand corner of the report summary window, click the **Export Data** icon. The Export Data dialog appears.

Step 3 Select an Available Results Set from the drop-down menu.

Step 4 Specify the data columns that you want to export by selecting the names from the Available Columns list and clicking the arrow button (>) to move them to the Selected Columns list. Or click the double arrows button (>>) to select and move all the columns.

To move unwanted selected columns back to the Available Columns list, select the column and click the reverse arrow button (<). To move all the columns back, click the double reverse arrows button (<<).

Step 5 Select an encoding style and separator type from their respective drop-down menus.

Step 6 Choose **Export Column Data Type**, and then click **OK**.

Printing a Report

You can print a report that appears in the viewer in HTML or PDF format. If you modify the report, you can choose to print the original report or the modified report. For more information, see Organizing and Formatting Report Data, page 24-12.

To print report data, complete the following steps:

Step 1 Run a report, as described in Running, Viewing, and Navigating Reports, page 24-3.

Step 2 In the top left-hand corner of the report summary window, click the **Print Report** icon. The Print dialog appears.

Step 3 Select a format, either HTML or PDF.

Step 4 For PDF, you can specify the size of the printout by selecting Auto, Actual Size, or Fit to Page.

Step 5 Specify the pages that you want printed by selecting either **All**, **Current Page**, or **Pages**. Then, enter a range of pages in the text field.

Step 6 Click **OK**. A printer-friendly formatted page appears, along with a Print dialog.

Step 7 Select the appropriate printer and click **OK**.

For more information:

See the Reports, page A-15 of Appendix A, "User Interface Reference," for details on the fields.

Deleting Reports

You can only delete customized reports. You are not allowed to delete catalog system reports.

Prerequisites

You should have created a customized catalog or favorites report, as described in the following sections:

- Customizing Catalog Reports, page 24-7
- Editing or Deleting Favorite Reports, page 24-10

To delete a customized report, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog**, **Favorites**, or **Shared**

Step 2 Navigate to the custom report and click the radio button next to the report name that you want to delete. The Delete button is activated.

Step 3 Click **Delete**, and then click **Yes** to confirm the action.

Catalog Reports

Catalog reports are preconfigured system reports. Reports of a similar nature are grouped in the same category. For a complete list of catalog reports, see Available Reports, page 24-42.

This section covers the following topics:

- Accessing Catalog Reports, page 24-6
- Customizing Catalog Reports, page 24-7
- Restoring Default Report Settings, page 24-7

Accessing Catalog Reports

This section shows you how to access the various system reports that are standard with ISE. For a complete list of catalog reports, see Available Reports, page 24-42.

To access catalog reports, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog**. A list of catalog report categories appears in the left-hand navigation pane.

Step 2 Select a category name in the left-hand Reports navigation pane. A list of reports for that category appears in the right-hand window.



Note Move your cursor over a report name to display a context-sensitive description for the report, along with its logging category, when applicable.

Step 3 Select a report from the list, and perform any of the following tasks:

- Running, Viewing, and Navigating Reports, page 24-3
- Customizing Catalog Reports, page 24-7
- Exporting and Printing Reports, page 24-4

For more information:

See section of Appendix A, "User Interface Reference," for details on the fields.

Customizing Catalog Reports

You can customize a catalog report and save the changes as a new report, or restore the default report settings.

Note If you save a customized report with the same name as the original system report (overwriting the original system report), you will not be allowed to delete it. To restore a customized report to the default, preconfigured system report settings, see Restoring Default Report Settings, page 24-7.

To customize a catalog report, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog**.

Step 2 Select a catalog category in the left-hand navigation pane, and then click the radio button next to a report name in the list that appears in the right-hand window.

Step 3 Click **Run**, and then modify fields in the Run Reports page as needed.

Step 4 Click **Run** again, to incorporate the changes that you made to the fields.

Step 5 (Optional) Perform the tasks that are described in Organizing and Formatting Report Data, page 24-12.

Step 6 Click **Save As** and enter a unique report name.

For more information:

See the Reports, page A-15 of Appendix A, "User Interface Reference," for details on the fields.

Restoring Default Report Settings

This section shows you how to restore a customized system report, with the same name as the default system report, back to its default settings.

Take, for example, the RADIUS_authentication report. If you save a customized version of this report under the same name, on the date and time changes on the RADIUS authentication system report. When you reset the report, the original date and time are reinstated.

Note This procedure resets all the reports in a particular catalog category. For example, if you reset a customized report that resides in the Endpoint category, this procedure resets all other reports within the Endpoint category as well.

Prerequisites

Before you begin this task, you should have customized a catalog report, as described in Customizing Catalog Reports, page 24-7.

To restore default report settings, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog.**

Step 2 Select the catalog category of the customized report from the left-hand navigation pane.

Step 3 Click **Reset Reports**.

Step 4 Click **Yes** to confirm that you want to reset all the catalog reports in the selected category to their factory defaults.

For more information:

See the Reports, page A-15 of Appendix A, "User Interface Reference," for details on the fields.

Favorite Reports

You can add reports that you use frequently to a list of favorites to make them easier to find, similar to how you bookmark favorite web sites in a browser. You can view and edit the parameters of your favorite reports, and then save the customized reports for reuse.

Note Every administrator account is assigned one or more administrative roles. Depending upon the roles that are assigned to your account, you may not be able to perform the tasks that are described in this section.

This section contains the following topics:

- Adding Favorite Reports, page 24-8
- Viewing Report Parameters, page 24-9
- Editing or Deleting Favorite Reports, page 24-10

Adding Favorite Reports

You can add preconfigured catalog system reports to your favorites list, as well as reports that you have customized.

The following preconfigured catalog system reports are available in **Operations > Reports > Favorites** by default:

- Authentications - RADIUS - Today—A report that is preconfigured from AAA Protocol > RADIUS_Authentication to run for the current system date.
- Authentications - RADIUS - Yesterday—A report that is preconfigured from AAA Protocol > RADIUS_Authentication to run for the previous day from the current system date.
- ISE-Server Configuration Audit - Today—A report that is preconfigured from Server Instance > Server_Configuration_Audit to run for the current system date.
- ISE-System Diagnostics -Today—A report that is preconfigured from Server Instance > Server_System_Diagnostics to run for the current system date.

This section shows you how to create a favorites list.

Prerequisites

Before beginning this task, you should have successfully completed Running, Viewing, and Navigating Reports, page 24-3.

To add a report to your favorites list, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog**.

Step 2 Select a catalog category in the left-hand navigation pane, and then click the radio button next to the report name in the list that appears in the right-hand window.

Step 3 Click **Add to Favorite**.

Step 4 Specify the following information on the Add to Favorite page:

a. Enter a unique favorite name.

b. Enter a server IP address, or select one from the drop-down list.

c. Select a time range from the drop-down list.

d. If you specified a custom time range, specify a start date and an end date for the report by clicking the calendar icon and selecting a date.

Step 5 Click **Add to Favorites**. The report appears on your Favorites list.

For more information:

See the Reports, page A-15 of Appendix A, "User Interface Reference," for details on the fields.

Viewing Report Parameters

Before running a Favorites report, you can view and edit the report parameters.

To view the parameters of a report, complete the following steps:

Step 1 Choose **Operations > Reports > Favorites**.

Step 2 Check the check box next to the report for which you want to view the parameters, and then click **Parameters**.

A window appears, listing the parameters in your report with their respective values.

Step 3 Click **Cancel** to return to the Favorites report.

For more information:

See the Reports, page A-15 of Appendix A, "User Interface Reference," for details on the fields.

Editing or Deleting Favorite Reports

After you view the existing parameters in your favorite report, you can edit them.

To edit the parameters in your favorite reports, complete the following steps:

Step 1 Choose **Operations > Reports > Favorites**.

A list of your favorite reports appears.

Step 2 To edit a report, check the check box next to the report and click **Edit**.

The Edit Favorite page appears.

Step 3 Modify the values for the parameters as needed.

Step 4 Do one of the following:

- To save the changes, click **Edit Favorite**.
- To restore the original values, click **Reset**.
- To cancel the changes and return to the Favorites page, click **Cancel**.

A status message appears, stating that the report was successfully edited.

Step 5 To customize the display of a favorite report, see Organizing and Formatting Report Data, page 24-12.

Step 6 To save your customizations, see Saving Customized Reports, page 24-39.

Step 7 To delete a favorite report, check the check box next to the report and click **Delete**.

For more information:

See the Reports, page A-15 of Appendix A, “User Interface Reference,” for details on the fields.

Shared Reports

You can share selected reports, making them available to other users. You share reports by adding them to a Shared folder.

To share reports with other users, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog** or **Favorites**, and select the report that you want to share.

Step 2 Run the report, as described in Running, Viewing, and Navigating Reports, page 24-3

Step 3 Launch the report in the Interactive Viewer, as described in Working with the Interactive Viewer Toolbar, page 24-12.

Step 4 Click the **Save** icon in the upper-left corner of the Interactive Viewer. The Save dialog appears.

Step 5 In the Save dialog, do the following:

a. In the Choose a Folder list, choose **Shared** by double clicking on Shared in the list. The Admin > Shared window would be displayed.

b. Enter a unique filename for the report.

c. Select a format from the Save as Type drop-down list.

Step 6 Click **Save**.

The report appears in your Shared folder and is available for all users.

System Reports

System reports allow you to view different types of system data, so that you can better monitor your ISE network. System reports include the following:

- Data Management
  - Administration Node: Backup History, Restore History
  - Monitoring Node: Backup History, Purging History
- Licensing History
- Log Collection Status, for ISE servers

Note The logging function that reports on system diagnostics is not enabled in Cisco ISE by default. To enable system diagnostic reports, see the "Enabling System Diagnostic Reports in Cisco ISE" section of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

To view history related system reports, complete the following steps:

Step 1 Select **Operations > Reports > System**.

Step 2 In the left-hand navigation pane, do one of the following:

- Select **Data Management** and then do one of the following:
  - Select **Administration Node**, and then select **Backup History** or **Restore History**. A history report for your selection appears in the right-hand panel.
  - Select **Monitor Node**, and then select **Backup History** or **Purging History**. A history report for your selection appears in the right-hand panel.
- Select **License History**. A history report for your selection appears in the right-hand panel.

Step 3 To filter applicable report data, see Filtering Report Data, page 24-24.

To view a log collection status report, complete the following steps:

Step 1 Select **Operations > Reports > System**.

Step 2 In the left-hand navigation pane, select **Log Collection Status**. A list of server log collections appears in the right-hand panel.

Step 3 To view a log collection, click the radio button next to a server name, and then click **Get Details**.

Step 4 To update the report information, click **Refresh**.

Step 5 To return to the list of server log collections, click **Back**.

Organizing and Formatting Report Data

You can modify the layout of reports, customize the display, and reformat the data. After you access a data source and select the data set to use, you determine the best way to display the data in a report.

This section covers the following topics:

- Working with the Interactive Viewer Toolbar, page 24-12
- Grouping, Sorting, and Hiding Data, page 24-13
- Changing Column Layouts, page 24-17
- Creating Report Calculations, page 24-21
- Filtering Report Data, page 24-24
- Working with Aggregate Data, page 24-28
- Working with Charts, page 24-29
- Formatting Reports, page 24-32
- Saving Customized Reports, page 24-39

Working with the Interactive Viewer Toolbar

The majority of the data formatting and organizing tasks are performed from the Interactive Viewer, working with the utilities that are shown on the toolbar. Move your cursor on top of a toolbar icon to display a tooltip with the name of the utility. The organizing and formatting data tasks refer to these icons, as appropriate.

Figure 24-4 Interactive Viewer Toolbar



In many cases, you have the option of using context menu shortcuts to access the same functionality as the icons shown on the toolbar.

To display and use the Interactive Viewer toolbar, complete the following steps:

Step 1 Select **Operations > Reports > Catalog**. Then select and run a report.

Step 2 In the upper right-hand corner of the Reports View window, click **Launch Interactive Viewer**. The toolbar appears at the top of the window.

Step 3 To activate the toolbar, select a column or other element in the report. The tools that are applicable to the selected element become active.

Note If you select inside a heading row, the tools for formatting text are activated. To activate the rest of the tools in the toolbar, click the bottom line of the heading.

For more information:

See Troubleshoot, page A-40 of Appendix A, "User Interface Reference," for details on the fields.

Grouping, Sorting, and Hiding Data

A group displays all the information about a type of item in one place, which allows you to better compare values and make assessments of the data. If a report presents all its data in an unorganized list, it is difficult to make comparisons and calculate values.

For example, you might group all the information about one customer to see how much that client ordered from your company in a specific quarter. And then you might group information about another customer for another quarter, and so on.

This section covers the following tasks:

- Grouping Data, page 24-13
- Sorting Data, page 24-14
- Hiding and Displaying Report Items, page 24-16
- Hiding and Displaying Column Data, page 24-16

Grouping Data

To organize information into a useful report, you create data groups. Data groups contain related data rows. For each group, you can show aggregate data, such as the total purchase price or a count of the items in a group. Grouping data gives your report a more polished, organized look, and it makes it easier to create useful comparisons and calculations.

The grouped-data changes that you make do not affect the report design. You can save the report output to reflect your changes.

Adding Groups

You can add groups in Interactive Viewer if the report design does not contain the desired grouping.

To create a data group, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Do one of the following:

- Select and highlight the column that you want to use to create a group, and then click the **Add Group** icon in the toolbar.
- Right-click the column that you want to use to create a group, and choose **Group > Add Group** from the context menu.

The new group appears in the viewer, expanding to show all the detail rows.

Step 3 (Optional) To collapse the group, click the minus sign (**-**) next to the group name.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Grouping Based on Date and Time

When you create a group based on a column that contains date or time data, you can set a grouping interval. For example, if the column contains time data, you can group hours, minutes, or seconds.

To create a group based on date and time, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Do one of the following:

- Select and highlight the column that you want to use to create a group, and then click the **Add Group** icon in the toolbar.
- Right-click the column that you want to use to create a group, and choose **Group > Add Group** from the context menu.

The Group Detail dialog box appears. To show every date or time value, leave the default setting **Group Using Individual Values**.

Step 3 (Optional) To set a grouping interval, choose **Group Every**, enter a value, and select the grouping interval. For example, to create a new group for every month, enter **1**, and choose **Month** from the drop-down list.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Removing an Inner Group

You can remove data groups in Interactive Viewer to attain the desired groupings.

To remove a specific data grouping, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Do one of the following:

- Select and highlight the column that you want to use to create a group, and then click the **Delete Inner Group** icon in the toolbar.
- Right-click the column that you want to use to create a group, and choose **Group > Delete Inner Group** from the context menu.

Step 3 To save your changes, see Saving Customized Reports, page 24-39.

Sorting Data

The data source determines the default sort order of the data rows in the report. Typically, data appears randomly, so sorting is an important task in creating a useful report. You can sort single data columns or multiple columns.

Sorting a Single Column

You can sort a single column of data in ascending order or descending order.

To sort a single data column, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a column in the report and do one of the following:

- Right-click and choose **Sort > Ascending** or **Sort > Descending** from the context menu.
- Choose either the **Sort Ascending** or **Sort Descending** icon on the toolbar.

Step 3 (Optional) To return the data to its original order, click the **Undo** icon on the toolbar.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Sorting Multiple Columns

You can sort multiple columns of data in a report, however, it is important to understand the order of precedence for the sort. Using Advanced Sort, the first column that you select becomes the primary sorting column, and the other columns are sorted in relation to the primary column.

For example, if the primary (first sorted) column is Customer Names and it is sorted in ascending order, the customers are shown in alphabetical order. If the next column that you select for sorting is Location, the order is also ascending, and within each Customer entry, the locations are sorted in ascending order. If the third column that you select for sorting is Order Number, the order is ascending, and within each location, the order numbers are sorted in ascending order.



Note If the report uses grouped data, the drop-down lists in Advanced Sort show only the detail columns in the report, not the columns that you used to group the data.

To sort multiple data columns, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside the primary sorting column, and choose **Sort > Advanced Sort** from the context menu.

Step 3 Select a column from the first drop-down list, and click either the **Ascending** or **Descending** radio button.

Step 4 Select the next column, choose a sort order, and so on.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Hiding and Displaying Report Items

You can hide and show selected items in a report.

To hide and display selected report items, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a column, and choose **Hide or Show Items** from the context menu. The Hide or Show Items dialog box appears.

Step 3 Do any of the following:

- Select any items that you want to hide.
- Deselect any hidden items that you want to display.
- To display all hidden items, and click **Clear**.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Hiding and Displaying Column Data

There may be times when you do not want to display all the data in a report. For example, a column of detail can display duplicate values in consecutive data rows. In this case, suppressing consecutive duplicate values makes the report easier to read. You can also choose to collapse groups or sections, so that you display only the column headings and summary data, such as aggregate data rows.

This section covers the following tasks:

- Suppressing and Displaying Repeated Values, page 24-16
- Hiding or Displaying Detail Rows in Groups or Sections, page 24-17

Suppressing and Displaying Repeated Values

Data rows appear in the report exactly as they appear in the data source, which may include rows with duplicate values. To make the report easier to read, you can choose to suppress the display of the repeated values. This suppression only alters the visual display and not the data source itself. You can later choose to redisplay the repeated values at any time.

To suppress and display repeated values in a report, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a column, and choose **Hide or Show Items** from the context menu. The Hide or Show Items dialog box appears.

Step 3 Do any of the following:

- Select any items that you want to hide.
- Deselect any hidden items that you want to display.
- To display all hidden items, click **Clear**.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Hiding or Displaying Detail Rows in Groups or Sections

If a report contains groups, you can easily collapse and expand a group to hide and show its contents.

To hide and display detail rows in groups or sections, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 To collapse a group or section, right-click the group or section and choose **Group > Hide Detail** from the context menu.

Step 3 To redisplay the group or section, right-click inside the report and choose **Group > Show Detail**.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Changing Column Layouts

You can change the display of columns and their content. This section shows you how to perform the following tasks:

- Modifying Column Display, page 24-17
- Realigning Column Data, page 24-18
- Hiding and Displaying Columns, page 24-19
- Merging Columns, page 24-20
- Selecting a Column from a Merged Column, page 24-20
- Moving Data from a Group Column into the Header, page 24-21

Modifying Column Display

The default formatting for column data comes from the data source. You can modify the default formatting of column data to enhance the appearance and readability of the report. When you format column data, the format changes are applied to the entire column, with the exception of the column header and aggregate rows. You are not allowed to modify the data itself.

To modify the formatting of column data, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a column and choose **Style > Font** from the context menu.

Step 3 In the Font form, modify the style properties that you want to change. You can see your changes applied immediately in the Preview field.

Step 4 Indicate whether to apply the new text style to all columns in the report or only to the selected column. The default setting is to apply the new style only to the selected column.

Step 5 Click **Apply**.

Step 6 To save your changes, see Saving Customized Reports, page 24-39.

Realigning Column Data

You can easily change the alignment of data in individual columns in a report, to enhance readability and visual appeal. The default is to align column data along the left side of the column. You can also choose to center the data or align it along the right-hand side of the column. Select the alignment that is best suited for your report data.

To change the alignment of column data, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a column to highlight, and then do one of the following:

- To align column data to the left, click the **Align Left** icon on the toolbar. This setting is the default.
- To center the column data, click the **Align Center** icon on the toolbar.
- To align column data to the right, click the **Align Right** icon on the toolbar.

Step 3 Repeat Step 2 with other columns in the report, as desired.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Reordering and Removing Columns

You can easily reorder and remove columns using the Interactive Viewer. This section walks you through the steps for these tasks.

Note When you remove a column from the report, you are not deleting the column from the information object or other data source. You are only removing the information from the report display.

To reorder a column, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Do one of the following:

- Click the **Reorder Columns** icon on the toolbar.
- Right-click inside a column and choose **Column > Reorder Columns** from the context menu.

Note You can select only detail rows, not groups or sections.

Step 3 Select a column header from the Arrange Columns dialog, and click the Up or Down arrows at the right until the column is in the desired position.

Step 4 Repeat Step 3 until all columns are in the desired order, and then click **Apply**. The order of the columns changes to match your selections.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

To remove a column, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 To remove a single column, select that column, and then click the **Delete** icon on the toolbar.

Step 3 To remove multiple columns press the **Control** key, and select the columns that you want to remove. Then click the **Delete** icon on the toolbar.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Hiding and Displaying Columns

You can easily hide and display columns using the Interactive Viewer.

To hide and display columns, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 To hide a column, select the column and do one of the following:

- Click the **Hide Column** icon on the toolbar.
- Right-click and choose **Column > Hide Column**.

Step 3 To redisplay hidden columns, select a column and do one of the following:

- Click the **Show Columns** icon on the toolbar.
- Right-click and choose **Column > Show Columns**.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Merging Columns

You can merge the data from two or more columns into one column.

To merge columns, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 To merge data in multiple columns, select the desired columns using the Control and arrow keys, and do one of the following:

- Click the **Merge Columns** icon on the toolbar.
- Right-click and choose **Column > Merge Columns** from the context menu.

Step 3 To save your changes, see Saving Customized Reports, page 24-39.

Selecting a Column from a Merged Column

You can aggregate, filter, and group data in a column that contains merged data from multiple columns. However, you first need to select one of the columns on which to aggregate, filter, or group the data.

To select column data from merged columns, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click the merged column, and select a command from the context menu, such as **Aggregation**, **Filter > Filter**, or **Group > Add Group**. The Select Data Item dialog box appears.

If you need to provide more information, a dialog box appears. For example, if you choose Aggregation, the Aggregation dialog box appears.

Step 3 From the Select Data drop-down list, select the column name to which the command will be applied, and then click **Apply**.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Moving Data from a Group Column into the Header

You can move data from a group column into the header.

To move data from columns to group headers, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Create a group, as described in Adding Groups, page 24-13.

Step 3 Right-click inside a column and choose **Column > Move to Group Header**. Then, select a group name from the drop-down menu.

Step 4 Select a header row value from the drop-down menu.

Step 5 Click **Apply**. The data value from the specified row in the selected group appears in the group column header.

Creating Report Calculations

Most reports require calculations to track sales, finances, inventory, and other critical business activities. You can use typical mathematical functions such as counting, addition, subtraction, multiplication, and division. In addition, you can write expressions that extend these basic functions.

This section covers the following topics:

- Creating a Calculated Column, page 24-21
- Using Numbers and Dates in an Expression, page 24-22
- Multiplying Values in Calculated Columns, page 24-22
- Adding Days to an Existing Date Value, page 24-23
- Subtracting Date Values in a Calculated Column, page 24-23

Creating a Calculated Column

Displaying calculated data in a report requires that you create a calculated column.

To create a calculated column, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a report column and then click the **Add Calculation** icon. The Calculation dialog box appears. The new calculated column appears to the right of the column that you selected.

Step 3 In the Column Label field, enter a header for the calculated column.The header must start with a letter and can contain only letters, numbers, underscores, and spaces.

Step 4 Write an expression in the Enter Expression field that indicates the data to use and how to display the calculated data. Follow the guidelines in Using Numbers and Dates in an Expression, page 24-22, as needed.

The expression contains a function and one or more arguments. Arguments indicate the data that you want to use to create the calculation.

Step 5 Select a function and provide the argument.

Step 6 To save your changes, see Saving Customized Reports, page 24-39.

For more information:

See Reports, page A-15 of Appendix A, "User Interface Reference," for details on the fields.

Using Numbers and Dates in an Expression

When you create an expression that contains a number, the number should be typed according to the conventions of the U.S. English locale. In other words, use a period (.), not a comma (,), as the decimal separator. For example:

Correct: 1234.56

Incorrect: 1234,56

When you create an expression that contains a date, type the date according to the conventions of the locale that you chose when you logged in. For example, in the French (France) locale, type 03/12/2007 to represent December 3, 2007, not 12/03/2007. You can enter a date, or a date and time. Dates and times must be enclosed in double quotes (""), for example:

"03/12/2007"

"03/12/2007 11:00 AM"

Multiplying Values in Calculated Columns

You can multiply values in a calculated column by completing the following task.

To multiply values in a calculated column, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a report column and then click the **Add Calculation** icon. The Calculation dialog box appears. The new calculated column appears to the right of the column that you selected.

Step 3 In the Column Label field, enter a header for the calculated column. The header must start with a letter and can contain only letters, numbers, underscores, and spaces.

Step 4 In the Enter Expression field, enter a left square bracket ([). A list of the columns in the report appears. This list includes any calculated columns that the report contains.

Select the column that contains the multiplier. For example, to multiply a unit price times the quantity ordered, select the column that contains unit prices.

Step 5 Enter an asterisk (*) as the multiplication operator. You do not need to include a space after the column name.

Step 6 Enter another left square bracket ([) and select the multiplicand. For example, if the multiplier is the unit price, select the column that contains the quantity ordered as the multiplicand.

Step 7 To verify the expression, click **Validate**. If the expression syntax is correct, the dialog box displays a validation message. If the expression syntax is incorrect, the dialog box displays a message explaining the error.

Step 8 After validating the expression, click **Apply**. The calculated column appears in the report.

Step 9 To save your changes, see Saving Customized Reports, page 24-39.

Adding Days to an Existing Date Value

You can create a column that displays date values that are greater than the date values in another column.

To add days to an existing date value, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a column in a report and then click the **Add Calculation** icon. The Calculation dialog box appears. The new calculated column appears to the right of the column that you selected.

Step 3 In the Column Label field, type a name for the calculated column. For example, enter the **Forecast Shipping Date**.

Step 4 In the Enter Expression field, enter **A**. A drop-down list appears, displaying functions that begin with A.

Step 5 Choose **ADD_DAY(date, daysToAdd)**.

Step 6 For the first argument, enter a left square bracket ([) and choose the date column from the drop-down list. For example, choose **Order Date**.

Step 7 For the second argument, enter the number of days to add. In this case, enter **7**.

Step 8 Validate the expression, and then click **Apply**.

The new calculated column appears in the report. For every value in the Order Date column, the calculated column displays a date seven days later than the order date.

Step 9 To save your changes, see Saving Customized Reports, page 24-39.

Subtracting Date Values in a Calculated Column

You can subtract date values in a calculated column by completing the following task.

To display the difference between two date values, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a report column and then click the **Add Calculation** icon. The Calculation dialog box appears. The new calculated column appears to the *right* of the column you selected.

Step 3 In the Column Label field, enter a name for the calculated column. For example, to subtract the actual shipping date from the date requested, enter **Shipping Delay**.

Step 4 In the Enter Expression field, enter **D**. A drop-down list appears, displaying functions that begin with D.

Step 5 Choose **DIFF_DAY(date1, date2)**.

Step 6 For the first argument, enter a left square bracket ([) and choose the first date column from the drop-down list. For example, choose **Date Requested**.

Step 7 For the second argument, enter a left square bracket ([) and choose the second date column from the drop-down list. For example, choose **Actual Shipping Date**.

Step 8 Validate the expression, and then click **Apply**. The new calculated column appears in the report, displaying the difference between the two dates.

Step 9 To save your changes, see Saving Customized Reports, page 24-39.

Filtering Report Data

Filters limit the data that appears in reports. For example, by using a database of customer data, you can use filters to run a report that lists only the customers in a specific state or province, or only the customers whose purchases total more than US$1.5 million. To limit the data even more, you can, for example, list customers in a specific state who have credit limits of less than US$50,000 and who have not made a purchase in the past 90 days.

This section covers the following tasks:

- Creating Filters, page 24-24
- Creating a Multiple Condition Filter, page 24-26
- Working with Aggregate Data, page 24-28
- Creating a Multiple Condition Filter, page 24-26
- Deleting One Condition in a Multiple Condition Filter, page 24-27

Creating Filters

A filter is based on one or more fields in a report. To create a filter based on a single field, you select a condition and a value. For example, you can create a filter that returns values that are equal to a specified value, less than a specified value, between two values, and so on.

To create a data filter, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a column, and do one of the following:

- Click the **Filter** icon on the toolbar.
- Right-click and choose **Filter > Filter** from the context menu.

The Filter dialog appears.

Note If the detail column that you selected is a merged column, the Select Data Item dialog box appears.

Step 3 Select a condition from the drop-down menu. Additional fields may appear, depending on the condition that you choose.

Step 4 Do one of the following:

- Enter values for each field. To view all possible values, click **Select Values** and then choose from the drop-down menu.
- To search for a value, enter the value in the Find Value field, and click **Find**. All values that match your filter text are returned. Double-click a value to select it. The value appears in the Value field.

Step 5 Click **Apply**.

Step 6 To save your changes, see Saving Customized Reports, page 24-39.

For more information:

See Filters, page A-38 of Appendix A, "User Interface Reference," for details on the fields.

Modifying or Removing a Filter

After you create a filter for a report, it is easy to change or remove the filter, as shown in the following task.

Prerequisites

Before you begin, you should have successfully completed the task for Creating Filters, page 24-24.

To modify or remove a data filter, complete the following steps:

Step 1 Select the column that uses the filter, and do one of the following:

- Click the **Filter** icon on the toolbar.
- Right-click and choose **Filter > Filter** from the context menu.

The Filter dialog appears, displaying the existing filter condition.

Step 2 To modify the filter, change the **c**ondition or values.

Step 3 To remove the filter, click **Clear**.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

For more information:

See Filters, page A-38 of Appendix A, "User Interface Reference," for details on the fields.

Filtering for Highest or Lowest Values

When a table contains hundreds of rows, it can be helpful to display the highest or lowest values in a column. For example, you might want to view the ten sales representatives who produce the most revenue or the top 25 percent of energy consumers.

Prerequisites

Before you begin, you should have successfully completed the task for Creating Filters, page 24-24.

To filter for highest or lowest values, complete the following steps:

Step 1 Right-click inside a column and choose **Filter >Top or Bottom N** from the context menu. The Top or Bottom N dialog box appears.

Step 2 From the Filter drop-down menu, select a particular number or percentage of rows.

Step 3 Enter a value in the field next to the Filter menu to specify the number or percentage of rows to display.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

For more information:

See Filters, page A-38 of Appendix A, "User Interface Reference," for details on the fields.

Creating a Multiple Condition Filter

You can create a filter with more than one condition. For example, you can create a filter that retrieves the names of customers who have a specific credit rank and who have open orders totaling between US$250,000 and US$500,000.

Advanced Filter options provide flexibility in setting filter values. For conditions that test equality and for the Between condition, you can either set a literal value or you can base the value on another data column. For example, you can request actual shipping dates that are greater than the forecast shipping dates, or actual sales that are less than sales targets.

To create a filter with multiple conditions, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a column and do one of the following:

- Click the **Filter** icon on the toolbar.
- Right-click and choose **Filter > Filter** from the context menu.

The Filter dialog appears.

Step 3 Click **Advanced Filter**. The Advanced Filter dialog box appears. The Filter By field displays the name of the first column in the report.

Step 4 From the Filter By menu, select the column that contains the data that you want to filter.

Step 5 In the Condition field, select a condition, such as Equal To, Between, or Less Than.

Step 6 Choose one of the following options for the **Value**:

- **Specify Literal Value**—This default value allows you to specify a literal value. To do so, enter a value in the field provided. If you choose **Select Values**, a field appears that displays all data values for the specified column. For long lists, you can find a value by entering the value in the Filter Text field and clicking **Find**.
- **Use Value from Data Field**—When you choose **Use Value from Data Field**, a drop-down list of columns appears. The columns in this list have the same data type as the column that you selected in the Filter By field.

Step 7 Click **Add Condition**, and then click **Validate** to validate the filter syntax. Repeat from Step 4 through Step 7 to create additional filter conditions.

Step 8 In the Filters area, adjust the filter conditions as needed. You can combine the conditions in the following ways:

- Using the AND, OR, and NOT operators. By default, the second filter condition is preceded by AND.

  AND means that both conditions must be true for a data row to appear in the report. You can change AND to OR by choosing OR. OR means that only one condition has to be true for a data row to appear in the report. If you choose NOT, NOT appears after the AND or OR. NOT means that the condition must be false for a data row to appear in the report.

- If you add more than one condition, you can use parentheses to group conditions.

  If you enclose two or more filter conditions in parentheses, the conditions in the parentheses are evaluated first. Then, the entire filter expression is evaluated. For example, A AND B OR C is evaluated from left to right, so A and B must be true, or C must be true for a data row to appear in the report. In the combination A AND (B OR C), B OR C is evaluated first, so A must be true, and B or C must be true for a data row to appear in the report.

Step 9 Click **Apply**.

Step 10 To save your changes, see Saving Customized Reports, page 24-39.

Deleting One Condition in a Multiple Condition Filter

If you created a filter with multiple conditions, it is easy to delete one of the conditions without deleting the entire filter.

Prerequisites

Before you begin, you should have successfully completed the task for Creating a Multiple Condition Filter, page 24-26.

To delete one condition in a multiple condition filter, complete the following steps:

Step 1 Select the column that uses the filter, and do one of the following:

- Click the **Filter** icon on the toolbar.
- Right-click and choose **Filter > Filter** from the context menu.

The Filter dialog appears.

Step 2 Click **Advanced Filter**. The lower portion of the Advanced Filter dialog displays the filter conditions.

Step 3 Select the filter condition that you want to remove, and then click **Delete**.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Working with Aggregate Data

An aggregate row displays a total, average, or other summary data for a column. For example, you can display the total amount of the customer purchases or the average amount of each order. You can also create calculations, such as sums, standard deviations, rankings, and differences.

This section covers the following topics:

- Adding an Aggregate Row, page 24-28
- Adding Additional Aggregate Rows, page 24-29
- Deleting Aggregate Rows, page 24-29

Adding an Aggregate Row

Typically, the default formatting of the aggregate row comes from the template or the theme.You can modify the formatting of the aggregate data value and the formatting of the label that precedes the data value. You cannot modify the text of the label or the data value.

To create an aggregate data row, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select a column, and then select **Aggregation**. The Aggregation dialog box appears. The name of the column that you selected is listed in the Selected Column field.

Step 3 From the Select Function menu, choose the appropriate function. The available functions depend on the type of data in the column:

- For text data, you can count all the values in the column, or count the distinct values in the column, for example.
- For numeric data, you can count values, get an average value or a weighted average, total the values in the column, and so on.

Step 4 In the Aggregate On field, do the following:

- Specify whether to display the aggregate value in the table header or footer. The default is to display the aggregate value in the table footer.
- If the selected column is a *grouped* column, specify whether to display the aggregate value in the group header or footer.

Step 5 Click **Apply**. The aggregate data appears in the report.

Step 6 To save your changes, see Saving Customized Reports, page 24-39.

Adding Additional Aggregate Rows

After you create a single aggregate row for a column, you can add up to two more aggregate rows for the same column. For an item total column, for example, you can create a sum of all the values, count all the values, and get the average order total.

To add additional aggregate rows to a report, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 To add an aggregate row, select a calculated column that contains an aggregate row, and then select **Aggregation**. The Aggregation window appears.

Step 3 Click **Add Aggregation**. An additional section appears in the Aggregation dialog box.

Step 4 Create the second aggregate row, and then click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Deleting Aggregate Rows

You can delete an aggregate row in much the same way that you delete any other row in a report.

To delete an aggregate row, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Select the calculated column containing the aggregation to be removed, and then choose **Aggregation**.

Step 3 The Aggregation dialog box appears, displaying the aggregations for the column.

Step 4 Select the aggregation that you want to remove, and then choose **Delete Aggregation** and click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Working with Charts

A **chart** is a graphical representation of data, or the relationships among data sets. Charts display complex data in an easy-to-assimilate format. A chart displays data as one or more sets of points, and organizes data points into sets of values called series. There are two types of series:

- Category series—The category series typically determines what text, numbers, or dates you see on the x-axis.
- Value series—The value series typically determines the text, numbers, or dates on the y-axis.

There are various chart types. Some types of data are best depicted with a specific type of chart. Charts can be used as reports in themselves, and they can be used together with tabular data report styles.

Note The basic characteristics of a chart are determined in the report design editor. Such things as the chart type and the data source are part of the report design and cannot be changed in the viewer.

This section covers the following tasks:

- Filtering Chart Data, page 24-30
- Changing Chart Subtypes, page 24-30
- Changing Chart Formatting, page 24-31

Filtering Chart Data

The data that is displayed in the chart can be filtered similar to how a data column is filtered. You can filter a chart along either the x-axis or the y-axis.

To filter chart data, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click on the chart and select **Filter** from the context menu. The Chart Filter dialog appears.

Step 3 Make your selections from the Chart Filter dialog, and click **Apply**.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Changing Chart Subtypes

Many charts have two-dimensional subtypes that you can select from to change how the chart shape appears. Some charts are two-dimensional and appear as flat against the background, while others can be displayed with depth in 3-D.

The chart subtypes from which you can select include the following:

- Bar chart—Side-by-side, stacked, percent stacked
- Line chart—Overlay, stacked, percent stacked
- Area chart—Overlay, stacked, percent stacked
- Meter chart—Standard, superimposed
- Stock chart—Candlestick, bar stick

To specify a new chart subtype, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside the chart, and select **Chart Subtype** from the context menu.

Step 3 Select the desired subtype from the Chart Subtype dialog and click **Apply**.

Step 4 To save your changes, see Saving Customized Reports, page 24-39.

Changing Chart Formatting

Some chart formatting, such as the colors of the bars in a bar chart and the background color of the chart, come from the report template or theme. If the formatting comes from a report template, you are not allowed to change the formatting. If the formatting comes from a theme, you are allowed to change the formatting by changing the theme. For more information, see Formatting Reports, page 24-32.

This procedure shows you how to modify other chart format items, including fonts and font sizes for the chart title and axis labels; the height and width of the chart; how to hide axis labels; how to place labels at an angle relative to the axis; and how to hide the legend or determine where to display the legend in relation to the chart.

To modify the formatting of chart data, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside the chart, and choose **Chart Format** from the context menu.

Step 3 From the Chart Format dialog, do any of the following:

- Edit and format the default chart title.
- Edit and format the default title for the category (x-axis).
- Modify settings for the labels on the x-axis in the following ways:
  - Indicate whether to display x-axis labels.
  - Indicate whether to rotate x-axis labels and set the degree of rotation.
  - Indicate whether to stagger x-axis labels. For example, you can show data points for every third month, every 10 days, every other year, and so on.
  - Set the interval for staggered x-axis labels.
- Edit and format the default title for the y-axis, if the chart uses a y-axis.
- Set the height and width of the chart.
- Select the dimension. The options are 2-dimensional and 2-dimensional with depth.
- Indicate whether to flip, or reverse, the chart's x- and y-axes.
- Indicate whether to show a legend, and if so, whether to place it above the chart, below the chart, or to the left or right of the chart.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Formatting Reports

This section shows you the various ways in which you can format reports using the Interactive Viewer, and it covers the following topics:

- Editing and Formatting Labels, page 24-32
- Formatting Data Types, page 24-33
- Applying Conditional Formats, page 24-36
- Setting and Removing Page Breaks, page 24-37

Editing and Formatting Labels

Labels are fields that can contain static text, such as the report title and items of the footer. In a typical report, some labels are editable and others are not. If a label such as a column header is editable, you can modify properties such as the type of font, font size, background color, and the text of the label.

Editing Labels

The text of a column header comes from the data source. If the data source displays column headers in capital letters with no spaces between words, the report design displays column header names in the same way. You are allowed to change the content of the column header.

To edit report label text, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click the label that you want to change.

Step 3 From the context menu, choose **Change Text**. The Edit Text dialog box appears.

Step 4 Modify the text and click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Formatting Labels

The formatting of the column header comes from the report template or from the theme. If the formatting comes from a report template, you are not allowed to change the formatting. If the formatting comes from a theme, you are allowed change the formatting by changing the theme.

To change report label formatting, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Click the **Launch Interactive Viewer** icon, and right-click the label.

Step 3 From the context menu, choose **Style > Font**. The Font dialog box appears.

Step 4 Modify the formats as necessary, and then click **Apply**.

Step 5 To save your customizations, see Saving Customized Reports, page 24-39.

Formatting Data Types

Reports can contain many different data types. A column can display numeric data, date-and-time data, or string data. Each data type has a range of unique formats. For more information on the various data types and how you can format them, see Reports, page A-15 of Appendix A, "User Interface Reference."

This section shows you how to perform the following tasks:

- Formatting Numeric Data, page 24-33
- Formatting Custom Numeric Data, page 24-34
- Formatting String and Custom String Data, page 24-35
- Formatting Date and Time, page 24-35
- Formatting Boolean Data, page 24-36

Formatting Numeric Data

Numeric data can take several forms. A column of postal codes requires different formatting than a column of sales figures.

The data type of a column is determined by the data source. Keep in mind that a text or string data type can contain numeric digits. A telephone number, for example, is frequently string data in the data source. The title of the formatting dialog box tells you what data type the column contains.

To format numeric data, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a column containing numeric data, and choose **Format** from the context menu. The Number column format dialog box appears.

Step 3 In the Format Number As field, select one of the following:

- General Number
- Currency

- Fixed
- Percent
- Scientific

The dialog options change to match the selected formatting type.

Step 4 Specify the following options, as appropriate for the selected formatting type:

- Symbol—Select a currency symbol.
- Symbol Position—Choose **Before** to place the currency or percentage symbol before the number. Choose **After** to place the symbol after the number.
- Decimal Places—Select the number of places to display after the decimal marker.
- Use 1000s Separator—Select to use a thousands separator such as a comma (,) or a period (.). Your locale determines the separator character.
- Negative Numbers—Select to display negative numbers. You can use a minus (-) sign before the number or parentheses around the number.

Step 5 Click **Apply**.

Step 6 To save your changes, see Saving Customized Reports, page 24-39.

Formatting Custom Numeric Data

To define a custom format, you can use special symbols to construct a format pattern. A format pattern shows where to place currency symbols, thousands separators, decimal points, or commas.

To format custom or numeric data, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a numeric data column, and choose **Format** from the context menu. The Number column format appears.

Step 3 In the Format Number As field, choose **Custom** from the drop-down list. The Format Code field appears.

Step 4 Enter a format pattern in the Format Code field.

Step 5 Click **Apply**.

Step 6 To save your changes, see Saving Customized Reports, page 24-39.

For more information:

See Data Formatting, page A-26 of Appendix A, “User Interface Reference,” for details on the fields.

Formatting String and Custom String Data

You can change the format of string data and even include special formatting, such as a space or a punctuation mark, at a specific place in the string. The following example shows the various ways that you can format the display of telephone numbers:

(415) 555-2121

415.555.2121

415-555-2121

To format string and custom string data, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a column containing string data, and choose **Format** from the context menu. The String column format dialog appears.

Step 3 Select the appropriate option from the drop-down menu, or choose **Custom** for custom formatting and enter a format pattern in the Format Code field.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

For more information:

See Data Formatting, page A-26 of Appendix A, "User Interface Reference."

Formatting Date and Time

A data source can provide both a date and a time, or only the date or time. If the data source provides both date and time data, you can format the column to display only a date, only a time, or both a date and a time. You can also specify the exact format for the date or time.

Standard Date and Time Formatting

The appearance of standard date and time formatting adheres to the locale standards in which you are viewing the report. For example, the following date and time format is correct for the U.S. English locale for the Pacific Standard Time zone:

March 5, 2007 11:00:00 AM PST

The following example shows the correct date and time format for a French (France) locale:

5 mars 2007 11:00:00 HNP (ÈUA)

Custom Date and Time Formatting

You should only use custom date formatting, if your report is intended for a single locale. Custom formats display dates in the format that you specify, and that format might be misinterpreted in other locales. For example, for the date format mm-dd-yy, the date January 10, 2006 appears as 01-10-06, regardless of the locale in which the report is viewed. For locales in which dates are typically displayed in date-month-year format, a 01-10-06 date would be interpreted as October 1, 2006.

To change the date and time format, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a column that contains date or time data, and choose **Format** from the context menu.

Step 3 To choose a standard format, select an option from the Format Date or Time As drop-down menu.

Note Selecting a standard date and time format ensures that the appropriate format is displayed for the locale, no matter where in the world the report is viewed.

Step 4 To specify a custom format, choose **Custom** from the Format Date or Time As drop-down menu and enter a format pattern in the Format Code field.

Step 5 Click **Apply**.

Step 6 To save your changes, see Saving Customized Reports, page 24-39.

For more information:

See Data Formatting, page A-26 of Appendix A, "User Interface Reference," or details on the fields.

Formatting Boolean Data

A Boolean expression evaluates to true or false. For example, you create a calculated column with the following expression:

ActualShipDate <= TargetShipDate

If the actual ship date is before or on the target ship date, the expression = true. If the actual ship date is after the target ship date, the expression = false. If you do not format a Boolean data type column, it displays, by default, the values of true and false.

To specify labels for Boolean data other than the defaults of true and false, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, then click **Launch Interactive Viewer**.

Step 2 Right-click inside a Boolean data column and choose **Format Data** from the context menu.

Step 3 Enter the labels as you want them to appear in the Boolean Column Format fields.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Applying Conditional Formats

Conditional formatting changes the formatting of data when a certain condition is true. For example, in a report that shows past-due invoices, you can highlight in red customer names with invoices that are 90 days or more past due. You can specify up to three conditional formatting rules for a single column. You can also remove or modify conditional formatting.

Conditional formatting allows you to set various types of comparisons, such as whether the data in the comparison column is null or false. You can also compare the column value to one or two other values. For example, you can specify that data less than or equal to a specified value triggers conditional formatting.

You can also create a condition to determine whether a value is between two other values, such as whether an order total is between US$10,000 and US$100,000. In this case, the names of the customers whose orders total between US$10,000 and US$100,000 would appear in conditional formatting.

After you create the condition, you specify the format in which the data is displayed when it meets the condition.

To set up conditional formatting for a column, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a column and choose **Style > Conditional Formatting** from the context menu. The Selected Column field displays the name of the column that will display the conditional format.

Step 3 Set the conditional formatting rule in the following way:

a. In the first drop-down list, select the column that contains the values that determine whether the conditional format takes effect. The column that you select can be the same as or different from the column in the Selected Column field.

b. In the next field, select an operator from the drop-down menu to apply to the column. You can choose **Equal to**, **Less than**, **Less than or Equal to**, and so on.

The fields that do or do not appear depend on your selection. If you choose **Is Null**, **Is Not Null**, **Is True**, or **Is False**, no fields appear. If you choose an operator that requires a comparison between values, one or more additional fields appear.

c. As needed, enter comparison values in each field.

For example, if you choose **Less than or Equal to** a third field appears, or if you choose **Between or Not Between**, two comparison fields appear. Comparison values can be entered directly, or you can choose **Change Value** and select a value from the Value dialog.

Step 4 To change the display formatting, on the Conditional Formatting dialog, choose **Format**.

You can set the font, font size, font color, and background color. You can also specify bold, italic, or underlined formatting.

Step 5 To add additional conditional formatting rules, on the Conditional Formatting dialog, choose **Add Rule**, and repeat Step 3 and Step 4 for each new rule.

Step 6 Click **Apply**.

Step 7 To save your changes, see Saving Customized Reports, page 24-39.

Setting and Removing Page Breaks

By using the Interactive Viewer, you can force page breaks after a specified number of rows for detail and group columns. This section covers the following tasks:

- Setting and Removing Page Breaks for Detail Columns, page 24-38
- Setting and Removing Page Breaks in a Group Column, page 24-38

Setting and Removing Page Breaks for Detail Columns

You may want to break a column after a specified set of rows to keep related information together when a report is printed. You can use the Interactive Viewer to add page breaks to your reports or remove page breaks from them.

Note The following task is specific to detail columns. For group columns, use the Setting and Removing Page Breaks in a Group Column, page 24-38 procedure.

To set and remove page breaks in detail columns, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then click **Launch Interactive Viewer**.

Step 2 Right-click inside a detail column, and choose **Group > Page Break** from the context menu.

Step 3 In the **Interval** field, do one of the following:

- Enter the number of rows after which to place the page break. The default is 50.
- Change an existing page break by modifying the number that appears in the Interval field, or remove the number entirely.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Setting and Removing Page Breaks in a Group Column

For reports with grouped data, you can set page breaks before or after the grouped data. These boundaries allow you to make sure grouped data stays together when it is printed, so it is easier to read and understand.

Note The following task is specific to group columns. For detail columns, use the Setting and Removing Page Breaks for Detail Columns, page 24-38 procedure.

To set and remove page breaks in a grouped column, complete the following steps:

Step 1 Open and run a report, as described in Running, Viewing, and Navigating Reports, page 24-3, and then create a group column as described in Adding Groups, page 24-13.

Step 2 Right-click inside a group column, and choose **Group > Page Break** from the context menu.

Step 3 Do one of the following:

- Under Before Group and After Group click the appropriate radio button for the following:
  - Always
  - Always Except for First
  - Always Except for Last
- To delete an existing page break, choose **None** for Before Group or After Group.

Step 4 Click **Apply**.

Step 5 To save your changes, see Saving Customized Reports, page 24-39.

Saving Customized Reports

You can save a report design from the Interactive Viewer for reuse at a later time.

Prerequisites

Create a customized report design, as described in the Organizing and Formatting Report Data, page 24-12 tasks.

To save a customized report under a unique name, complete the following steps:

Step 1 Click **Save As**. The Save As dialog box appears.

Step 2 Navigate to the location where you want to save the file, and enter a unique filename.

Step 3 Click **Save**, and then click **OK**.

Working with Active RADIUS Sessions

ISE provides a dynamic Change of Authorization (CoA) feature for the RADIUS Active Sessions report that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a network access device (NAD) to perform the following tasks:

- Troubleshoot issues related to authentication—You can use the Disconnect:None option to follow up with an attempt to reauthenticate again. However, you must not use the disconnect option to restrict access. To restrict access, use the shutdown option.
- Block a problematic host—You can use the Disconnect:Port Disable option to block an infected host that sends a lot of traffic over the network. However, the RADIUS protocol does not currently support a method for re-enabling a port that has been shut down.
- Force endpoints to reacquire IP addresses—You can use the Disconnect:Port Bounce option for endpoints that do not have a supplicant or client to generate a DHCP request after VLAN change.
- Push an updated authorization policy to an endpoint—You can use the Re-Auth option to enforce an updated policy configuration, such as a change in the authorization policy on existing sessions based on the discretion of the administrator. For example, if posture validation is enabled, when an endpoint gains access initially, it is usually quarantined. After the identity and posture of the endpoint are known, it is possible to send the CoA Re-Auth command to the endpoint for the endpoint to acquire the actual authorization policy based on its posture.

For CoA commands to be understood by the device, it is important that you configure the options appropriately.

For CoA to work properly, you must configure (in ISE) the shared secret of each device that requires a dynamic change of authorization. ISE uses the shared secret configuration to request access from the device and issue CoA commands to it. For more information, see Chapter 5, “Managing External Identity Sources.”

Note In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is limited to 100,000.

Changing Authorization for RADIUS Sessions

Some network access devices on your network may not send an Accounting Stop or Accounting Off packet after a reload. As a result, you might find two sessions in the Session Directory reports, one which has expired.

To dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session, be sure to choose the most recent session.

To change authorization or disconnect an active RADIUS session, complete the following steps:

Step 1 Choose **Operations > Reports > Catalog**, and then choose the **Session Directory** category in the left-hand navigation pane.

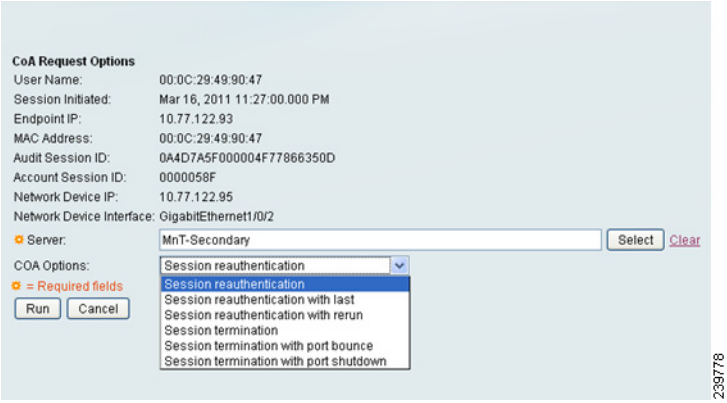
Step 2 Choose **RADIUS Active Sessions** from the list.

Step 3 Click the CoA link for the RADIUS session that you want to issue CoA with reauthenticate or terminate options.

The Change of Authorization Request page appears.

Step 4 Click **Select** and choose a server from which the CoA communicates to the network device. The network device is shown as the Network Device IP in the following illustration.

Figure 24-5 CoA Request Options



Step 5 Choose one of the following CoA options from the drop-down list:

Note For Inline Posture nodes and where wireless LAN controllers (WLC) are in use, only two options are available: Session reauthentication and Session termination.

- **Session reauthentication**—Reauthenticate session.
- **Session reauthentication with last**—Use the last successful authentication method for this session.
- **Session reauthentication with rerun**—Run through the configured authentication method from the beginning.

Note **Session reauthentication with last** and **Session reauthentication with rerun** options are not currently supported in Cisco IOS.

- **Session termination**—Just end the session. The switch re-authenticates the client in different session.
- **Session termination with port bounce**—Terminate session and restart port.
- **Session termination with port shutdown**—Terminate session and shutdown port.

Step 6 Click **Run** to issue CoA with selected reauthenticate or terminate option.

If your CoA fails, it could be for any of the following reasons:

- Device does not support CoA.
- Changes have occurred to the identity or authorization policy.
- There is a shared secret mismatch.

Step 7 To save your changes, see Saving Customized Reports, page 24-39.

For more information:

See Troubleshooting RADIUS Authentications, page 23-31. A failed dynamic CoA will be listed under failed RADIUS authentications.

For information on CoA, policies, and profiles, see the following:

- Cisco ISE Authorization Policies and Profiles, page 17-5
- Configuring Authorization Policies, page 17-14
- Chapter 18, “Configuring Endpoint Profiling Policies”
- Chapter 20, “Configuring Client Posture Policies”

Troubleshooting Topics

- Cisco ISE Does Not Issue CoA Following Authentication, page D-28
- CoA Not Initiating on Client Machine, page D-3
- RADIUS Server Error Message Entries Appearing in Cisco ISE, page D-14
- RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE), page D-15

Available Reports

The following table lists the preconfigured catalog reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided.

Table 24-1 Available Reports

Report Name	Description	Logging Category
AAA Protocol		
AAA_Diagnostics	Provides AAA diagnostic details based on severity for a selected time period.	Policy diagnostics, Identity Stores Diagnostics, Authentication Flow Diagnostics, RADIUS Diagnostics
Authentication_Trend	Provides RADIUS authentication summary information for a selected time period, along with a graphical representation.	Passed authentications, Failed attempts
RADIUS_Accounting	Provides user accounting information that is based on RADIUS for a selected time period.	RADIUS accounting
RADIUS_Authentication	Provides RADIUS authentication details for a selected time period.	Passed authentications, Failed attempts
Allowed Protocol		
Allowed_Protocol_Authentication_ Summary	Provides RADIUS authentication summary information for a particular allowed protocol for a selected time period, along with a graphical representation.	Passed authentications, Failed attempts
Top_N_Authentications_By_ Allowed_Protocol	Provides the top *n* passed, failed, and total authentication count for RADIUS authentications with respect to the allowed protocol for a selected time period.	Passed authentications, Failed attempts
Server Instance		
OCSP Monitoring	Provides a summary of all the OCSP certificate validation operations performed by Cisco ISE.	System statistics
Server_Administrator_Entitlement	Provides a list of administrators and their assigned entitlement roles.	Resources and privileges, configuration changes, logins
Server_Administrator_Logins	Provides access-related events for administrators that includes login, logout, events, and information about excessive failed login attempts over standalone, and other distributed nodes when the account is locked or disabled in Cisco ISE.	Administrative and operational audit

Table 24-1 Available Reports (continued)

Report Name	Description	Logging Category
Server_Authentication_Summary	Provides RADIUS authentication summary information for a particular instance for a selected time period, along with a graphical representation. This report could take several minutes to run, depending on the number of records in the database. **Note** When you reload this report, if the rate of incoming syslog messages is around 150 messages per second or more, the total number of passed and failed authentications that appears above the graph and the passed and failed authentication count displayed in the table, do not match.	Passed authentications, Failed attempts
Server_Configuration_Audit	Provides all the configuration changes made by the administrator for a selected time period.	Administrative and operational audit
Server_Health_Summary	Provides the CPU, memory utilization, RADIUS data and throughput (in tabular and graphical formats), as well as process status, process downtime, and disk space utilization for a particular instance in a selected time period.	System statistics
Server_Operations_Audit	Provides all the operational changes made by the administrator for a selected time period.	Administrative and operational audit
Server_System_Diagnostics	Provides system diagnostic details that are based on severity for a selected time period.	Internal operations diagnostics, distributed management, administrator authentication and authorization
Top_N_Authentications_By_Server	Provides the top *n* passed, failed, and total authentication count for RADIUS protocol with respect to a particular ISE instance for a selected time period.	Passed authentications, Failed attempts
User_Change_Password_Audit	Provides the username of the internal user, identity store name, name of the instance, and time when the user password was changed. Helps track all changes that are made to internal user passwords across all interfaces.	Administrative and operational audit
Endpoint		
Endpoint_MAC_Authentication_ Summary	Provides the RADIUS authentication summary information for a particular MAC or MAB for a selected time period; along with a graphical representation.	Passed authentications, Failed attempts

Table 24-1 Available Reports (continued)

Report Name	Description	Logging Category
Endpoint_Profiler_Summary	Provides profile information for endpoints that are accessing the network. **Note** For endpoints that do not register a session time, such as a Cisco IP-Phone, the term Not Applicable is shown in the Endpoint session time field.	Profiler
Endpoint_Time_To_Profile	Provides information on time taken to an endpoint that has an Unknown profile by using a particular MAC address for a selected time period.	Profiler
Top_N_Authentications_By_Endpoint _Calling _Station_ID	Provides the top *n* passed, failed, and total authentication count with respect to endpoint calling station IDs.	Passed authentications, Failed attempts
Top_N_Authentications_By_Machine	Provides the top *n* passed, failed, and total authentication count for RADIUS protocol with respect to machine information for a selected time period.	Passed authentications, Failed attempts
Failure Reason		
Authentication_Failure_Code_Lookup	Provides the description and the appropriate resolution steps for a particular failure reason.	—
Failure_Reason_Authentication_ Summary	Provides the RADIUS authentication summary information for a particular failure reason, along with a graphical representation for a selected time period.	Failed attempts
Top_N_Authentications_By_Failure_ Reason	Provides the top *n* failed authentication count for RADIUS protocols with respect to the failure reason for a selected time period.	Failed attempts
Network Device		
AAA_Down_Summary	Provides the number of AAA unreachable events that a NAD logs within a selected time period.	Passed authentications, Failed attempts
Network_Device_Authentication_ Summary	Provides the RADIUS authentication summary information for a particular network device for a selected time period, along with the graphical representation.	Passed authentications, Failed attempts
Network_Device_Log_Messages	Provides the log information of a particular network device for a specified time period.	Passed authentications, Failed attempts

Table 24-1 Available Reports (continued)

Report Name	Description	Logging Category
Session_Status_Summary	Provides the port sessions and status of a particular network device obtained by the Simple Network Management Protocol (SNMP). **Note** If you have configured your network device with SNMPv3 parameters, you cannot generate the Network Device Session Status Summary report provided by the Monitoring service (**Operations > Reports > Catalog > Network Device > Session Status Summary**). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.	—
Top_N_AAA_Down_By_Network_Device	Provides the top *n* AAA down events that is encountered by each of the network devices.	—
Top_N_Authentications_By_Network_Device	Provides the top *n* passed, failed, and total authentication count for RADIUS protocols with respect to a network device for a selected time period.	Passed authentications, Failed attempts
User		
Client_Provisioning	Provides a summary of successful and unsuccessful client provisioning evaluation and download events, displayed according to the associated User ID.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics
Guest_Accounting	Provides session (login and log out) information for selected guests over a specified time period.	Passed authentications, RADIUS accounting
Guest_Activity	Provides guest information for a selected time period. **Note** For this report to collect and display the list of URLs visited by the guest user, you must enable guest access syslog configuration on the NAD that inspects guest traffic in your ISE network.	Passed authentications
Guest_Sponsor_Summary	Provides sponsor information along with a graphical representation, for a selected time period.	Passed authentications
Top_N_Authentications_By_User	Provides top *n* passed, failed, and total authentication count for RADIUS protocol with respect to users for a selected time period.	Passed authentications, Failed attempts
Unique_Users	Provides the count for the number of unique users.	Passed authentications, Failed attempts
User_Authentication_Summary	Provides RADIUS authentication summary information for a particular user for a selected time period, along with the graphical representation.	Passed authentications, Failed attempts
Security Group Access		
PAC Provisioning	Provides a summary of SGA PAC generated.	—

Table 24-1 Available Reports (continued)

Report Name	Description	Logging Category
Policy CoA	Provides the summary of the policy change request through policy CoA.	—
RBACL_Drop_Summary	Provides a summary of RBAC drop events.	—
SGT_Assignment_Summary	Provides a summary of security group tag (SGT) assignments for a selected time period.	Passed authentications
Top_N_RBACL_Drops_By_Destination	Provides the top *n* role-based access control list (RBAC) drop event count with respect to destination for a selected time period.	—
Top_N_RBACL_Drops_By_User	Provides the top *n* RBAC drop event count with respect to the user for a selected time period.	—
Top_N_SGT_Assignments	Provides the top *n* SGT assignment count for a selected time period.	Passed authentications
Session Directory		
RADIUS_Active_Sessions	Provides information on RADIUS authenticated, authorized, and started sessions. Dynamically control active RADIUS sessions. Send a reauthenticate or disconnect request to a NAD to perform the following CoA actions: • Quarantine • Session reauthentication • Session reauthentication with last • Session reauthentication with rerun • Session termination • Session termination with port bounce • Session termination with port shut down The RADIUS_Active_Sessions report will display WLC Roam status as N (N stands for No) for any wired active session.	Passed authentications, RADIUS accounting
RADIUS_Session_History	Provides a summary of RADIUS session history, such as total authenticated and terminated sessions, as well as total and average session duration and throughput for a selected time period.	Passed authentications, RADIUS accounting
RADIUS_Terminated_Sessions	Provides all the RADIUS terminated session information for a selected time period.	Passed authentications, RADIUS accounting
Posture		
Posture_Detail_Assessment	Provides a summary of all the endpoints that logged on for a selected period of time. Includes a detailed status of compliance against the posture policies that are used during posture assessment.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics

Table 24-1 Available Reports (continued)

Report Name	Description	Logging Category
Posture_Trend	Provides a graphical representation of posture compliance for a selected period of time. Includes a summary of compliant and noncompliant endpoints against which the posture policies were evaluated.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics
Endpoint Protection Service		
Endpoint_Operations_History	Provides EPS action history information, comprised of these values: Timestamp, Endpoint MAC Address, Endpoint IP Address, Operation Type, Operation Status, Operation ID, Audit Session ID, Admin Username, Admin IP Address.	—



PART 5

Reference



APPENDIX A

User Interface Reference

This chapter is a reference for Identity Services Engine (ISE) user interface elements, and covers the following main elements:

- Operations, page A-1
- Policy, page A-54
- Administration, page A-58

Operations

This section covers the following subtabs:

- Authentications, page A-1
- Alarms, page A-3
- Reports, page A-15
- Troubleshoot, page A-40

Authentications

Go to **Operations > Authentications** to display the Authentications page. Authentications data categories are described in the following table.

Table A-1 Authentications

Option	Description
Time	Shows the time that the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.
Status	Shows if the authentication was successful or a failure. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.
Details	Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more-detailed information on the selected authentication scenario. This column is required and cannot be deselected.
Username	Shows the username that is associated with the authentication.

Table A-1 Authentications (continued)

Option	Description
Calling Station ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
IP Address	Shows the IP address of the endpoint device.
NAD	IP address of the network access device.

Optionally, you can choose to show the following categories:

Table A-2 Optional Authentications Categories

Option	Description
Server	Indicates the policy service ISE node from which the log was generated.
NAS Port ID	Network access server (NAS) port at which the endpoint is connected.
Failure Reason	Shows a detailed reason for failure, if the authentication failed.
SGA Security Group	Shows a security profile for the authentication.
Authorization Profiles	Shows an authorization profile that was used for authentication.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2), IEE 802.1x or dot1x, and the like.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.
SGA Security Group	Shows the trust group that is identified by the authentication log.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was generated.
Posture Status	Shows the status of posture validation and details on the authentication.

Alarms

This section covers the following:

- Alarms Inbox, page A-3
- Rules, page A-5
- Schedules, page A-14

Alarms Inbox

This section covers the following:

- Inbox, page A-3
- Edit > Alarm, page A-4
- Edit > Status, page A-4

Inbox

The **Operations > Alarms > Inbox** options are as follows:

Table A-3 Inbox

Option	Description
Severity	*Display only*. Indicates the severity of the associated alarm. Options are: • Critical • Warning • Info
Name	Indicates the name of the alarm. Click to display the Alarms: Properties page and edit the alarm.
Time	*Display only*. Indicates the time of the associated alarm generation in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = Day of the month, from 01 to 31. • hh = Hour of the day, from 00 to 23. • mm = Minute of the hour, from 00 to 59. • ss = Second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit year.
Cause	*Display only*. Indicates the cause of the alarm.
Assigned To	*Display only*. Indicates who is assigned to investigate the alarm.

Table A-3 Inbox (continued)

Option	Description
Status	*Display only*. Indicates the status of the alarm. Options are: • New—The alarm is new. • Acknowledged—The alarm is known. • Closed—The alarm is closed.
Edit	Check the check box next to the alarm that you want to edit, and click **Edit** to edit the status of the alarm and view the corresponding report.
Close	Check the check box next to the alarm that you want to close, and click **Close** to close the alarm. You can enter closing notes before you close an alarm. **Note** Closing an alarm only removes the alarm. It does not delete the alarm.
Delete	Check the check box next to the alarm that you want to delete, and click **Delete** to delete the alarm.

Edit > Alarm

Click **Edit** on the Inbox to bring up this page that provides information on the event that triggered the alarm. You cannot edit any of the fields in the Alarm tab. The options are shown in the following table.

Table A-4 Edit Alarm

Option	Description
Occurred At	Date and time when the alarm was triggered.
Cause	The event that triggered the alarm.
Detail	Additional details about the event that triggered the alarm. ISE usually lists the counts of items that exceeded the specified threshold.
Report Links	Wherever applicable, one or more hyperlinks are provided to the relevant reports that allow you to further investigate the event.
Threshold	Information on the threshold configuration.

Edit > Status

Click **Edit** on the Inbox to bring up this page that allows you to edit the status of the alarm and add a description to track the event. The options are shown in the following table.

Table A-5 Edit Status

Option	Description
Status	Status of the alarm. When an alarm is generated, its status is New. After you view the alarm, change the status of the alarm to Acknowledged or Closed to indicate the current status of the alarm.
Assigned To	(Optional) Specify the name of the user to whom this alarm is assigned.
Notes	(Optional) Enter any additional information about the alarm that you want to record.

Rules

Click **Operations > Alarms > Rules** to specify parameters for the following alarm rules:

- Passed Authentications, page A-6
- Failed Authentications, page A-8
- Authentication Inactivity, page A-9
- ISE Configuration Changes, page A-9
- ISE System Diagnostics, page A-10
- ISE Process Status, page A-10
- ISE System Health, page A-11
- ISE AAA Health, page A-11
- Authenticated But No Accounting Start, page A-12
- Unknown NAD, page A-12
- External DB Unavailable, page A-13
- RBACL Drops, page A-13
- NAD-Reported AAA Downtime, page A-14

Passed Authentications

Modify the fields described in the following table, to create a threshold with the passed authentication criteria.

Table A-6 Passed Authentications

Option	Description
Passed Authentications	Greater than <*count*> <**occurrences** | **%**> in the past <*time*> <***Minutes*** | ***Hours***> for a <*object*>, where: • <*count*> values can be the absolute number of occurrences or percent. Valid values are: – *count* must be in the range 0 to 99 for greater than. – *count* must be in the range 1 to 100 for lesser than. • <**occurrences** | **%**> value can be occurrences or %. • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be any of the following: – ISE Instance – User – Identity Group – Device IP – Identity Store – Allowed Protocol – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel **Note** In a distributed deployment, if there are two instances, the count is calculated as an absolute number or as a percentage for each of the instances. An alarm is triggered only when the individual count of any instance exceeds the threshold.
Filter	
ISE Instance	Choose a valid ISE instance for the threshold.
User	Choose or enter a valid username for the threshold.
Identity Group	Choose a valid identity group name for the threshold.
Device Name	Choose a valid device name for the threshold.
Device IP	Choose or enter a valid device IP address for the threshold.
Device Group	Choose a valid device group name for the threshold.
Identity Store	Choose a valid identity store name for the threshold.

Table A-6 Passed Authentications (continued)

Option	Description
Allowed Protocol	Choose a valid allowed protocol name for the threshold.
MAC Address	Choose or enter a valid MAC address for the threshold. This filter is available only for RADIUS authentications.
NAD Port	Choose a port for the network device for the threshold. This filter is available only for RADIUS authentications.
AuthZ Profile	Choose an authorization profile for the threshold. This filter is available only for RADIUS authentications.
AuthN Method	Choose an authentication method for the threshold. This filter is available only for RADIUS authentications.
EAP AuthN	Choose an EAP authentication value for the threshold. This filter is available only for RADIUS authentications.
EAP Tunnel	Choose an EAP tunnel value for the threshold. This filter is available only for RADIUS authentications.
Protocol	Configure the protocol that you want to use for your threshold.

Failed Authentications

Modify the fields described in the following table, to create a threshold with the passed authentication criteria.

Table A-7 Failed Authentications

Option	Description
Failed Authentications	Greater than <*count*> <**occurrences** | **%**> in the past <*time*> <*Minutes*|*Hours*> for a <*object*>, where: • <*count*> values can be the absolute number of occurrences or percent. Valid values must be in the range 0 to 99. • <**occurrences** | **%**> value can be occurrences or %. • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be any of the following: – ISE Instance – User – Identity Group – Device IP – Identity Store – Allowed Protocol – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel **Note** In a distributed deployment, if there are two instances, the count is calculated as an absolute number or as a percentage for each of the instances. An alarm is triggered only when the individual count of any instance exceeds the specified threshold.
Filter	
Failure Reason	Enter a valid failure reason name for the threshold.
ISE Instance	Choose a valid ISE instance for the threshold.
User	Choose or enter a valid username for the threshold.
Identity Group	Choose a valid identity group name for the threshold.
Device Name	Choose a valid device name for the threshold.
Device IP	Choose or enter a valid device IP address for the threshold.
Device Group	Choose a valid device group name for the threshold.
Identity Store	Choose a valid identity store name for the threshold.
Allowed Protocol	Choose a valid allowed protocol name for the threshold.
MAC Address	This filter is available only for RADIUS authentications.

Table A-7 Failed Authentications (continued)

Option	Description
NAD Port	This filter is available only for RADIUS authentications.
AuthZ Profile	This filter is available only for RADIUS authentications.
AuthN Method	This filter is available only for RADIUS authentications.
EAP AuthN	This filter is available only for RADIUS authentications.
EAP Tunnel	This filter is available only for RADIUS authentications.
Protocol	Configure the protocol that you want to use for your threshold.

Authentication Inactivity

Define threshold criteria based on authentications that are inactive, modifying the following fields necessary.

Table A-8 Authentication Inactivity

Option	Description
ISE Instance	Choose a valid instance for the threshold.
Device	Choose a valid device for the threshold.
Protocol	Choose the protocol for threshold.
Inactive for	Select one of the following options: • Hours—Number of hours, from 1 to 744. • Days—Number of days, from 1 to 31.

ISE Configuration Changes

Define threshold criteria based on system diagnostics in the ISE instance.

Table A-9 ISE Configuration Changes

Option	Description
Administrator	Choose a valid administrator username for the threshold.
Object Name	Enter the name of the object for the threshold.
Object Type	Choose a valid object type for the threshold.
Change	Select a administrative change for the threshold: • Any • Create—Includes “duplicate” and “edit” administrative actions. • Update • Delete
Filter	
ISE Instance	Choose a valid ISE instance for the threshold.

ISE System Diagnostics

Define threshold criteria based on system diagnostics in the ISE instance.

Table A-10 ISE System Diagnostics

Option	Description
Severity at and above	Choose the severity level for the threshold. This setting captures the indicated severity level and those that are higher within the threshold: • Fatal • Error • Warning • Info • Debug
Message Text	Enter the message text for the threshold. Maximum character limit is 1024.
Filter	
ISE Instance	Choose a valid ISE instance for the threshold.

ISE Process Status

Define rule criteria based on ISE process status.

Table A-11 ISE Process Status

Option	Description
Monitor Processes	
ISE Database	Adds the ISE database to the configuration.
ISE Database Listener	Adds the ISE management to the configuration.
ISE Application server	Adds the ISE runtime to the configuration.
ISE M&T Session	Monitors this process. If this process goes down, an alarm is generated.
ISE M&T Log Collector	Monitors this process. If this process goes down, an alarm is generated.
ISE M&T Alert Process	Monitors this process. If this process goes down, an alarm is generated.
ISE M&T Log Processor	Monitors this process. If this process goes down, an alarm is generated.
Filter	
ISE Instance	Choose a valid ISE instance for the threshold.

ISE System Health

Define threshold criteria for ISE system health.

Table A-12 ISE System Health

Option	Description
Average over the past	Select the amount of time, where <min> minutes values are: 15, 30, 45, 60
CPU	Enter the percentage of CPU usage. The valid range is from 1 to 100.
Memory	Enter the percentage of memory usage (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk I/O	Enter the percentage of disk usage (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk Space Used/opt	Enter the percentage of /opt disk space (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk Space Used/local disk	Enter the percentage of local disk space (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk Space Used/	Enter the percentage of the / disk space (greater than or equal to the specified value). The valid range is from 1 to 100.
Disk Space Used/tmp	Enter the percentage of temporary disk space (greater than or equal to the specified value). The valid range is from 1 to 100.
Filter	
ISE Instance	Choose a valid ISE instance.

ISE AAA Health

Define threshold criteria for ISE AAA Health.

Table A-13 ISE AAA Health

Option	Description
Average over the past	Select the amount of time, where <min> minutes values are: 15, 30, 45, 60
RADIUS Throughput	Enter the number of RADIUS transactions per second (lesser than or equal to the specified value). The valid range is from 1 to 999999.
RADIUS Latency	Enter the number in milliseconds for RADIUS latency (greater than or equal to the specified value). The valid range is from 1 to 999999.
Filter	
ISE Instance	Choose a valid ISE instance for the threshold.

Authenticated But No Accounting Start

Define the threshold rule criteria for a specified number of authenticated sessions for a device IP

Table A-14 Authentication But No Accounting Start

Option	Description
More than <*num*> authenticated sessions in the past 15 minutes, where accounting start event has not been received for a Device IP	<*num*>—A count of authenticated sessions in the past 15 minutes.
Filter	
Device IP	Choose or enter a valid device IP address.

Unknown NAD

Define threshold criteria based on authentications that have failed because of an unknown NAD.

Table A-15 Unknown NAD

Option	Description
Unknown NAD count	Greater than <*num*> in the past <*time*> <*Minutes*|*Hours*> for a <*object*>, where: • <*num*> values can be any five-digit number greater than or equal to zero (0). • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – ISE Instance – Device IP
Filter	
ISE Instance	Choose a valid ISE instance.
Device IP	Choose or enter a valid device IP address .
Protocol	Select a protocol for the threshold. Valid options are: RADIUS

External DB Unavailable

Define threshold criteria based on an external database that ISE is unable to connect to.

Table A-16 External DB Unavailable

Option	Description
External DB Unavailable	<*percent*|*count*> greater than <*num*> in the past <*time*> <*Minutes*|*Hours*> for a <*object*>, where: • <Percent|Count> value can be Percent or Count. • <*num*> values can be any one of the following: – 0 to 99 for percent – 0 to 99999 for count • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – ISE Instance – Identity Store
Filter	
ISE Instance	Choose a valid ISE instance.
Identity Group	Choose a valid identity group name.
Identity Store	Choose a valid identity store name.
Allowed Protocol	Choose a valid allowed protocol name.
Protocol	Select a protocol. Valid options are: RADIUS

RBACL Drops

Define the RBACL Drops threshold.

Table A-17 RBACL Drops

Option	Description
RBACL drops	Greater than <*num*> in the past <*time*> <*Minutes*|*Hours*> by a <*object*>, where: • <*num*> values can be any five-digit number greater than or equal to zero (0). • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – NAD – SGT – DGT – DST_IP

Table A-17 RBACL Drops (continued)

Option	Description
Filter	
Device IP	Choose or enter a valid device IP address.
SGT	Choose or enter a valid source group tag.
DGT	Choose or enter a valid destination group tag.
Destination IP	Choose or enter a valid destination IP address.

NAD-Reported AAA Downtime

Define threshold criteria based on the AAA downtime that a network access device reports.

Table A-18 NAD-Reported AAA Downtime

Option	Description
AAA down	Greater than <*num*> in the past <*time*> <*Minutes*|*Hours*> by a <*object*>, where: • <*num*> values can be any five-digit number greater than or equal to zero (0). • <*time*> values can be 1 to 1440 minutes, or 1to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – Device IP – Device Group
Filter	
ISE Instance	Choose a valid ISE instance.
Device IP	Choose or enter a valid device IP address.
Device Group	Choose a valid device group name.

Schedules

Click **Operations > Alarms > Schedules** to establish schedules for alarm rules.

Table A-19 Schedules

Option	Description
Filter	Enter a text string on which to filter for a schedule.
Go	Click to filter on the text string.
Clear Filter	Click to clear the filter field.
Name	The name of the schedule. Click the name link to view and/or edit schedule details.
Description	Description of the schedule.

Table A-19 Schedules (continued)

Option	Description
Create	Click to create a new schedule. Specify the following: • Name • Description • Schedule—Click a square to select/deselect that hour. • Select All—Click to select all hours. • Clear All—Click to clear all selected hours. • Undo All—Click to clear all fields on this page. • Submit—Click to create the schedule. • Cancel—Click to cancel to exit without saving the schedule.
Edit	Select a schedule and click Edit to make changes to the schedule. Edit options are the same as the Create options.
Delete	Select a schedule and click Delete to delete the schedule. Confirm you choice by clicking Yes in the Confirm Deletion dialog, or No to exit without deleting the schedule.

Reports

This section covers the following user interface elements:

- Catalog, page A-15
- Favorites, page A-23
- Report Context Menus, page A-23
- Data Formatting, page A-26
- Filters, page A-38

Catalog

Select **Operations > Reports > Catalog.** Preconfigured system reports are grouped in categories, as shown in Report Type by Category, page A-15.

Report Type by Category

Table A-20 Report Type by Category

Report Name	Description	Logging Category
AAA Protocol		
AAA_Diagnostics	Provides AAA diagnostic details based on severity for a selected time period.	Policy diagnostics, Identity Stores Diagnostics, Authentication Flow Diagnostics, RADIUS Diagnostics

Table A-20 Report Type by Category (continued)

Report Name	Description	Logging Category
Authentication_Trend	Provides RADIUS authentication summary information for a selected time period; along with a graphical representation.	Passed authentications, Failed attempts
RADIUS_Accounting	Provides user accounting information based on RADIUS for a selected time period.	RADIUS accounting
RADIUS_Authentication	Provides RADIUS authentication details for a selected time period.	Passed authentications, Failed attempts
Allowed Protocol		
Allowed_Protocol_Authentication_Summary	Provides RADIUS authentication summary information for a particular allowed protocol for a selected time period; along with a graphical representation.	Passed authentications, Failed attempts
Top_N_Authentications_By_Allowed_Protocol	Provides the top N passed, failed, and total authentication count for RADIUS authentications with respect to the allowed protocol for a selected time period.	Passed authentications, Failed attempts
Server Instance		
OCSP Monitoring	Provides a summary of all the OCSP certificate validation operations performed by Cisco ISE.	—
Server_Administrator_Entitlement	Provides a list of administrators and their assigned entitlement roles.	Resources and privileges, configuration changes, logins
Server_Administrator_Logins	Provides access-related events for administrators that includes login, logout, events, and information about excessive failed login attempts over standalone, and other distributed nodes when the account is locked or disabled in Cisco ISE.	Administrative and operational audit
Server_Authentication_Summary	Provides RADIUS authentication summary information for a particular ISE instance for a selected time period, along with a graphical representation. This report could take several minutes to run depending on the number of records in the database. **Note** When you reload this report, if rate of incoming syslog messages is around 150 messages per second or more, the total number of passed and failed authentications that appear above the graph and the passed and failed authentication count that is displayed in the table do not match.	Passed authentications, Failed attempts
Server_Configuration_Audit	Provides all the configuration changes done in ISE by the administrator for a selected time period.	Administrative and operational audit
Server_Health_Summary	Provides the CPU, memory utilization, RADIUS and throughput (in tabular and graphical formats) and also process status, process downtime, and disk space utilization for a particular ISE instance in a selected time period.	System statistics

Table A-20 Report Type by Category (continued)

Report Name	Description	Logging Category
Server_Operations_Audit	Provides all the operational changes done in ISE by the administrator for a selected time period.	Administrative and operational audit
Server_System_Diagnostics	Provides system diagnostic details based on severity for a selected time period.	Internal Operations Diagnostics, distributed management, administrator authentication and authorization
Top_N_Authentications_By_Server	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to a particular ISE instance for a selected time period.	Passed authentications, Failed attempts
User_Change_Password_Audit	Provides the username of the internal user, identity store name, name of the ISE instance, and time when the user password was changed. Helps to keep track of all changes made to internal user passwords across all ISE interfaces.	Administrative and operational audit
Endpoint		
Endpoint_MAC_Authentication_ Summary	Provides the RADIUS authentication summary information for a particular MAC or MAB for a selected time period, along with a graphical representation.	Passed authentications, Failed attempts
Endpoint_Profiler_Summary	Provides the endpoint profiler summary information for a particular MAC address for a selected time period.	Profiler
Endpoint_Time_To_Profile	Provides information on time taken to an endpoint that has an Unknown profile by using a particular MAC address for a selected time period.	Profiler
Top_N_Authentications_By_ Endpoint_Calling _Station_ID	Provides the top N passed, failed, and total authentication count with respect to endpoint calling station IDs.	Passed authentications, Failed attempts
Top_N_Authentications_By_ Machine	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to machine information for a selected time period.	Passed authentications, Failed attempts
Failure Reason		
Authentication_Failure_Code_ Lookup	Provides the description and the appropriate resolution steps for a particular failure reason.	—
Failure_Reason_Authentication_ Summary	Provides the RADIUS authentication summary information for a particular failure reason, along with a graphical representation for a selected time period.	Failed attempts
Top_N_Authentications_By_ Failure_Reason	Provides the top N failed authentication count for RADIUS protocols with respect to Failure Reason for a selected time period.	Failed attempts
Network Device		
AAA_Down_Summary	Provides the number of AAA unreachable events that a NAD logs within a selected time period.	Passed authentications, Failed attempts

Table A-20 Report Type by Category (continued)

Report Name	Description	Logging Category
Network_Device_Authentication_ Summary	Provides the RADIUS authentication summary information for a particular network device for a selected time period, along with a graphical representation.	Passed authentications, Failed attempts
Network_Device_Log_Messages	Provides you the log information of a particular network device, for a specified time period.	Passed authentications, Failed attempts
Session_Status_Summary	Provides the port sessions and status of a particular network device obtained by SNMP.	—
Top_N_AAA_Down_By_Network_ Device	Provides the number of AAA down events encountered by each of the network devices.	Passed authentications, Failed attempts
Top_N_Authentications_By_ Network_Device	Provides the top N passed, failed, and total authentication count for RADIUS with respect to network device for a selected time period.	Passed authentications, Failed attempts
User		
Client_Provisioning	Provides a summary of successful and unsuccessful client provisioning evaluation and download events, displayed according to the associated User ID.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics
Guest_Accounting	Provides session (login and log out) information for selected guests over a specified time period.	Passed authentications, RADIUS accounting
Guest_Activity	Provides guest information for a selected time period.	Passed authentications
Guest_Sponsor_Summary	Provides sponsor information along with a graphical representation, for a selected time period.	Passed authentications
Top_N_Authentications_By_User	Provides top N passed, failed, and total authentication count for RADIUS with respect to users for a selected time period.	Passed authentications, Failed attempts
Unique_Users	Provides the count for the number of unique users.	Passed authentications, Failed attempts
User_Authentication_Summary	Provides RADIUS authentication summary information for a particular user for a selected time period; along with the graphical representation.	Passed authentications, Failed attempts
Security Group Access		
PAC Provisioning	Provides a summary of SGA PAC generated.	—
Policy CoA	Provides the summary of the policy change request through policy CoA.	—
RBACL_Drop_Summary	Provides a summary of RBAC drop events.	—
SGT_Assignment_Summary	Provides a summary of SGT assignments for a selected time period.	Passed authentications
Top_N_RBACL_Drops_By_ Destination	Provides the top N RBACL drop event count with respect to destination for a selected time period.	—
Top_N_RBACL_Drops_By_User	Provides the top N RBACL drop event count with respect to the user for a selected time period.	—

Table A-20 Report Type by Category (continued)

Report Name	Description	Logging Category
Top_N_SGT_Assignments	Provides the top N SGT assignment count for a selected time period.	Passed authentications
Session Directory		
RADIUS_Active_Sessions	Provides information on RADIUS authenticated, authorized, and started sessions. Dynamically control active RADIUS sessions. Send a reauthenticate or disconnect request to a NAD to perform the following CoA actions: • Quarantine • Session reauthentication • Session reauthentication with last • Session reauthentication with rerun • Session termination • Session termination with port bounce • Session termination with port shut down The RADIUS_Active_Sessions report will display WLC Roam status as N (N stands for No) for any wired active session.	Passed authentications, RADIUS accounting
RADIUS_Session_History	Provides a summary of RADIUS session history, such as total authenticated, active, and terminated sessions and total and average session duration and throughput for a selected time period.	Passed authentications, RADIUS accounting
RADIUS_Terminated_Sessions	Provides all the RADIUS terminated session information for a selected time period.	Passed authentications, RADIUS accounting
Posture		
Posture_Detail_Assessment	Provides the posture authentication summary information for a particular user for a selected time period.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics
Posture_Trend	Provides the count of passed or failed, as well as status information for a particular policy for a selected time period; along with the graphical representation.	Posture and Client Provisioning Audit, Posture and Client Provisioning Diagnostics
Endpoint Protection Service		
Endpoint_Operations_History	Provides EPS action history information comprising these values: Timestamp, Endpoint MAC Address, Endpoint IP Address, Operation Type, Operation Status, Operation ID, Audit Session ID, Admin Username, AdminIP Address.	—

Report Type Page

Select a category name from the Reports navigation pane. The Reports Type page appears.

Table A-21 Report Type Page

Option	Description
Report Name	A list of available report names for the category you selected.
Type	The type of report.
Modified At	The time the report was last modified by an administrator, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit representation of the year.
Filter	Enter a text string to search for a report in the text field and click **Go**. Click **Clear Filter** to list the Catalog reports.

Report Name Page

Not all options listed in the following table are used in all reports.

Table A-22 Report Name Page

Option	Description
User	Enter a username or click **Select** to enter a valid username on which to configure your threshold.
MAC Address	Enter a MAC address or click **Select** to enter a valid MAC address on which to run your report.
Identity Group	Enter an identity group name or click **Select** to enter a valid identity group name on which to run your report.
Device Name	Enter a device name or click **Select** to enter a valid device name on which to run your report.
Device IP	Enter a device IP address or click **Select** to enter a valid device IP address on which to run your report.
Device Group	Enter a device group name or click **Select** to enter a valid device group name on which to run your report.

Table A-22 Report Name Page (continued)

Option	Description
Allowed Protocol	Enter an allowed protocol name or click **Select** to enter a valid allowed protocol name on which to run your report
Identity Store	Enter an identity store name or click **Select** to enter a valid identity store name on which to run your report.
ISE Instance	Enter an ISE instance name or click **Select** to enter a valid ISE instance name on which to run your report.
Failure Reason	Enter a failure reason name or click **Select** to enter a valid failure reason name on which to run your report.
Protocol	Use the drop down list box to select which protocol on which you want to run your report. RADIUS is the only option at this time.
Authentication Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: • Pass Or Fail • Pass • Fail
Radius Audit Session ID	Enter the RADIUS audit session identification name on which you want to run a report.
ISE Session ID	Enter the ISE session identification name on which you want to run a report.
Severity	Use the drop down list box to select the severity level on which you want to run a report. This setting captures the indicated severity level and those that are higher within the threshold. Valid options are: • Fatal • Error • Warning • Info • Debug
End Point IP Address	Enter the end point IP address on which you want to run a report.
Command Accounting Only	Check the check box to enable your report to run for command accounting.

Table A-22 Report Name Page (continued)

Option	Description
Top	Use the drop down list box to select the number of top (most frequent) authentications by allowed protocol on which you want to run your report. Valid options are: • 10 • 50 • 100 • 500 • 1000 • All
By	Use the drop down list box to select the type of authentications on which you want to run your report. Valid options are: • Passed Authentications • Failed Authentications • Total Authentications
Administrator Name	Enter the administrator username, or click Select to select the administrator username, for which you want to run your report.
Object Type	Enter a valid object type on which you want to run your report.
Object Name	Enter the name, or click Select to select the object name, of the object on which you want to run your report.
Authorization Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: • Pass Or Fail • Pass • Fail
Time Range	Use the drop down list box to select the time range on which you want to run your report. Valid options are: • Last Hour (for the ISE Health Summary report only) • Today • Yesterday • Last 7 Days • Last 30 Days • Custom—You must configure a Start Date and End Date, or a Day. **Note** Some options are not valid for some Time Range entries of the various reports.
Start Date	Enter a date, or click the date selector icon to select a start date for running your report.
End Date	Enter a date, or click the date selector icon to select an end date for running your report.

Table A-22 Report Name Page (continued)

Option	Description
Day	Enter a date, or click the date selector icon to select an end date for running your report.
Clear	Click to delete the contents of an associate text box.
Run	Click to run the report for which you have made selections.

Favorites

Select **Operations > Reports > Favorites** to display a list of favorite reports. Favorites allows you to bookmark frequently used reports by saving them as favorite reports.

The following preconfigured catalog system reports are available in **Operations > Reports > Favorites** by default:

- Authentications - RADIUS - Today—A report that is preconfigured from AAA Protocol > RADIUS_Authentication to run for the current system date.
- Authentications - RADIUS - Yesterday—A report that is preconfigured from AAA Protocol > RADIUS_Authentication to run for the previous day from the current system date.
- ISE-Server Configuration Audit - Today—A report that is preconfigured from Server Instance > Server_Configuration_Audit to run for the current system date.
- ISE-System Diagnostics -Today—A report that is preconfigured from Server Instance > Server_System_Diagnostics to run for the current system date.

For a list of all available reports, see Report Type by Category, page A-15.

Favorites Page

Table A-23 Favorites Page

Option	Description
Favorite Name	The name of the favorites report. Click to open a summary of an associated report.
Report Name	The report name associated with a Catalog (Report) type.
Report Type	The general category name associated with the report.

Report Context Menus

Use context menus as shortcuts to performing data formatting and organizing tasks from the Interactive Viewer. To bring up a context menu, right click an element in a report. The context menu options that are displayed are unique to the element selected.

For more information, see Organizing and Formatting Report Data, page 24-12.

Related Topics

- Data Formatting, page A-26
- Filters, page A-38

Table A-24 Report Context Menus

Option	Description
Aggregation	Opens a dialog box that supports creating an aggregate row for this column.
Alignment	Opens a submenu that contains: • Align Left. Aligns the column data to the left. • Align Center. Centers the column data. • Align Right. Aligns the column data to the right.
Calculation	Opens a submenu that supports creating a calculated column based on this column.
Chart	Opens a submenu that supports inserting a chart.
Column	Opens a submenu that contains: • Delete Column. Deletes the selected column. • Reorder Columns. Opens a dialog box that supports changing the order of columns in the report design. • Column Width. Opens the Column Properties dialog box, which supports setting the column width. • Do Not Repeat Values. Suppresses consecutive duplicate data values in a column. If the column is already set to Do Not Repeat Values, this menu item changes to Repeat Values.
Data Fields	Opens a dialog box that displays the report columns. Supports adding or removing data fields.
Filter	Opens a submenu that contains: • Filter. Opens a dialog box that supports creating filters based on this column. • Top or Bottom N. Opens a dialog box that supports displaying the highest or lowest *n* values or the highest or lowest *n* percent in the column.
Format Data	Opens a dialog box that supports formatting the data type. For example, if the column contains numeric data, the Number column format dialog box opens and you can format the data as currency, percentages, and so on.

Table A-24 Report Context Menus (continued)

Option	Description
Group	Opens a submenu that contains: • Add Group. Creates a group based on this column. When you select a grouped column, this menu item changes to Delete Group. • Add Section. Creates a section based on this column. When you select a section column, this menu item changes to Delete Section. • Hide Detail. Hides the group's or section's detail rows. If the detail rows are hidden, this menu item changes to Show Detail. This option is available when you select a grouped column or a section column. • Page Break. Sets a page break before or after a group or section. This option is available when you select a grouped column or a section column.
Sort	Opens a submenu that contains: • Sort Ascending. Sorts the column rows in ascending order. • Sort Descending. Sorts the column rows in descending order. • Advanced Sort. Opens the Advanced Sort dialog box, which supports performing a sort based on additional columns.
Style	Opens a submenu that contains: • Font. Opens the Font dialog box, which supports modifying the font properties of column data. • Conditional Formatting. Opens a dialog box that supports setting conditional formatting rules for data in this column.

Data Formatting

This section describes data formatting for you to format data presented in the reports by using the Interactive Viewer.

Data Types and Formats

Table A-25 Data Types and Formats

Data type	Option	Description
Date and Time	Unformatted	The data retains the default format set by the template or theme.
	General Date	June 5, 2006 12:00:00 AM GMT +00:00
	Long Date	June 5, 2006
	Medium Date	Jun 5, 2006
	Short Date	6/5/06
	Long Time	12:00:00 AM GMT +00:00
	Medium Time	12:00:00 AM
	Short Time	12:00
	Custom	The format depends on a format code you type. For example, typing yyyy/mm results in 2006/10. You learn more about custom formatting later in this chapter.
Number	Unformatted	The number retains the default format set by the template or theme.
	General Number	6066.88 or 6067, depending on the decimal and thousands separator settings
	Currency	$6,067.45 or ¥6067, depending on the locale and optional settings
	Fixed	6067 or 6,067 or 6067.45, depending on optional settings
	Percent	45% or 45.8%, depending on optional settings
	Scientific	2E04 or 2.67E04, where the number after the E represents the exponent of 10, depending on optional settings. For example, 2.67E04 means 2.67 multiplied by 10 raised to the fourth power.
	Custom	The format depends on a format code you type. For example, typing #,### results in a format with a comma as a thousands separator and no decimal points. You learn more about custom formats later in this chapter.
String	Unformatted	The string retains the default format set by the template or theme.
	Uppercase	The string displays in all uppercase, for example GREAT NEWS.
	Lowercase	The string displays in all lowercase, for example great news.
	Custom	The format depends on the format code you type. Use custom formatting for postal codes, telephone numbers, and other data that does not match standard formats.

Custom Number Format Patterns

Table A-26 Custom Number Format Patterns

Format pattern	Data in the data set	Result of formatting
0000.00	12.5 124.5 1240.553	0012.50 0124.50 1240.55
#.000	100 100.25 100.2567	100.000 100.250 100.257
$#,###	2000.00 20000.00	$2,000 $20,000
ID #	15	ID 15

Symbols for Defining Custom String Formats

Symbol	Description
@	Character placeholder. Each @ character displays a character in the string. If the string has fewer characters than the number of @ symbols that appear in the format pattern, spaces appear. Placeholders are filled from right to left, unless you specify an exclamation point (!) at the beginning of the format pattern.
&	Same as @, except that if the string has fewer characters, spaces do not appear.
!	Specifies that placeholders are to be filled from left to right.
>	Converts string characters to uppercase.
<	Converts string characters to lowercase.

Results of Custom String Format Patterns

Table A-27 Results of Custom String Format Patterns

Format pattern	Data in the data source	Results of formatting
(@@@) @@@-@@@@	6175551007 5551007	(617) 555-1007 ( ) 555-1007
(&&&) &&&-&&&&	6175551007 5551007	(617) 555-1007 () 555-1007
!(@@@) @@@-@@@@	6175551007 5551007	(617) 555-1007 (555) 100-7
!(&&&) &&&-&&&&	6175551007 5551007	(617) 555-1007 (555) 100-7
!(@@@) @@@-@@@@ + ext 9	5551007	(555) 100-7 + ext 9
!(&&&) &&&-&&&& + ext 9	5551007	(555) 100-7 + ext 9
>&&&-&&&&&-&&	D1234567xy	D12-34567-XY
<&&&-&&&&&-&&	D1234567xy	d12-34567-xy

Results of Custom Date Formats

Table A-28 Results of Custom Date Formats

Format	Result of formatting
MM-dd-yy	04-15-06
E, M/d/yyyy	Fri, 4/15/2006
MMM d	Apr 15
MMMM	April
yyyy	2006
W	3 (the week in the month)
w	14 (the week in the year)
D	105 (the day in the year)

Supported Calculation Functions

Table A-29 Supported Calculation Functions

Function	Description	Example of use
ABS(num)	Displays an absolute value for the data in a column.	`ABS([TemperatureCelsius])`
ADD_DAY (date, daysToAdd)	Adds a specified number of days to a date value and displays the result as a date value.	`ADD_DAY([ClosingDate], 30)`
ADD_HOUR (date, hoursToAdd)	Adds a specified number of hours to a time value and displays the result as a time value.	`ADD_HOUR([OpenHour], 8)`
ADD_MINUTE (date, minutesToAdd)	Adds a specified number of minutes to a time value and displays the result as a time value.	`ADD_MINUTE([StartTime], 60)`
ADD_MONTH (date, monthsToAdd)	Adds a specified number of months to a date value and displays the result as a date value.	`ADD_MONTH([InitialRelease], 2)`
ADD_QUARTER (date, quartersToAdd)	Adds a specified number of quarters to a date value.	`ADD_QUARTER([ForecastClosing], 2)`
ADD_SECOND (date, secondsToAdd)	Adds a specified number of seconds to a time value.	`ADD_SECOND([StartTime], 30)`
ADD_WEEK (date, weeksToAdd)	Adds a specified number of weeks to a date value and displays the result as a date value.	`ADD_WEEK([askByDate], 4)`
ADD_YEAR (date, yearsToAdd)	Adds a specified number of years to a date value.	`ADD_YEAR([HireDate], 5)`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
AND	Combines two conditions and returns records that match both conditions. For example, you can request records from customers who spend more than $50,000 a year and also have a credit rank of A.	This function is used to connect clauses in an expression and does not take arguments.
AVERAGE(expr)	Displays an average value for the column.	`AVERAGE([CostPerUnit])`
AVERAGE (expr, groupLevel)	Displays the average value at the specified group level.	`AVERAGE([TotalCost], 2)`
BETWEEN(value, upperBound, lowerBound)	For a specified column, displays true if a value is between two specified values and false otherwise. String values and date or time values must be enclose in quotation marks. For dates and times, use the short date and short time formats.	`BETWEEN([PostalCode], 11209, 12701)` `BETWEEN([ReceiptDate], "10/01/06", "12/31/06")`
CEILING (num, significance)	Rounds a number up, away from 0, to the nearest specified multiple of significance. For data that has been converted from a double or float to an integer, displays the smallest integer that is greater than or equal to the float or double.	`CEILING([PortfolioAverage], 1)`
COUNT( )	Counts the rows in a table.	`COUNT( )`
COUNT(groupLevel)	Counts the rows at the specified group level.	`COUNT(2)`
COUNTDISTINCT(expr)	Counts the rows that contain distinct values in a table.	`COUNTDISTINCT([CustomerID])` `COUNTDISTINCT([Volume]*2)`
COUNTDISTINCT (expr, groupLevel)	Counts the rows that contain distinct values at the specified group level.	`COUNTDISTINCT([CustomerID], 3)`
DAY(date)	Displays the number of a day in the month, from 1 to 31, for a date-and-time value.	`DAY([forecastShipping])`
DIFF_DAY(date1, date2)	Displays the difference between two date values, in the number of days.	`DIFF_DAY([checkoutDate], [returnDate])`
DIFF_HOUR(date1, date2)	Displays the difference between two time values, in the number of hours.	`DIFF_HOUR([StartTime],[Finish Time])`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
DIFF_MINUTE (date1, date2)	Displays the difference between two time values, in the number of minutes.	`DIFF_MINUTE([StartTime], [FinishTime])`
DIFF_MONTH (date1, date2)	Displays the difference between two date values, in the number of months.	`DIFF_MONTH([askByDate], [shipByDate])`
DIFF_QUARTER (date1, date2)	Displays the difference between two date values, in the number of quarters.	`DIFF_QUARTER([PlanClosing], [ActualClosing])`
DIFF_SECOND (date1, date2)	Displays the difference between two time values, in the number of seconds.	`DIFF_SECOND([StartTime], [FinishTime])`
DIFF_WEEK(date1, date2)	Displays the difference between two weeks as a number.	`DIFF_WEEK([askByDate], [shipByDate])`
DIFF_YEAR(date1, date2)	Displays the difference between two years as a number.	`DIFF_YEAR([HireDate], [TerminationDate])`
false	The Boolean false. This function is used in expressions to indicate that an argument is false.	In the following example, false indicates that the second argument, ascending, is false and therefore the values should be returned in descending order. `RANK([Score], false)`
FIND(strToFind, str)	Displays the index of the first occurrence of specified text. The index is zero-based. The search is case sensitive and the search string cannot include wildcards. The value in the strToFind argument must be enclosed in quotation marks.	`FIND("HQ", [OfficeName])`
FIND(strToFind, str, startPosition)	Similar to FIND(strToFind, str) but supports providing a start position for the search. The index is zero-based.	`FIND("HQ", [OfficeName], 3)`
FIRST(expr)	Places the first value that appears in a specified column into the calculated column. This function supports viewing a row-by-row comparison against a specific value.	`FIRST([customerID])`
FIRST(expr, groupLevel)	Displays the first value that appears in the specified column at the specified group level.	`FIRST([customerID], 3)`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
IF(condition, doIfTrue, doIfFalse)	Displays the result of an If...Then...Else statement.	`IF([purchaseVolume] >5 , 7 , 0)` where • [purchaseVolume] is the column name and >5 is the test condition. • 7 is the value to place in the new column if the condition is true. • 0 is the value to place in the new column if the condition is false.

IN(value, check)	Displays true if a data row contains a value specified by the check argument and false otherwise. String values and date or time values must be enclosed in quotation marks. For dates and times, use the short date and short time formats for your locale.	`IN([custID], 101)`
		`IN([city], "New Haven")`
		`IN([FinishTime], "16:09")`

IN(value, check1, ..., checkN)	Displays true if a data row contains any value specified by the check argument list and false otherwise. String values and date or time values must be enclosed in quotation marks. For dates and times, use the short date and short time formats for your locale.	`IN([city], "New Haven", "Baltimore", "Cooperstown")` `IN([ShipDate], "05/01/06", "05/10/06", "05/15/06")`
ISBOTTOMN(expr, n)	Displays true if the value is within the lowest *n* values for the expression, and false otherwise.	`ISBOTTOMN([OrderTotals], 50)`
ISBOTTOMN (expr, n, groupLevel)	Displays true if the value is within the lowest *n* values for the expression at the specified group level, and false otherwise.	`ISBOTTOMN([OrderTotals], 50, 2)`
ISBOTTOMNPERCENT (expr, percent)	Displays the lowest *n* percentage.	`ISBOTTOMNPERCENT([Sales Total], 5)`
ISBOTTOMNPERCENT (expr, percent, groupLevel)	Displays the lowest *n* percentage for the expression at the specified group level.	`ISBOTTOMNPERCENT([Sales Total], 5, 3)`
ISNULL(value)	Displays true if a row does not display a value. Displays false if a row displays a value.	`ISNULL([DepartmentName])`
ISTOPN(expr, n)	Displays true if the value is within the highest *n* values for the expression, and false otherwise.	`ISTOPN([OrderTotals], 10)`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
ISTOPN(expr, n, groupLevel)	Displays true if the value is within the highest *n* values for the expression at the specified group level, and false otherwise.	`ISTOPN([OrderTotals], 10, 3)`
ISTOPNPERCENT(expr, percent)	Displays true if the value is within the highest *n* percentage, and false otherwise.	`ISTOPNPERCENT([SalesTotals], 5)`
ISTOPNPERCENT(expr, percent, groupLevel)	Displays true if the value is within the highest *n* percentage values for the expression at the specified group level, and false otherwise.	`ISTOPNPERCENT([SalesTotals], 5, 3)`
LAST(expr)	Displays the last value in a specified column.	`LAST([FinishTime])`
LAST(expr, groupLevel)	Displays the last value for the expression at the specified group level.	`LAST([FinishTime], 3)`
LEFT(str)	Displays the character at the left of the specified string.	`LEFT([city])`
LEFT(str, n)	Displays the specified number of characters in a column's string, counting from the left.	`LEFT([city], 3)`
LEN(str)	Displays the length of a string, including spaces and punctuation marks.	`LEN([Description])`
LIKE(str)	Displays true if the values match, and false otherwise. Use SQL syntax to specify the string pattern. The following rules apply: • Literal pattern characters must match exactly. LIKE is case-sensitive. • A percent character (%) matches zero or more characters. • An underscore character (_) matches any single character. • Escape a literal percent, underscore, or backslash character (\) with a backslash character.	`LIKE([customerName], "D%")` `LIKE([quantityOrdered], "2_")`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
LOWER(str)	Displays the string in a specified column in lowercase.	`LOWER([cityName])`
MAX(expr)	Displays the highest value in the specified column.	`MAX([OrderTotal])`
MAX(expr, groupLevel)	Displays the highest value for the expression at the specified group level.	`MAX([OrderTotal], 2)`
MEDIAN(expr)	Displays the median value in a specified column.	`MEDIAN([HomePrices])`
MEDIAN (expr, groupLevel)	Displays the median value for the expression at the specified group level.	`MEDIAN([HomePrices], 2)`
MIN(expr)	Displays the lowest value in the specified column.	`MIN([OrderTotal])`
MIN(expr, groupLevel)	Displays the lowest value for the expression at the specified group level.	`MIN([OrderTotal], 1)`
MOD(num, div)	Displays the remainder after a number is divided by a divisor. The result has the same sign as the divisor.	`MOD([Salary], 12)`
MONTH(date)	Displays the name of the month for a specified date-and-time value.	`MONTH([ForecastShipDate])`
MONTH(date, option)	Displays the month of a specified date-and-time value, in one of three optional formats: • 1 - Displays the month number of 1 through 12. • 2 - Displays the complete month name in the user's locale. • 3 - Displays the abbreviated month name in the user's locale.	`MONTH([Semester], 2)`
MOVINGAVERAGE (expr, window)	Displays an average value over a specified window, such as an average price or volume over a number of days.	`MOVINGAVERAGE([Price], [Days])`
NOTNULL(value)	For a specified column, displays true if a data value is not empty. Displays false if a data value is empty.	`NOTNULL([DepartmentID])`
NOW( )	Displays the current time stamp.	`NOW([PastDueDate])`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
OR	The logical OR operator.	This function is used to connect clauses in an expression and does not take arguments.
PERCENTILE(expr, pct)	Displays a percentile value, a value on a scale of 100 that indicates the percent of a distribution that is equal to or below the specified value. Valid pct argument ranges are 0 to 1. 0 returns the minimum value of the series. 1 returns the maximum value of the series.	`PERCENTILE([Rank], 1)`
PERCENTILE (expr, pct, groupLevel)	Displays a percentile value for the expression at the specified group level. Valid pct argument ranges are 0 to 1. 0 returns the minimum value of the series. 1 returns the maximum value of the series.	`PERCENTILE([Income], 60, 1)`
PERCENTRANK(expr)	Displays the percentage rank of a value.	`PERCENTRANK([TestScores])`
PERCENTRANK(expr, groupLevel)	Displays the percentage rank of a value at the specified group level.	`PERCENTRANK([TestScores], 2)`
PERCENTSUM(expr)	Displays a value as a percentage of a total.	`PERCENTSUM([OrderTotals])`
PERCENTSUM(expr, groupLevel)	Displays a value as a percentage of a total at the specified group level.	`PERCENTSUM([OrderTotals], 3)`
QUARTER(date)	Displays the quarter number, from 1 through 4, of a specified date-and-time value.	`QUARTER([ForecastCloseDate])`
QUARTILE(expr, quart)	Displays the quartile value, where the quart argument is an integer between 0 and 4.	`QUARTILE([OrderTotal], 3)`
QUARTILE (expr, quart, groupLevel)	Displays the quartile value for the expression at the specified group level, where the quart argument is an integer between 0 and 4.	`QUARTER([OrderTotal], 2, 3)`
RANK(expr)	Displays the rank of a number, string, or date-and-time value, starting at 1. Duplicate values receive identical rank but the duplication does not affect the ranking of subsequent values.	`RANK([AverageStartTime])`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
RANK(expr, ascending, groupLevel)	Displays the rank of a number, string, or date-and-time value in either ascending or descending order, at the specified group level. To display values in ascending order, use true as the second argument. To display values in descending order, use false as the second argument.	`RANK([Score], false, 3)` `RANK([Score], true, 2)`
RIGHT(str)	Displays the character at the right of a string.	`RIGHT([name])`
RIGHT(str, n)	Displays the specified number of characters in a string, counting from the right.	`RIGHT([name], 3)`
ROUND(num)	Rounds a number.	`ROUND([SalesTarget])`
ROUND(num, dec)	Rounds a number to the specified number of digits. The default value for dec is 0.	`ROUND([StockValue], 2)`
ROUNDDOWN(num)	Rounds a number down.	`ROUNDDOWN([StockPrice])`
ROUNDDOWN(num, dec)	Rounds a number down, away from 0, to the specified number of digits. The default value for dec is 0.	`ROUNDDOWN([StockPrice], 2)`
ROUNDUP(num)	Rounds a number up.	`ROUNDUP([TotalValue])`
ROUNDUP(num, dec)	Rounds a number up, away from 0, to the specified number of digits. The default value for dec is 0.	`ROUNDUP([TotalValue], 2)`
RUNNINGSUM(expr)	Displays a running total, adding the values in successive data rows.	`RUNNINGSUM([StockValue])`
SEARCH(pattern, str)	Case-insensitive search function that can use wildcard characters. An asterisk (*) matches any sequence of characters, including spaces. A question mark (?) matches any single character.	The following search yields New York, New Haven, and so on from the City column: `SEARCH([CustomerData:city], "new*")`
SEARCH (pattern, str, startPosition)	Searches for a specified pattern in a string, starting at a specified position in the string. A case-insensitive search function that can use wildcard characters.	`SEARCH([Location], "new", 1)`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
SQRT(num)	Displays the square root of a value.	`SQRT([PrincipalValue])`
STDEV(expr)	Displays the standard deviation.	`STDEV([PurchaseFrequency])`
SUM(expr)	Displays the sum of two specified values.	`SUM([Price]+[Tax])`
TODAY( )	Displays a time stamp value equal to midnight of the current date.	`TODAY([DueDate])`
TRIM(str)	Displays a string with all leading and trailing blank characters removed. Also removes all consecutive blank characters. Leading and trailing blanks can be spaces, tabs, and so on.	`TRIM([customerName])`
TRIMLEFT(str)	Displays a string with all leading blanks removed. Does not remove consecutive blank characters.	`TRIMLEFT([PortfolioName])`
TRIMRIGHT(str)	Displays a string with all trailing blanks removed. Does not remove consecutive blank characters.	`TRIMRIGHT([Comments])`
true	The Boolean true. This function is used in expressions to indicate that an argument is true.	In the following example, true indicates that the second argument, ascending, is true and therefore the values should be returned in ascending order. `RANK([Score], true)`
UPPER(str)	Displays a string in a specified column in all uppercase.	`UPPER([cityName])` `UPPER("new haven")`
VAR(expr)	Displays a variance for the specified expression.	`VAR([EstimatedCost])`
WEEK(date)	Displays the number of the week, from 1 through 52, for a date-and-time value.	`WEEK([LeadQualifyingDate])`

Table A-29 Supported Calculation Functions (continued)

Function	Description	Example of use
WEEKDAY(date, option)	Displays the day of the week in one of the following format options: • 1 - Returns the day number, from 1 (Sunday) through 7 (Saturday). 1 is the default option. • 2 - Returns the day number, from 1 (Monday) through 7 (Sunday). • 3 - Returns the day number, from 0 (Monday) through 6 (Sunday). • 4 - Returns the weekday name according to the user's locale. • 5 - Returns the abbreviated weekday name according to the user's locale.	`WEEKDAY([DateSold], 4)`
WEIGHTEDAVERAGE (value, weight)	Displays a weighted average of a specified value.	`WEIGHTEDAVERAGE([Score], weight)`
YEAR(date)	Displays the four-digit year value for a date-and-time value.	`YEAR([ClosingDate])`

Supported Operator Formats

Table A-30 Supported Operator Formats

Operator	Description
x + y	Addition of numeric values
x - y	Subtraction of numeric values
x * y	Multiplication of numeric values
x / y	Division of numeric values
x%	Percentage of a numeric value
x & y	Concatenation of string values
x = y	Test for equality of two values
x > y	Tests whether x is greater than y
x < y	Tests whether x is less than y
x >= y	Tests whether x is greater than or equal to y
x <= y	Tests whether x is less than or equal to y
x <> y	Tests whether x is not equal to y

Table A-30 Supported Operator Formats (continued)

Operator	Description
x AND y	Tests for values that meet both condition x and condition y
x OR y	Tests for values that meet either condition x or condition y
NOT x	Tests for values that are not x

Aggregate Function Formats

Table A-31 Aggregate Function Formats

Aggregate functions	Description
Average	Calculates the average value of a set of data values.
Count	Counts the data rows in the column.
Count Value	Counts distinct values in the column.
First	Returns the first value in the column.
Last	Returns the last value in the column.
Max	Returns the highest value in the column.
Median	Returns the median value in the column.
Min	Returns the lowest value in the column.
Mode	Returns the most frequently-occurring value in the column.
Quartile	Returns one of four equal-sized sets of data, based on the rank you select. For example, you can request the first quartile to get the top quarter of the data set or the fourth quartile to get the fourth quarter of the data set.
Standard Deviation	Returns the standard deviation, the square root of the variance.
Sum	Adds the values in the column.
Variance	Returns a value that indicates the spread around a mean or expected value.
Weighted average	Returns the weighted average of a numeric field over a set of data rows. In a weighted average, some numbers carry more importance, or weight, than others.

Filters

Conditions for Filters

Table A-32 Conditions for Filters

Condition	Description
Any Of	Returns any of the values you specify.
Between	Returns values that are between two specified values. When you select Between, a second Value field appears for the second default value.

Table A-32 Conditions for Filters (continued)

Condition	Description
Bottom N	Returns the lowest *n* values in the column.
Bottom Percent	Returns the lowest *n* percent of values in the column.
Equal to	Returns values that are equal to a specified value.
Greater Than	Returns values that are greater than a specified value.
Greater Than or Equal to	Returns values that are greater than or equal to a specified value.
Is False	In a column that evaluates to true or false, returns data rows that contain false values.
Is Not Null	Returns data rows that contain values.
Is Null	Returns data rows that do not contain values.
Is True	In a column that evaluates to true or false, returns data rows that contain true values.
Less Than	Returns values that are less than another value.
Less Than or Equal to	Returns values that are less than or equal to another value.
Like	Returns strings that match all or part of the specified string. % matches zero or more characters. _ matches one character.
Not Between	Returns values that are not between two specified values. When you select Not Between, a second Value field appears for the second default value.
Not Equal to	Returns values that are not equal to another value.
Not Like	Returns strings that do not match all or part of the specified string. % matches zero or more characters. _ matches one character.
Top N	Returns the top *n* values in the column.
Top Percent	Returns the top *n* percent of values in the column.

Filter Condition Examples

Table A-33 Filter Condition Examples

Type of filter condition	Description	Examples of instructions to data source

Comparison	Compares the value of one expression to the value of another expression using:
	• Equal to
	• Not Equal to
	• Less Than
	• Less Than or Equal to
	• Greater Than
	• Greater Than or Equal to
		`quantity = 10`
		`custName = 'Acme Inc.'`
		`custName > 'P'`
		`custState <> 'CA'`
		`orderDate > {d '2005-06-30'}`

Table A-33 Filter Condition Examples (continued)

Type of filter condition	Description	Examples of instructions to data source

Range	Tests whether the value of an expression falls or does not fall within a range of values using Between or Not Between. The test includes the endpoints of the range.	`price BETWEEN 1000 AND 2000`
		`custName BETWEEN 'E' AND 'K'`
		`orderDate BETWEEN`
		`{d '2005-01-01'} AND {d '2005-06-30'}`

Membership	Tests whether the value of an expression matches one value in a set of values using Any Of.	`officeCode IN (101,103,104)`
		`itemType IN ('sofa', 'loveseat',`
		`'endtable', 'clubchair')`
		`orderDate IN`
		`({d '2005-10-10'}, {d '2005-10-17'})`

Pattern-matching	Tests whether the value of a string field matches or does not match a specified pattern using Like or Not Like. % matches zero or more characters.
	_ matches one character.
		`custName LIKE 'Smith%'`
		`custName LIKE 'Smiths_n'`
		`custState NOT LIKE 'CA%'`

Null value	Tests whether a field has or does not have a null, or missing, value using Is Null or Is Not Null.	`manager IS NULL`
		`shipDate IS NULL`
		`shipDate IS NOT NULL`

Troubleshoot

To bring up Cisco ISE troubleshooting tools, go to **Operations > Troubleshoot > Diagnostic Tools**. Use the following tools to solve problems that may appear on your network:

- General Tools, page A-40
- Security Group Access Tools, page A-47

General Tools

To access the following General Tools for troubleshooting, go to **Operations > Troubleshoot > Diagnostic Tools** and expand **General Tools** in the left panel. Choose from the following tools:

- Connectivity Tests, page A-41
- RADIUS Authentication Troubleshooter, page A-41
- Execute Network Device Command, page A-43
- Evaluate Configuration Validator, page A-44
- Posture Troubleshooting, page A-45
- TCP Dump, page A-47

Connectivity Tests

Perform connectivity tests to troubleshoot failed authentications and other problems.

Table A-34 Connectivity Tests

Option	Description
Hostname or IP Address	Enter the hostname or IP address for a connection you want to test. Click **Clear** to clear the hostname or IP address .
ping	Click **ping** to view the packets sent and received, packet loss (if any) and the time it takes for the test to complete.
traceroute	Click **traceroute** to view the intermediary IP addresses (hops) between the Monitoring persona node and the tested hostname or IP address, and the time it takes for each hop to complete.
nslookup	Click **nslookup** cto view the server and IP address of your tested domain name server hostname or IP address.

RADIUS Authentication Troubleshooter

Check RADIUS authentication results and troubleshoot problems that may occur.

Table A-35 RADIUS Authentication Troubleshooter

Option	Description
Search and select a RADIUS authentication for troubleshooting	
Username	Enter the username of the user whose authentication you want to troubleshoot, or click **Select** to choose the username from a list. Click **Clear** to clear the username.
MAC Address	Enter the MAC address of the device that you want to troubleshoot, or click **Select** to choose the MAC address from a list. Click **Clear** to clear the MAC address.
Audit Session ID	Enter the audit session ID that you want to troubleshoot. Click **Clear** to clear the audit session ID.
NAS IP	Enter the NAS IP address or click **Select** to choose the NAS IP address from a list. Click **Clear** to clear the NAS IP address.
NAS Port	Enter the NAS port number or click **Select** to choose a NAS port number from a list. Click **Clear** to clear the NAS port number.
Authentication Status	Choose the status of your RADIUS authentication from the Authentication Status drop-down list box. The available options are: • Pass or Fail • Pass • Fail
Failure Reason	Enter the failure reason or click **Select** to choose a failure reason from a list. Click **Clear** to clear the failure reason.

Table A-35 RADIUS Authentication Troubleshooter (continued)

Option	Description
Time Range	Select a time range from the drop-down list. The RADIUS authentication records that are created during this time range are used: • Last hour • Last 12 hours • Today • Yesterday • Last 7 days • Last 30 days • Custom
Start Date-Time	(Only if you choose Custom Time Range) Enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
End Date-Time	(Only if you choose Custom Time Range) Enter the end date and time, or click the calendar icon to select the end date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
Fetch Number of Records	Choose the number of records that you want to fetch from the drop-down list: 10, 20, 50, 100, 200, or 500.

RADIUS Authentication Troubleshooting—Progress Details

Table A-36 RADIUS Authentication Troubleshooting Progress Details

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.

Table A-36 RADIUS Authentication Troubleshooting Progress Details (continued)

Option	Description
Use Console Server	Select this check box to use the console server.
Console IP Address	(If the Use Console Server check box is selected) Enter the console IP address.
Advanced (Use if there is an "Expect timeout error" or the device has non-standard prompt strings)	
Note The Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

RADIUS Authentication Troubleshooting—Results Summary

Table A-37 RADIUS Authentication Troubleshooting Results Summary

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

Execute Network Device Command

Execute the **show** command on a network device.

Table A-38 Execute Network Device Command

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device on which you want to run the command.
Command	Enter the **show** command.

Evaluate Configuration Validator

Evaluate the configuration of a network device and identify any configuration problems.

Table A-39 Evaluate Configuration Validator

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device whose configuration you want to evaluate.
Select the configuration items below that you want to compare against the recommended template.	
AAA	This option is selected by default.
RADIUS	This option is selected by default.
Device Discovery	This option is selected by default.
Logging	This option is selected by default.
Web Authentication	Select this check box to compare the web authentication configuration.
Profiler Configuration	Select this check box to compare the Profiler configuration.
SGA	Check this check box if you want to compare Security Group Access configuration.
802.1X	Check this check box if you want to compare the 802.1X configuration, and choose one of the following options: • Open Mode • Low Impact Mode (Open Mode + ACL) • High Security Mode (Closed Mode)

Progress Details

Table A-40 Progress Details

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.

Table A-40 Progress Details (continued)

Option	Description
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings)	
Note The Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Results Summary

Table A-41 Results Summary

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

Posture Troubleshooting

Find and resolve posture problems on the network.

Table A-42 Posture Troubleshooting

Option	Description
Search and Select a Posture event for troubleshooting	
Username	Enter the username to filter on.
MAC Address	Enter the MAC address to filter on, using format: xx-xx-xx-xx-xx-xx

Table A-42 Posture Troubleshooting (continued)

Option	Description
Posture Status	Select the authentication status to filter on: • Any • Compliant • Noncompliant • Unknown
Failure Reason	Enter the failure reason or click **Select** to choose a failure reason from a list. Click **Clear** to clear the failure reason.
Time Range	Select a time range from the drop-down list . The RADIUS authentication records that are created during this time range are used: • Last hour • Last 12 hours • Today • Yesterday • Last 7 days • Last 30 days • Custom
Start Date-Time:	(Only if you choose Custom Time Range) Enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
End Date-Time:	(Only if you choose Custom Time Range) Enter the end date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
Fetch Number of Records	Select the number of records to display: 10, 20, 50, 100, 200, 500
Search Result	
Time	Time of the event
Status	Posture status
Username	User name associated with the event
MAC Address	MAC address of the system
Failure Reason	Failure reason for the event

TCP Dump

Use the **tcpdump** utility to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear.

Table A-43 TCP Dump

Option	Description
Status:	• Stopped—the tcpdump utility is not running • Start—Click to start the tcpdump utility monitoring the network. • Stop—Click to stop the tcpdump utility
Host Name	Choose the name of the host to monitor from the drop-down list.
Network Interface	Choose the network interface to monitor from the drop-down list.
Promiscuous Mode	• On—Click to turn on promiscuous mode (default). • Off—Click to turn off promiscuous mode. Promiscuous mode is the default packet sniffing mode. It is recommended that you leave it set to On. In this mode the network interface is passing all traffic to the system's CPU.
Filter	Enter a boolean expression on which to filter. Standard tcpdump filter expressions are supported.
Format	Select a format for the tcpdump file from the drop-down list: • Human Readable • Raw Packet Data

Dump File	Displays data on the last dump file, such as the following:
	Last created on Wed Apr 27 20:42:38 UTC 2011 by admin
	`File size: 3,744 bytes`
	`Format: Raw Packet Data`
	`Host Name: Positron`
	`Network Interface: GigabitEthernet 0`
	`Promiscuous Mode: On`
	• Download—Click to download the most recent dump file.
	• Delete—Click to delete the most recent dump file.

Security Group Access Tools

To access the following General Tools for troubleshooting, go to **Operations > Troubleshoot > Diagnostic Tools** and expand **Security Group Access Tools** in the left panel. Choose from the following tools:

- Egress SGACL Policy, page A-48
- SXP-IP Mappings, page A-49
- IP User SGT, page A-51
- Device SGT, page A-53

Egress SGACL Policy

Compare Security Group Access-enabled devices using theEgress policy diagnostic too.

Progress Details

Table A-44 Progress Details for Egress SGACL Policy

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings) **Note** The Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Results Summary

Table A-45 Results Summary for Egress SGACL Policy

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

SXP-IP Mappings

Compare SXP-IP mappings between a device and its peers.

Peer SXP Devices

Table A-46 Peer SXP Devices for SXP-IP Mappings

Option	Description
Peer SXP Devices	
Peer IP Address	IP address of the peer SXP device.
VRF	The VRF instance of the peer device.
Peer SXP Mode	The SXP mode of the peer device; for example, whether it is a speaker or a listener.
Self SXP Mode	The SXP mode of the network device; for example, whether it is a speaker or a listener.
Connection State	The status of the connection.
Common Connection Parameters	
User Common Connection Parameters	Check this check box to enable common connection parameters for all the peer SXP devices. **Note** If the common connection parameters are not specified or if they do not work for some reason, the Expert Troubleshooter again prompts you for connection parameters for that particular peer device.
Username	Enter the username of the peer SXP device.
Password	Enter the password to gain access to the peer device.

Table A-46 Peer SXP Devices for SXP-IP Mappings

Option	Description
Protocol	• Choose the protocol from the Protocol drop-down list box. Valid options are: – Telnet – SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	• Enter the port number. The default port number for Telnet is 23 and SSH is 22.
Enable Password	Enter the enable password if it is different from your login password.
Same as login password	Check this check box if your enable password is the same as your login password.

Progress Details

Table A-47 Progress Details for SXP-IP Mappings

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings)	
Note The Advanced options appear only for some of the troubleshooting tools.	

Table A-47 Progress Details for SXP-IP Mappings (continued)

Option	Description
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Results Summary

Table A-48 Results Summary for SXP-IP Mappings

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

IP User SGT

Use the IP User SGT diagnostic tool to compare IP-SGT values on a device with an ISE assigned SGT.

Table A-49 IP User SGT

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device.
Filter Results	
Username	Enter the username of the user whose records you want to troubleshoot.
User IP Address	Enter the IP address of the user whose records you want to troubleshoot.
SGT	Enter the user SGT value.

Progress Details

Table A-50 Progress Details for IP User SGT

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, SSH connections must be enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings) **Note** Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Results Summary

Table A-51 Results Summary for IP User SGT

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.

Table A-51 Results Summary for IP User SGT (continued)

Option	Description
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

Device SGT

Use the Device SGT diagnostic tool to compare the device SGT with the most recently assigned value.

Table A-52 Device SGT

Option	Description
Enter Information	
Network Device IPs (comma-separated list)	Enter the network device IP addresses (whose device SGT you want to compare with an ISE-assigned device SGT) separated by commas.
Common Connection Parameters	
Use Common Connection Parameters	Select this check box to use the following common connection parameters for comparison: • Username—Enter the username of the network device. • Password—Enter the password. • Protocol—Choose the protocol from the Protocol drop-down list box. Valid options are: – Telnet – SSHv2 **Note** Telnet is the default option. If you choose SSHv2, SSH connections must be enabled on the network device. • Port—Enter the port number. The default port number for Telnet is 23 and SSH is 22.
Enable Password	Enter the enable password if it is different from your login password.
Same as login password	Select this check box if your enable password is the same as your login password.

Policy

This section covers the following user interface elements:

- Authentication, page A-54

Authentication

Allowed Protocols Service

Table A-53 Allowed Protocols Service

Option	Description
Allowed Protocols	
Process Host Lookup	Check this check box to configure Cisco ISE to process the Host Lookup field (for example, when the RADIUS Service-Type equals 10) and use the System UserName attribute from the RADIUS Calling-Station-ID attribute. Uncheck this check box if you want Cisco ISE to ignore the Host Lookup request and use the original value of the system UserName attribute for authentication. When unchecked, message processing is done according to the protocol (for example, PAP).
Authentication Protocols	
Allow PAP/ASCII	This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol. When you check the Allow PAP/ASCII check box, you can check the Detect PAP as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of PAP) request.
Allow CHAP	This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
Allow MS-CHAPv1	This option enables MS-CHAPv1.
Allow MS-CHAPv2	This option enables MS-CHAPv2.
Allow EAP-MD5	This option enables EAP-based MD5 hashed authentication. When you check the Allow EAP-MD5 check box, you can check the Detect EAP-MD5 as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of EAP-MD5) request.

Table A-53 Allowed Protocols Service (continued)

Option	Description
Allow EAP-TLS	This option enables the EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how Cisco ISE will verify the user identity as presented in the EAP identity response from the end-user client. User identity is verified against information in the certificate that the end-user client presents. This comparison occurs after an EAP-TLS tunnel is established between Cisco ISE and the end-user client. **Note** EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates. Refer to Chapter 13, "Managing Certificates" for more information on certificates.
Allow LEAP	This option enables Lightweight Extensible Authentication Protocol (LEAP) authentication.
Allow PEAP	This option enables the PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2. When you check the Allow PEAP check box, you can configure the following PEAP inner methods: • Allow EAP-MS-CHAPv2—Check this check box to use EAP-MS-CHAPv2 as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-GTC—Check this check box to use EAP-GTC as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method.

Table A-53 Allowed Protocols Service (continued)

Option	Description
Allow EAP-FAST	This option enables the EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MS-CHAPv2. When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method: • Allow EAP-MS-CHAPv2 – Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Allow EAP-GTC • Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. • Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Use PACs—Choose this option to configure Cisco ISE to provision authorization PACs[1] for EAP-FAST clients. Additional PAC options appear. • Don't use PACs—Choose this option to configure Cisco ISE to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and Cisco ISE responds with a Success-TLV without a PAC. When you choose this option, you can configure Cisco ISE to perform machine authentication.

1. PACs = Protected Access Credentials.

PAC Options

Table A-54 PAC Options

Option	Description
Use PAC	• Tunnel PAC Time to Live—The TTL[1] value restricts the lifetime of the PAC. Specify the lifetime value and units. The default is 90 days. The range is between 1 and 1825 days. • Proactive PAC Update When: <n%> of PAC TTL is Left—The Update value ensures that the client has a valid PAC. Cisco ISE initiates an update after the first successful authentication but before the expiration time that is set by the TTL. The update value is a percentage of the remaining time in the TTL. The default is 90%. • Allow Anonymous In-band PAC Provisioning—Check this check box for Cisco ISE to establish a secure anonymous TLS handshake with the client and provision it with a PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. **Note** To enable anonymous PAC provisioning, you must choose both of the inner methods, EAP-MSCHAPv2 and EAP-GTC. • Allow Authenticated In-band PAC Provisioning—Cisco ISE uses SSL server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning but requires that a server certificate and a trusted root CA be installed on Cisco ISE. When you check this option, you can configure Cisco ISE to return an Access-Accept message to the client after successful authenticated PAC provisioning. – Server Returns Access Accept After Authenticated Provisioning—Check this check box if you want Cisco ISE to return an access-accept package after authenticated PAC provisioning. • Allow Machine Authentication—Check this check box for Cisco ISE to provision an end-user client with a machine PAC and perform machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by the administrator (out-of-band). When Cisco ISE receives a valid machine PAC from the end-user client, the machine identity details are extracted from the PAC and verified in the Cisco ISE external identity source. After these details are correctly verified, no further authentication is performed. **Note** Cisco ISE only supports Active Directory as an external identity source for machine authentication. When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When Cisco ISE receives an expired machine PAC, it automatically reprovisions the end-user client with a new machine PAC (without waiting for a new machine PAC request from the end-user client).

Table A-54 PAC Options (continued)

Option	Description
	• Enable Stateless Session Resume—Check this check box for Cisco ISE to provision authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled). Uncheck this check box in the following cases: – If you do not want Cisco ISE to provision authorization PACs for EAP-FAST clients – To always perform phase two of EAP-FAST When you check this option, you can enter the authorization period of the user authorization PAC. After this period, the PAC expires. When Cisco ISE receives an expired authorization PAC, it performs phase two EAP-FAST authentication. • Preferred EAP Protocol—Check this check box to choose your preferred EAP protocols from any of the following options: EAP-FAST, PEAP, LEAP, EAP-TLS, and EAP-MD5. By default, LEAP is the preferred protocol to use if you do not enable this field.

1. TTL = Time To Live

Administration

This section covers the following:

- System > Settings > Monitoring, page A-58
- System > Maintenance > Data Management > Monitoring Node, page A-61

System > Settings > Monitoring

To access system monitoring tools go to **Administration > System > Settings**, then expand **Monitoring** in the left panel. This section covers the user interface elements for the following monitoring tools:

- Alarm Syslog Targets, page A-59
- Email Settings, page A-59
- Failure Reasons Editor, page A-59
- System Alarm Settings, page A-60

Alarm Syslog Targets

Define the destination where alarm syslog messages are sent.

Table A-55 Alarm Syslog Targets

Option	Description
Identification	
Name	Name of the alarm syslog target. The name can be 255 characters in length.
Description	(Optional) A brief description of the alarm that you want to create. The description can be up to 255 characters in length.
Configuration	
IP Address	IP address of the machine that receives the syslog message. This machine must have the syslog server running on it. It is recommended that you use a Windows or a Linux machine to receive syslog messages.
Use Advanced Syslog Options	
Port	Port in which the remote syslog server listens. By default, it is set to 514. Valid options are from 1 to 65535.
Facility Code	Syslog facility code to be used for logging. Valid options are Local0 through Local7.

Email Settings

Define the email address for the mail server and the name that is shown for messages received from the mail server, such as admin@somedomain.com.

Table A-56 Email Settings

Option	Description
Mail Server	Enter a valid email host server.
Mail From	Enter the name that users see when they receive a message from the mail server, such as admin@somedomain.com.

Failure Reasons Editor

View and edit failure reasons.

Viewing Failure Reasons

Table A-57 Viewing Failure Reasons

Option	Description
Failure Reasons	The name of possible failure reasons. Click a failure reason name to open the Failure Reasons Editor page.

Editing Failure Reasons

Table A-58 Editing Failure Reasons

Option	Description
Failure Reason	Display only. The error code and associated failure reason name.
Description	Enter a free text description of the failure reason to assist administrators; use the text tools as needed.
Resolution Steps	Enter a free text description of possible resolution steps for the failure reason to assist administrators; use the text tools as needed.

Results Summary

Table A-59 Results Summary for Failure Reasons

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

System Alarm Settings

Enable, disable, and configure system alarm notification settings.

Table A-60 System Alarm Settings

Option	Description
System Alarm Settings	
Notify System Alarms	Check this check box to enable system alarm notification.
System Alarms Suppress Duplicates	Designate the number of hours that you want to suppress duplicate system alarms from being sent to the Email Notification User List. Valid options are 1, 2, 4, 6, 8, 12, and 24.
Email Notification	

Table A-60 System Alarm Settings (continued)

Option	Description
Email Notification User List	Enter a comma-separated list of e-mail addresses or ISE administrator names or both. Do one of the following: • Enter the e-mail addresses. • Click **Select** and enter valid administrator names. The administrator is notified by e-mail only if e-mail identification is specified in that administrator's account. When a system alarm occurs, an e-mail is sent to all the recipients in the Email Notification User List. Click **Clear** to clear this field.
Email in HTML Format	Select this check box to send e-mail notifications in HTML format, or uncheck to send s plain text.
Syslog Notification	
Send Syslog Message	Select this check box to send a syslog message for each system alarm generates **Note** To send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. See Configuring Alarm Syslog Targets, page 23-54 for more information.

System > Maintenance > Data Management > Monitoring Node

To access monitoring data management tools, go to **Administration > System > Maintenance**, then expand **Data Management > Monitoring Node** in the left panel. This section covers the user interface elements for the following tools:

- Full Backup On Demand, page A-61
- Scheduled Backup, page A-62
- Data Purging, page A-62
- Data Restore, page A-63

Full Backup On Demand

Perform a full backup of the monitoring database on demand.

Table A-61 Full Backup On Demand

Option	Description
Data Repository	Select a repository from the drop-down list, in which to back up the monitoring database. If no repository is selected, a backup will not occur.
Backup Now	Click to perform a full backup of the monitoring database.
Full Backup On Demand Status	Shows the Name, Start Time, End Time, and Status of an on demand backup.

Scheduled Backup

Schedule an incremental or full monitoring database backup.

Table A-62 Scheduled Backup

Option	Description
Incremental Backup	
On	Click the **On** radio button to enable incremental backup.
Off	Click the **Off** radio button to disable incremental backup.
Configure Incremental Monitor Database Backup	
Data Repository	Select a data repository for the backup files.
Schedule	Select the time of the day to perform the incremental backup.
Frequency	Choose the frequency of incremental backups: • Daily • Weekly—Typically occurs at the end of every week. • Monthly—Typically occurs at the end of every month.
Configure Full Monitor Database Backup	
Data Repository	Select a data repositoryused to store the backup files.
Schedule	Select the time of the day to perfrom the database backup.
Frequency	Choose the frequency of the backups: • Daily—Occurs at the specified time each day. • Weekly—Occurs on the last day of every week. • Monthly—Occurs on the last day of every month.

Data Purging

Purge data prior to an incremental or full backup.

Table A-63 Data Purging

Option	Description
Data Purging	
Percentage of Disk Space	Enter a numerical percentage value for allowed disk space usage. This threshold triggers a purge when disk space usage meets or exceeds this value. The default is 80 percent. The maximum value allowed is 100 percent.
Data Repository	Select the data repository to backup data prior to purge.
Maximum Stored Data Period	Enter a value in (30-day) months to be utilized when the disk space usage threshold for purging (Percentage of Disk Space) is met. **Note** For this option, each month consists of 30 days. The default of three months equals 90 days.

Table A-63 Data Purging (continued)

Option	Description
Submit	Click to proceed with the data purge.
Cancel	Click to exit without purging data.

Data Restore

Restore a full or incremental backup.

Table A-64 Data Restore

Column	Description
Available Backups to Restore	Select the radio button next to the name of the backup you want to restore. The backup filename includes the time stamp. For example, ISEViewBackup-20090618_003400.
Date	Shows the date of the backup
Repository	Shows the name of the repository where the backup is stored.
Type	Shows the type of backup, full or incremental
Restore	Click to restore the selected backup of the monitoring database.



APPENDIX B

Network Access Flows

This appendix describes the authentication flows in Cisco Identity Services Engine (ISE) by using RADIUS-based Extensible Authentication Protocol (EAP) and non-EAP protocols.

Authentication verifies user information to confirm user identity. Traditional authentication uses a name and a fixed password. More-secure methods use cryptographic techniques, such as those used inside the Challenge Authentication Handshake Protocol (CHAP), one-time password (OTP), and advanced EAP-based protocols. Cisco ISE supports a variety of these authentication methods.

A fundamental implicit relationship exists between authentication and authorization. The more authorization privileges that are granted to a user, the stronger the authentication should be. Cisco ISE supports this relationship by providing various methods of authentication.

The most popular, simplest, and least-expensive method of authentication involves the use of usernames and passwords. The disadvantage is that this information can be told to someone else, guessed, or captured. An approach that uses simple, unencrypted usernames and passwords is not considered a strong authentication mechanism, but it can be sufficient for low-authorization or low-privilege levels such as Internet access.

You should use encryption to reduce the risk of password capture on the network. Client and server access control protocols such as RADIUS encrypt passwords to prevent them from being captured within a network. However, RADIUS operates only between the authentication, authorization, and accounting (AAA) client and Cisco ISE. Before this point in the authentication process, unauthorized persons can obtain cleartext passwords; for example, in the following setups:

- The communication between an end-user client that dials up over a phone line
- An ISDN line that terminates at a network access server
- Over a Telnet session between an end-user client and the hosting device

RADIUS is a client/server protocol through which remote-access servers communicate with a central server to authenticate dial-in users, and to authorize their access to the requested system or service. You can use RADIUS to maintain user profiles in a central database that all remote servers can share. This protocol provides better security, and you can use it to set up a policy that is applied at a single administered network point.

RADIUS also functions as a RADIUS client in Cisco ISE to proxy requests to a remote RADIUS server, and it provides Change of Authorization (CoA) activities during an active session.

Cisco ISE supports RADIUS protocol flow according to RFC 2865 and generic support for all general RADIUS attributes as described in RFC 2865 and its extension. Cisco ISE supports parsing of vendor-specific attributes only for vendors that are defined in the Cisco ISE dictionary. See "Dictionaries and Dictionary Attributes" section on page 7-1 for information on dictionaries.

RADIUS interface supports the following attribute data types that are defined in RFC 2865:

- Text (Unicode Transformation Format [UTF])
- String (binary)
- Address (IP)
- Integer
- Time

Network Access Use Cases

For network access, a host connects to the network device and requests to use network resources. The network device identifies the newly connected host, and, using the RADIUS protocol as a transport mechanism, requests Cisco ISE to authenticate and authorize the user.

Cisco ISE supports the following categories of network access flows, depending on the protocol that is transported over the RADIUS protocol:

- RADIUS-Based Protocols Without EAP, page B-2
- RADIUS-Based EAP Protocols, page B-4

RADIUS-Based Protocols Without EAP

RADIUS-based protocols that do not include EAP include the following:

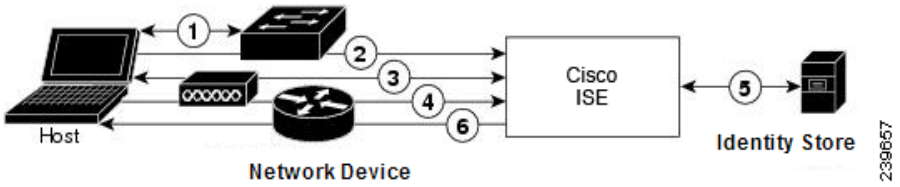
- Password Authentication Protocol (PAP)
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)
- MS-CHAP version 2 (MS-CHAPv2)

This section describes the RADIUS-based flow without EAP authentication. RADIUS-based flow with PAP authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends a RADIUS Access-Request to Cisco ISE that contains RADIUS attributes that are appropriate to the specific protocol that is being used (PAP, CHAP, MS-CHAPv1, or MS-CHAPv2).
3. Cisco ISE uses an identity store to validate user credentials.
4. The RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

Figure B-1 shows a RADIUS-based authentication without EAP.

Figure B-1 RADIUS-Based Authentication Without EAP



Cisco ISE supports the following non-EAP protocols:

- Password Authentication Protocol, page B-3
- Challenge Handshake Authentication Protocol, page B-4
- Microsoft Challenge Handshake Authentication Protocol version 1, page B-4
- Microsoft Challenge Handshake Authentication Protocol version 2, page B-4

Password Authentication Protocol

The PAP provides a simple method for users to establish their identity by using a two-way handshake. The PAP password is encrypted with a shared secret and is the least sophisticated authentication protocol.

Cisco ISE checks the username and password pair against the identity stores, until it eventually acknowledges the authentication or terminates the connection.

PAP is not a strong authentication method, since it offers little protection from repeated trial-and-error attacks.

The RADIUS-with-PAP-authentication flow includes logging of passed and failed attempts.

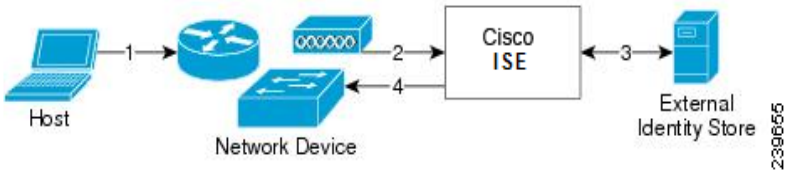
RADIUS PAP Authentication

You can use different levels of security concurrently with Cisco ISE for different requirements. PAP applies a two-way handshaking procedure. If authentication succeeds, Cisco ISE returns an acknowledgement; otherwise, Cisco ISE terminates the connection or gives the originator another chance.

The originator is in total control of the frequency and timing of the attempts. Therefore, any server that can use a stronger authentication method will offer to negotiate that method prior to PAP. RFC 1334 defines PAP.

Figure B-2 illustrates RADIUS with PAP authentication.

Figure B-2 RADIUS with PAP Authentication



1. A host connects to the network. Any communication protocol can be used, depending on the host.
2. The network device sends a RADIUS Access-Request to Cisco ISE.
3. Cisco ISE uses an external identity store to validate user credentials.
4. The RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

Cisco ISE supports standard RADIUS PAP authentication that is based on the RADIUS UserPassword attribute. RADIUS PAP authentication is compatible with all identity stores.

Challenge Handshake Authentication Protocol

CHAP uses a challenge-response mechanism with one-way encryption on the response. CHAP enables Cisco ISE to negotiate downward from the most-secure to the least-secure encryption mechanism, and it protects passwords that are transmitted in the process. CHAP passwords are reusable. If you are using the Cisco ISE internal database for authentication, you can use PAP or CHAP. CHAP does not work with the Microsoft user database. Compared to RADIUS PAP, CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client.

Cisco ISE supports standard RADIUS CHAP authentication that is based on the RADIUS ChapPassword attribute. Cisco ISE supports RADIUS CHAP authentication only with internal identity stores.

Microsoft Challenge Handshake Authentication Protocol version 1

Cisco ISE supports the RADIUS MS-CHAPv1 authentication and change-password features. RADIUS MS-CHAPv1 contains two versions of the change-password feature: Change-Password-V1 and Change-Password-V2.

Note Cisco ISE does not support Change-Password-V1 based on the RADIUS MS-CHAP-CPW-1 attribute, and supports only Change-Password-V2 based on the MS-CHAP-CPW-2 attribute.

The RADIUS MS-CHAPv1 authentication and change-password features are supported with the following identity sources:

- Internal identity stores
- Microsoft Active Directory identity store

Microsoft Challenge Handshake Authentication Protocol version 2

The RADIUS MS-CHAPv2 authentication and change-password features are supported with the following identity sources:

- Internal identity stores
- Active Directory identity store

RADIUS-Based EAP Protocols

EAP provides an extensible framework that supports various authentication types. Among them, Cisco ISE supports the following EAP methods:

- Simple EAP methods that do not use certificates:
  - Extensible Authentication Protocol-Message Digest 5
  - Lightweight Extensible Authentication Protocol
- EAP methods in which the client uses the Cisco ISE server certificate to perform server authentication:
  - Protected Extensible Authentication Protocol/EAP-MS-CHAPv2
  - Protected Extensible Authentication Protocol/EAP-GTC
  - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling/EAP-MS-CHAPv2
  - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling/EAP-GTC
- EAP methods that use certificates for both server and client authentication:

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

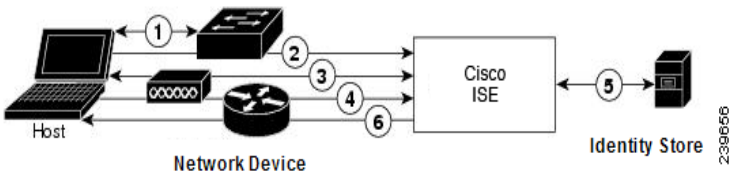
In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

Figure B-3 shows a RADIUS-based authentication with EAP.

Figure B-3 RADIUS-Based Authentication with EAP



Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) provides one-way client authentication. The server sends the client a random challenge. The client proves its identity by hashing the challenge and its password with MD5. Because a man in the middle could see the challenge and response, EAP-MD5 is vulnerable to dictionary attack when used over an open medium. Since no server authentication occurs, it is also vulnerable to spoofing. Cisco ISE supports EAP-MD5 authentication against the ISE internal identity store. Host Lookup is also supported when using the EAP-MD5 protocol. See "Table 16-3 Allowed Protocols Service" on page 16-15 for more information on Host Lookup.

Lightweight Extensible Authentication Protocol

Cisco ISE currently uses Lightweight Extensible Authentication Protocol (LEAP) only for Cisco Aironet wireless networking. If you do not enable this option, Cisco Aironet end-user clients who are configured to perform LEAP authentication cannot access the network. If all Cisco Aironet end-user clients use a different authentication protocol, such as Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) we recommend that you disable this option.

Note If users access your network by using a AAA client that is defined in the *Network Devices* section as a RADIUS (Cisco Aironet) device, then you must enable LEAP, EAP-TLS, or both; otherwise, Cisco Aironet users cannot authenticate.

Protected Extensible Authentication Protocol

Protected Extensible Authentication Protocol (PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol. Cisco ISE supports PEAP version 0 (PEAPv0) and PEAP version 1 (PEAPv1) with Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol (EAP-MS-CHAP), Extensible Authentication Protocol-Generic Token Card (EAP-GTC), and EAP-TLS inner methods. The Cisco Secure Services Client (SSC) supplicant supports all of the PEAPv1 inner methods that Cisco ISE supports.

Advantages of Using PEAP

Using PEAP presents these advantages:

- PEAP is based on TLS, which is widely implemented and has undergone extensive security review.
- It establishes a key for methods that do not derive keys.
- It sends an identity within the tunnel.
- It protects inner method exchanges and the result message.
- It supports fragmentation.

Supported Supplicants

PEAP supports these supplicants:

- Microsoft Built-In Clients 802.1X XP
- Microsoft Built-In Clients 802.1X Vista

- Cisco Secure Services Client (SSC) Release 4.0
- Cisco SSC Release 5.1
- Funk Odyssey Access Client 4.72
- Intel 12.4.0.0

PEAP Protocol Flow

A PEAP conversation can be divided into three parts:

1. Cisco ISE and the peer build a TLS tunnel. Cisco ISE presents its certificate, but the peer does not. The peer and Cisco ISE create a key to encrypt the data inside the tunnel.
2. The inner method determines the flow within the tunnel:
   - EAP-MS-CHAPv2 inner method—EAP-MS-CHAPv2 packets travel inside the tunnel without their headers. The first byte of the header contains the type field. EAP-MS-CHAPv2 inner methods support the change-password feature. You can configure the number of times that the user can attempt to change the password through the Cisco ISE user interface. User authentication attempts are limited by this number.
   - EAP-GTC inner method—Both PEAPv0 and PEAPv1 support the EAP-GTC inner method. The supported supplicants do not support PEAPv0 with the EAP-GTC inner method. EAP-GTC supports the change-password feature. You can configure the number of times that the user can attempt to change the password through the Cisco ISE user interface. User authentication attempts are limited by this number.
   - EAP-TLS inner method—The Windows built-in supplicant does not support fragmentation of messages after the tunnel is established, and this affects the EAP-TLS inner method. Cisco ISE does not support fragmentation of the outer PEAP message after the tunnel is established. During tunnel establishment, fragmentation works as specified in PEAP documentation. In PEAPv0, EAP-TLS packet headers are removed, and in PEAPv1, EAP-TLS packets are transmitted unchanged.
   - Extensible Authentication Protocol-type, length, value (EAP-TLV) extension—EAP-TLV packets are transmitted unchanged. EAP-TLV packets travel with their headers inside the tunnel.
3. There is protected acknowledgement of success and failure if the conversation has reached the inner method.

Note The client EAP message is always carried in the RADIUS Access-Request message, and the server EAP message is always carried in the RADIUS Access-Challenge message. The EAP-Success message is always carried in the RADIUS Access-Accept message. The EAP-Failure message is always carried in the RADIUS Access-Reject message. Dropping the client PEAP message results in dropping the RADIUS client message.

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is an authentication protocol that provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.

Benefits of EAP-FAST

EAP-FAST provides the following benefits over other authentication protocols:

- Mutual authentication—The EAP server must be able to verify the identity and authenticity of the peer, and the peer must be able to verify the authenticity of the EAP server.
- Immunity to passive dictionary attacks—Many authentication protocols require a password to be explicitly provided, either as cleartext or hashed, by the peer to the EAP server.
- Immunity to man-in-the-middle attacks—In establishing a mutually authenticated protected tunnel, the protocol must prevent adversaries from successfully interjecting information into the conversation between the peer and the EAP server.
- Flexibility to enable support for many different password authentication interfaces such as MS-CHAPv2, Generic Token Card (GTC), and others—EAP-FAST is an extensible framework that allows support of multiple internal protocols by the same server.
- Efficiency—When using wireless media, peers are limited in computational and power resources. EAP-FAST enables the network access communication to be computationally lightweight.
- Minimization of the per-user authentication state requirements of the authentication server—With large deployments, it is typical to have many servers acting as the authentication servers for many peers. It is also highly desirable for a peer to use the same shared secret to secure a tunnel much the same way that it uses the username and password to gain access to the network. EAP-FAST facilitates the use of a single, strong, shared secret by the peer, while enabling servers to minimize the per-user and device state that it must cache and manage.

EAP-FAST Flow

The EAP-FAST protocol flow is always a combination of the following phases:

- Provisioning phase—This is phase zero of EAP-FAST. During this phase, the peer is provisioned with a unique, strong secret that is referred to as the PAC that is shared between the Cisco ISE and the peer.
- Tunnel establishment phase—The client and server authenticate each other by using the PAC to establish a fresh tunnel key. The tunnel key is then used to protect the rest of the conversation and provides message confidentiality and with authenticity.
- Authentication phase—The authentication is processed inside the tunnel and includes the generation of session keys and protected termination.

Cisco ISE supports EAP-FAST versions 1 and 1a.



APPENDIX C

Switch Configuration Required to Support Cisco ISE Functions

To ensure Cisco ISE is able to interoperate with network switches and functions from Cisco ISE are successful across the network segment, you need to configure network switches with the necessary NTP, RADIUS/AAA, 802.1X, MAB, and other settings for communication with Cisco ISE, according to the following topics:

- Enable Your Switch to Support Standard Web Authentication, page C-2
- Define a Local User Name and Password for Synthetic RADIUS Transactions, page C-2
- Set the NTP Server to Ensure Accurate Log and Accounting Timestamps, page C-2
- Enable AAA Functions, page C-3
- RADIUS Servers Configuration, page C-3
- Enable RADIUS Change of Authorization (CoA), page C-4
- Enable Device Tracking and DHCP Snooping, page C-4
- Enable 802.1X Port-Based Authentication, page C-4
- Use EAP for Critical Authentications, page C-4
- Throttle AAA Requests Using Recovery Delay, page C-4
- Define VLANs Based on Enforcement States, page C-5
- Define Local (Default) ACLs on the Switch, page C-5
- Enable Cisco Security Group Access Switch Ports, page C-6
- Enable EPM Logging, page C-8
- Enable SNMP Traps, page C-8
- Enable SNMP v3 Query for Profiling, page C-8
- Enable MAC Notification Traps for Profiler to Collect, page C-8
- Configure the RADIUS Idle-Timeout, page C-8

Enable Your Switch to Support Standard Web Authentication

Ensure you include the following command lines in your switch configuration to enable standard Web Authenticating functions for Cisco ISE, including provisions for URL redirection upon authentication.

```
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.2.3
ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443
ip http secure-server
```

Define a Local User Name and Password for Synthetic RADIUS Transactions

Use this function to enable the switch to talk to the Cisco ISE node as though it is the RADIUS server for this network segment.

```
username test-radius password 0 cisco123
```

Set the NTP Server to Ensure Accurate Log and Accounting Timestamps

Be sure to specify the same NTP server as is set in Cisco ISE at **Administration > System > Settings > System Time**.

```
ntp server <IP_address>|<domain_name>
```

Enable AAA Functions

Use the following command lines to enable the various AAA functions between the switch and Cisco ISE, including 802.1X and MAB authentication functions.

```
aaa new-model
! Creates an 802.1X port-based authentication method list
aaa authentication dot1x default group radius
! Required for VLAN/ACL assignment
aaa authorization network default group radius
! Authentication & authorization for webauth transactions
aaa authorization auth-proxy default group radius
! Enables accounting for 802.1X and MAB authentications
aaa accounting dot1x default start-stop group radius
!
aaa session-id common
!
aaa accounting update periodic 15
aaa accounting update newinfo
! Update AAA accounting information periodically every 15 minutes, which is the minimum
recommended value.
aaa accounting system default start-stop group radius
!
aaa server radius dynamic-author <cr>
client 10.0.56.17 server-key cisco
! Enables ISE to act as a AAA server when interacting with the client at IP address
10.0.56.17
```

RADIUS Servers Configuration

Configure the switch to interoperate with Cisco ISE acting as the RADIUS source server.

```
!
radius-server attribute 6 on-for-login-auth
! Include RADIUS attribute 8 in every Access-Request
radius-server attribute 8 include-in-access-req
! Include RADIUS attribute 25 in every Access-Request
radius-server attribute 25 access-request include
! Wait 3 x 30 seconds before marking RADIUS server as dead
radius-server dead-criteria time 30 tries 3
!
! Use RFC-standard ports (1812/1813)
radius-server host <Cisco_ISE_IP_address> auth-port 1812 acct-port 1813 test username
test-radius key 0 <RADIUS-KEY>
!
radius-server vsa send accounting
radius-server vsa send authentication
!
! send RADIUS requests from the MANAGEMENT VLAN
ip radius source-interface <VLAN_number>
```

Note We recommend that you configure a dead-criteria time of 30 seconds with 3 retries to provide longer response times for RADIUS requests that use Active Directory for authentication.

Enable RADIUS Change of Authorization (CoA)

Specify the settings here to ensure the switch is able to appropriately handle RADIUS Change of Authorization behavior supporting Posture functions from Cisco ISE.

```
aaa server radius dynamic-author
  client <ISE-IP> server-key 0 cisco123
```

Note Cisco ISE uses port 1700 (IOS default) versus RFC default port 3799 for CoA. Existing Cisco Secure ACS 5.x customers may already have this set to port 3799 if they are using CoA as part of an existing ACS implementation.

Enable Device Tracking and DHCP Snooping

To help provide optional security-oriented functions from Cisco ISE, you can enable device tracking and DHCP snooping for IP substitution in dynamic ACLs on switch ports.

```
! Optional
ip dhcp snooping
! Required!
ip device tracking
```

Enable 802.1X Port-Based Authentication

This command line turns 802.1X authentication on for switch ports, globally.

```
dot1x system-auth-control
```

Use EAP for Critical Authentications

To support supplicant authentication requests over the LAN, enable EAP for critical authentications (Inaccessible Authentication Bypass).

```
dot1x critical eapol
```

Throttle AAA Requests Using Recovery Delay

When a critical authentication recovery event takes place, you can configure the switch to automatically introduce a delay (in seconds) to ensure Cisco ISE is able to launch services again following recovery.

```
authentication critical recovery delay 1000
```

Define VLANs Based on Enforcement States

Use the following command lines to define the VLAN names, numbers, and SVIs based on known enforcement states in your network. Create the respective VLAN interfaces to enable routing between networks. This can be especially helpful to handle multiple sources of traffic passing over the same network segments—traffic from both PCs and the IP phone through which the PC is connected to the network, for example.

Note The first IP helper goes to the DHCP server and the second IP helper sends a copy of the DHCP request to the inline posture node for profiling.

```
vlan <VLAN_number>
 name ACCESS
!
vlan <VLAN_number>
 name VOICE
!
interface <VLAN_number>
 description ACCESS
 ip address 10.1.2.3 255.255.255.0
 ip helper-address <DHCP_Server_IP_address>
 ip helper-address <Cisco_ISE_IP_address>
!
interface <VLAN_number>
 description VOICE
 ip address 10.2.3.4 255.255.255.0
 ip helper-address <DHCP_Server_IP_address>
 ip helper-address <Cisco_ISE_IP_address>
```

Define Local (Default) ACLs on the Switch

Enable these functions on older switches (with IOS releases earlier than 12.2(55)SE) to ensure Cisco ISE is able to perform the dynamic ACL updates required for authentication and authorization.

```
ip access-list extended ACL-ALLOW
 permit ip any any
!
ip access-list extended ACL-DEFAULT
  remark DHCP
  permit udp any eq bootpc any eq bootps
  remark DNS
  permit udp any any eq domain
  remark Ping
  permit icmp any any
  remark Ping
  permit icmp any any
  remark PXE / TFTP
  permit udp any any eq tftp
  remark Allow HTTP/S to ISE and WebAuth portal
  permit tcp any host <Cisco_ISE_IP_address> eq www
  permit tcp any host <Cisco_ISE_IP_address> eq 443
  permit tcp any host <Cisco_ISE_IP_address> eq 8443
  permit tcp any host <Cisco_ISE_IP_address> eq 8905
  permit udp any host <Cisco_ISE_IP_address> eq 8905
  permit udp any host <Cisco_ISE_IP_address> eq 8906
  permit tcp any host <Cisco_ISE_IP_address> eq 8080
  permit udp any host <Cisco_ISE_IP_address> eq 9996
```

```
remark Drop all the rest
  deny   ip any any log
!
! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL-WEBAUTH-REDIRECT
 deny ip any host <Cisco_ISE_IP_address>
 permit tcp any any eq www
 permit tcp any any eq 443
 permit tcp any any eq 8443
```

Enable Cisco Security Group Access Switch Ports

To ensure Cisco ISE is able to interoperate with an existing Cisco Security Group Access deployment, use the following procedure to ensure you have enabled all of the functions necessary on the switch.

Step 1 Enter configuration mode for all of the access switch ports:

```
interface range FastEthernet0/1-8
```

Step 2 Enable the switch ports for access mode (instead of trunk mode):

```
switchport mode access
```

Step 3 Statically configure the access VLAN. This provides local provisioning the access VLANs and is required for open-mode authentication.

```
switchport access <VLAN_number>
```

Step 4 Statically configure the voice VLAN:

```
switchport voice <VLAN_number>
```

Step 5 Enable open-mode authentication. Open-mode allows traffic to be bridged onto the data and voice VLANs before authentication is completed. Cisco strongly recommends using a port-based ACL in a production environment to prevent unauthorized access.

```
! Enables pre-auth access before AAA response; subject to port ACL
authentication open
```

Step 6 Apply a port-based ACL to determine which traffic should be bridged by default from unauthenticated endpoints onto the access VLAN. Since you should allow all access first and enforce policy later, you should apply ACL-ALLOW to permit all traffic through the switch port. You have already created a default ISE authorization to allow all traffic for now since we want complete visibility and not impact the existing end user experience yet.

```
! An ACL must be configured to prepend dACLs from AAA server.
ip access-group ACL-ALLOW in
```

Note Prior to software versions 12.2(55)SE on DSBU switches, a port ACL is required for dynamic ACLs from a RADIUS AAA server to be applied. Failure to have a default ACL will result in assigned dACLs being ignored by the switch. With 12.2(55)SE a default ACL will be automatically generated and applied.

Note We are using ACL-ALLOW at this point in the lab because we want to enable 802.1X port-based authentication but have no impact on the existing network. In a later exercise we will apply a different ACL-DEFAULT which blocks undesired traffic for a production environment.

Step 7 Enable Multi-Auth host mode. Multi-Auth is essentially a superset of Multi-Domain Authentication (MDA). MDA only allows a single endpoint in the data domain. When multi-auth is configured, a single authenticated phone is allowed in the voice domain (as with MDA) but an unlimited number of data devices can be authenticated in the data domain.

```
! Allow voice + multiple endpoints on same physical access port
authentication host-mode multi-auth
```

Note Multiple data devices (whether virtualized devices or physical devices connected to a hub) behind an IP phone can exacerbate the access ports' physical link-state awareness.

Step 8 Enable various authentication method options:

```
! Enable re-authentication
authentication periodic
! Enable re-authentication via RADIUS Session-Timeout
authentication timer reauthenticate server
authentication event fail action next-method
authentication event server dead action authorize <VLAN_number>
authentication event server alive action reinitialize
! IOS Flex-Auth authentication should do 802.1X then MAB
authentication order dot1x mab
authentication priority dot1x mab
```

Step 9 Enable 802.1X port control on the switchport:

```
! Enables port-based authentication on the interface
authentication port-control auto
authentication violation restrict
```

Step 10 Enable MAC Authentication Bypass (MAB):

```
! Enable MAC Authentication Bypass (MAB)
mab
```

Step 11 Enable 802.1X on the switchport

```
! Enables 802.1X authentication on the interface
dot1x pae authenticator
```

Step 12 Set the retransmit period to 10 seconds:

```
dot1x timeout tx-period 10
```

Note The dot1x tx-period timeout should be set to 10 seconds. Do not change this unless you understand the implications.

Step 13 Enable the portfast feature:

```
spanning-tree portfast
```

Enable EPM Logging

Set up standard logging functions on the switch to support possible troubleshooting/recording for Cisco ISE functions.

```
epm logging
```

Enable SNMP Traps

Ensure the switch is able to receive SNMP trap transmissions from Cisco ISE over the appropriate VLAN in this network segment.

```
snmp-server community public RO
snmp-server trap-source <VLAN_number>
```

Enable SNMP v3 Query for Profiling

Configure the switch to ensure SNMP v3 polling takes place as intended to support Cisco ISE profiling services. First, configure the SNMP settings in Cisco ISE at **Administration > Network Resources > Network Devices >Add | Edit > SNMP Settings**. See "Table 6-2 Network Devices List Page: SNMP Settings" on page 6-5 for details.

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
snmp-server group <group> v3 priv
snmp-server group <group> v3 priv context vlan-1
```

Note The **snmp-server group** <*group*> **v3 priv context** *vlan-1* command must be configured for each context. The **snmp show context** command lists all the context information.

If the SNMP Request times out and there is no connectivity issue, then you can increase the Timeout value.

Enable MAC Notification Traps for Profiler to Collect

Configure your switch to transmit the appropriate MAC notification traps so that the Cisco ISE Profiler function is able to collect information on network endpoints.

```
mac address-table notification change
mac address-table notification mac-move
snmp trap mac-notification change added
snmp trap mac-notification change removed
```

Configure the RADIUS Idle-Timeout

To configure the RADIUS Idle-timeout on a switch, use the following command:

```
Switch(config-if)# authentication timer inactivity
```

where inactivity is interval of inactivity in seconds, after which client activity is considered unauthorized.

In Cisco ISE, you can enable this option for any Authorization Policies to which such a session inactivity timer should apply from **Policy > Policy Elements > Results > Authorization > Authorization Profiles**. For more information on creating Authorization Policies, see Configuring Permissions for Authorization Profiles, page 17-27.



APPENDIX D

Troubleshooting Cisco ISE

This appendix addresses several categories of troubleshooting information that are related to identifying and resolving problems that you may experience when you use Cisco Identity Services Engine (ISE). This appendix contains the following sections:

- Installation and Network Connection Issues, page D-2
- Licensing and Administrator Access, page D-8
- Configuration and Operation (Including High Availability), page D-9
- External Authentication Sources, page D-12
- Client Access, Authentication, and Authorization, page D-17
- Error Messages, page D-29
- Configure NADs for ISE Monitoring, page D-33
- Troubleshooting APIs, page D-34
- Contacting the Cisco Technical Assistance Center, page D-35

Note This appendix is kept as up-to-date as possible with regards to presentation on Cisco.com as well as the online Help content available in the Cisco ISE software application, itself. For the most up-to-date material following Cisco Identity Services Engine, Release 1.1, however, Cisco recommends using the stand-alone *Cisco Identity Services Engine Troubleshooting Guide, Release 1.1*.

Installation and Network Connection Issues

If you believe you are experiencing hardware-related complications, first verify the following on all of your deployed Cisco ISE nodes:

- The external power cable is connected, and the proper power source is being applied.
- The external cables connecting the appliance to the network are all secure and in good order.
- The appliance fan and blower are operating.
- Inadequate ventilation, blocked air circulation, excessive dust or dirt, fan failures, or any environmental conditions that might affect the power or cooling systems.
- The appliance software boots successfully.
- The adapter cards (if installed) are properly installed in their slots, and each card initializes (and is enabled by the appliance software) without problems. Check status LEDs on the adapter card that can aid you identifying a potential problem.

For more information on Cisco ISE hardware installation and operational troubleshooting, including power and cooling requirements and LED behavior, see the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

Tip For issues regarding potential network access device (NAD) configuration issues, including AAA, RADIUS, profiler, and web authentication, you can perform several validation analyses by choosing the Cisco ISE **Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator** options.

Current Installation and Network Connection Troubleshooting Topics

- Unknown Network Device, page D-3
- CoA Not Initiating on Client Machine, page D-3
- Users Are Assigned to Incorrect VLAN During Network Access Sessions, page D-3
- Client Machine URL Redirection Function Not Working, page D-4
- Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page D-5
- RADIUS Accounting Packets (Attributes) Not Coming from Switch, page D-5
- Policy Service ISE Node Not Passing Traffic, page D-6
- Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation, page D-7
- Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working, page D-7

Unknown Network Device

Symptoms or Issue	Cisco ISE is not able to identify the specified Network Access Device (NAD).
Conditions	Click the magnifying glass icon in Authentications to display the steps in the Authentication Report. The logs display the following error message: • 11007 Could not locate Network Device or AAA Client Resolution
Possible Causes	• The administrator did not correctly configure the network access device (NAD) type in Cisco ISE. • Could not find the network device or the AAA Client while accessing NAS by IP during authentication.
Resolution	• Add the NAD in Cisco ISE again, verifying the NAD type and settings. • Verify whether the Network Device or AAA client is correctly configured in **Administration > Network Resources > Network Devices**

CoA Not Initiating on Client Machine

Symptoms or Issue	Users logging into the Cisco ISE network are not experiencing the required Change of Authorization (CoA).
Conditions	Cisco ISE uses port 1700 by default for communicating RADIUS CoA requests from supported network devices.
Possible Causes	Cisco ISE network enforcement points (switches) may be missing key configuration commands, may be assigning the wrong port (i.e., a port other than 1700), or have an incorrect or incorrectly entered key.

Resolution	Ensure the following commands are present in the switch configuration file (this is required on switch to activate CoA and configure):
	`aaa server radius dynamic-author`
	`client <Monitoring_node_IP_address> server-key <radius_key>`

Users Are Assigned to Incorrect VLAN During Network Access Sessions

Symptoms or Issue	Client machines are experiencing a variety of access issues related to VLAN assignments.

Conditions	Click on the magnifying glass icon in Authentications to launch the Authentication Details. The session event section of the authentication report should have the following lines: • %AUTHMGR-5-FAIL: Authorization failed for client (001b.a912.3782) on Interface Gi0/3 AuditSessionID 0A000A760000008D4C69994E • %DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND: Attempt to assign non-existent or shutdown VLAN 666 to 802.1x port FastEthernet1/9 You can also run the troubleshooting workflow for the authentication. This workflow compares the ACL authentication log that contains RADIUS switch responses with the switch message database. Logging configuration (global) details may also be displayed: • Mandatory Expected Configuration Found On Device • logging monitor informational Missing • logging origin-id ip Missing • logging source-interface <*interface_id*> Missing • logging <*syslog_server_IP_address_x*> transport udp port 20514 Missing **Note** The network device must send syslog messages to the Monitoring ISE node server port 20514.
Possible Causes	The switch is missing (or contains the incorrect) name and numbers on the switch.
Resolution	Verify VLAN configuration(s) on the network access/enforcement points (switches) in your deployment.

Client Machine URL Redirection Function Not Working

Symptoms or Issue	Users are not appropriately redirected to the correct URL for authentication.
Conditions	The monitoring and troubleshooting configuration validator is designed to catch this. The web authentication configuration (global) details may display something like the following: • Mandatory Expected Configuration Found On Device • aaa authorization auth-proxy default group <*radius_group*> aaa authorization auth-proxy default group radius • aaa accounting auth-proxy default start-stop group <*radius_group*> Missing • ip admission name <*word*> proxy http inactivity-time 60 Missing fallback profile <*word*> • ip access-group <*word*> in • ip admission <*word*> Missing • ip http server ip http server • ip http secure-server ip http secure-server
Possible Causes	The switch is missing the **ip http server** and/or **ip http secure-server** command.
Resolution	Verify and (if necessary) adjust the configuration on the switch.

Cisco ISE Profiler is Not Able to Collect Data for Endpoints

Symptoms or Issue	Known devices on the network are not being profiled according to profiler policies in Cisco ISE.
Conditions	The monitoring and troubleshooting workflow catches device discovery configuration (global) details like the following: • Mandatory Expected Configuration Found On Device • ip dhcp snooping vlan <*Vlan_ID_for_DHCP_Snooping*> ip dhcp snooping vlan 1-4096 • no ip dhcp snooping information option Missing • ip dhcp snooping ip dhcp snooping • ip device tracking ip device tracking
Possible Causes	One or more Cisco ISE network enforcement points (switches) may be missing the **ip dhcp snooping** and/or **ip device tracking** commands that enable Profiler to perform its function.
Resolution	Verify switch configuration for those network segments where endpoints are not being appropriately profiled to ensure that: • The required information to profile the endpoint is being sent to Cisco ISE for it to profile. • Probes are configured on the network Policy Service ISE node entities. • Verify that packets are received at the Cisco ISE profiler module by running the tcpdump function at **Operations > Troubleshoot > Diagnostic Tools > General Tools > Tcpdump**. **Note** If you are observing this issue with endpoints on a WAN collected by HTTP, Netflow, and NMAP, ensure that the endpoint IP address has been updated with a RADIUS/DHCP Probe before other attributes are updated using the above probes.

RADIUS Accounting Packets (Attributes) Not Coming from Switch

Symptoms or Issue	The switch is not transmitting RADIUS accounting packets (attributes) to the RADIUS server.

Conditions	Click on the magnifying glass icon in Authentications to launch the authentication details. The session event section of the authentication report should show the accounting events. Clicking on the accounting events shows that audit-session-id fields are blank because the VSA[1] are blocked and no cisco-av-pair=audit-session-id messages are sent from the switch. The same can be done by running the accounting report for the day, where all audit-session-id fields should be blank. **Note** This issue is reported by the monitoring and troubleshooting configuration validator's RADIUS configuration (global) details. – Mandatory Expected Configuration Found On Device – radius-server attribute 6 support-multiple Missing – radius-server attribute 8 include-in-access-req radius-server attribute 8 include-in-access-req – radius-server host <*radius_ip_address1*> auth-port 1812 acct-port 1813 key <*radius_key*> Missing – radius-server vsa send accounting radius-server vsa send accounting – radius-server vsa send authentication radius-server vsa send authentication **Note** Be sure to include “radius-server attribute 25 access-request include” in the switch configuration.
Possible Causes	The Cisco ISE network enforcement device (switch) is missing the **radius-server vsa send accounting** command.
Resolution	Verify that the switch RADIUS configuration for this device is correct and features the appropriate command(s).

1. VSA = vendor-specific attribute

Policy Service ISE Node Not Passing Traffic

Symptoms or Issue	Network traffic is not traversing the network segment where a network policy enforcement device is installed.
Conditions	This issue can affect a Cisco ISE and other types of NADs that have been deployed as Policy Service ISE nodes to interoperate with another network device.
Possible Causes	There are multiple possible causes for an issue such as this.
Resolution	1. Use the **tcpdump** command in the NAD command-line interface (CLI) or from the Administration ISE node user interface at **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump** to verify whether the machine is receiving and forwarding traffic as required for your network. 2. If the TCP dump operation indicates that the Cisco ISE or NAD is working as configured, verify other adjacent network components.

Registered Nodes in Cisco ISE Managed List Following Standalone Reinstallation

Symptoms or Issue	The Administration ISE node user interface displays the Policy Service ISE node host name and configuration information when Cisco ISE is reimaged and installed as a new standalone node.
Conditions	This applies to a Cisco ISE node previously deployed as the Administration persona managing one or more associated Policy Service ISE nodes.
Possible Causes	If the Policy Service ISE nodes are still configured to send syslog updates to the Administration persona as it was originally set up, node information is learned when the Administration persona receives syslog messages. That information is likely used to populate the system summary page on the Administration persona.
Resolution	If you have not "deregistered" the Policy Service ISE nodes from the Cisco ISE node, reconfigure the Policy Service ISE nodes so that it sends syslog messages to itself, rather than the Cisco ISE node and restart the Policy Service ISE node. **Note** If you deregister any associated Policy Service ISE nodes before reinstalling the Cisco ISE software and reconfiguring the Administration persona, the Policy Service ISE nodes will operate in standalone mode and will not transmit the erroneous syslog updates.

Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working

Symptoms or Issue	Two Inline Posture nodes that are deployed as high-availability peers appear dead to one another.
Conditions	Two Inline Posture nodes that are deployed in a "collocated" high-availability deployment.
Possible Causes	If the eth2 and eth3 interfaces on the Inline Posture nodes are not connected, both nodes will act as though the other node in the deployment has experienced some sort of failure.
Resolution	The heartbeat protocol requires a direct cable connection between the eth2 interfaces of both nodes in a high-availability pair, as well as a direct cable connection between the eth3 interfaces of the two nodes. You can use any Ethernet cable to make these connections.

Licensing and Administrator Access

- Certificate Expired, page D-8

Certificate Expired

Symptoms or Issue	• Administrator begins to see alarm messages starting 30 days before certificate expiration. • If the certificate has expired, users cannot log into the network via Cisco ISE until the certificate has been refreshed.
Conditions	This issue can apply to any expired certificates on Cisco ISE.
Possible Causes	Your Cisco ISE certificate is about to expire or has expired.
Resolution	Refresh your Cisco ISE trusted certificate.

Configuration and Operation (Including High Availability)

- Client Machines Are Not Able to Authenticate, page D-9
- Users Are Not Appropriately Redirected to URL, page D-9
- Cannot Download Remote Client Provisioning Resources, page D-10
- Lost Monitoring and Troubleshooting Data After Registering Policy Service ISE Node to Administration ISE Node, page D-10
- Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8, page D-11
- Data Out of Sync Between Primary And Secondary ISE Nodes, page D-11

Client Machines Are Not Able to Authenticate

Symptoms or Issue	• Client sessions are not completing 802.1X authentication. • Click the magnifying glass icon in Authentications for the specific DACL to launch the authentication details. The content of the ACL should reveal one or more bad characters.
Conditions	Click on magnifying glass icon in Authentications to launch the Authentication Details. The session event section of the authentication report should have the following entry: `%EPM-4-POLICY_APP_FAILURE: IP 0.0.0.0| MAC 0002.b3e9.c926| AuditSessionID 0A000201000023903983718| AUTHTYPE DOT1X| POLICY_TYPE Named ACL| POLICY_NAME xACSACLx-IP-acl_access-4918c248| RESULT FAILURE| REASON Interface ACL not configured`
Possible Causes	• The DACL syntax may be incorrect or not configured in Cisco ISE. • When Cisco ISE enforces the DACL and there is no pre-authentication ACL configured on the switch, the NAD brings down the session and authentication fails.
Resolution	Depending on the nature of the problem: • Correct the DACL syntax configured in Cisco ISE and ensure that it also includes the **permit udp any any** command. • Configure the appropriate pre-authentication ACL on the switch.

Users Are Not Appropriately Redirected to URL

Symptoms or Issue	Administrator receives one or more “Bad URL” error messages from Cisco ISE.
Conditions	This scenario applies to 802.1X authentication as well as guest access sessions. Click the magnifying glass icon in Authentications to launch the Authentication Details. The authentication report should have the redirect URL in the RADIUS response section as well as the session event section (which displays the switch syslog messages).

Possible Causes	Redirection URL is entered incorrectly with invalid syntax or a missing path component.
Resolution	Verify that the redirection URL specified in Cisco ISE via Cisco-av pair "URL Redirect" is correct per the following options: • CWA Redirection URL: https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cwa • 802.1X Redirection URL: url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&action=cpp

Cannot Download Remote Client Provisioning Resources

Symptoms or Issue	Administrator receives one or more "java.net.NoRouteToHostException: No route to host" error messages when trying to download client provisioning resources.
Conditions	This issue applies to any Cisco ISE that is connected to an external client provisioning resource store.
Possible Causes	Your internet connection may not be working properly or reliably.
Resolution	• Verify your internet connection settings. • Ensure that you have configured the correct proxy settings in Cisco ISE at **Administration > System > Settings > Proxy**.

Lost Monitoring and Troubleshooting Data After Registering Policy Service ISE Node to Administration ISE Node

Symptoms or Issue	The known collection of profiled endpoints is not visible on the secondary Policy Service ISE node when it is registered to the original (primary) Administration persona.
Conditions	This issue can come up in a deployment in which you register a new Policy Service ISE node to what has been, until the moment of registration, a standalone Cisco ISE node with a large store of known and profiled endpoints.
Possible Causes	Because of its potentially huge size, monitoring and troubleshooting data is not replicated between two nodes when the new node is registered to the original standalone Cisco ISE node. Cisco ISE does not replicate a data store that could conceivably be gigabytes in size, because it could impact network connectivity in a deployment environment.
Resolution	Ensure that you export monitoring and troubleshooting information *prior to* registering the new Policy Service ISE node to the formerly standalone Cisco ISE.

Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8

Symptoms or Issue	Administrator sees one or more “There is a problem with this website's security certificate.” messages after clicking on the dashlets in the Cisco ISE monitoring portal.
Conditions	This issue is specific to Internet Explorer 8. (This issue has not been observed when using Mozilla Firefox.)
Possible Causes	The security certificate for the Internet Explorer 8 browser connection is invalid or expired.
Resolution	Use Internet Explorer 8 to reimport a valid security certificate to view the dashlets appropriately.

Data Out of Sync Between Primary And Secondary ISE Nodes

Symptoms or Issues	Administrator sees any one of the following Replication or Sync Status: • Out of Sync • Node is not reachable • Replication disabled
Conditions	This issue occurs when the primary and secondary ISE nodes’ database are out of sync.
Possible Causes	This issue can occur: • When the database sync has failed because of change in system time backwards or any interruption during database sync. • When the node is not reachable. • When the certificate has expired. • When the secondary node is down for more than six hours.
Resolutions	You can do the following: • For out of sync issues, which most likely are due to time changes or NTP sync issues, you must correct the system time and perform a manual sync up through the UI. • For certificate expiry issues, you must install a valid certificate and perform a manual sync up through the UI. • For a node that has been down for more than six hours, you must restart the node, check for connectivity issues, and perform a manual sync up through the UI.

External Authentication Sources

- User Authentication Failed, page D-12
- Missing User for RADIUS-Server Test Username in Cisco ISE Identities, page D-12
- Connectivity Issues Between the Network Access Device (Switch) and Cisco ISE, page D-13
- Active Directory Disconnected, page D-13
- Cisco ISE Node Not Authenticating with Active Directory, page D-14
- RADIUS Server Error Message Entries Appearing in Cisco ISE, page D-14
- RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE), page D-15

User Authentication Failed

Symptoms or Issue	Authentications report failure reason: "Authentication failed: 22040 Wrong password or invalid shared secret"
Conditions	Click the magnifying glass icon in Authentications to view the steps in the authentication report that should display a brief series of messages as follows: • 24210 Looking up User in Internal Users IDStore - test-radius • 24212 Found User in Internal Users IDStore • 22040 Wrong password or invalid shared secret
Possible Causes	The user or device may not be supplying the correct credentials or RADIUS key to match with the external authentication source.
Resolution	Verify that the user credentials that are entered on the client machine are correct, and verify that the RADIUS server shared secret is correctly configured in both the NAD and Cisco ISE (they should be the same).

Missing User for RADIUS-Server Test Username in Cisco ISE Identities

Symptoms or Issue	The administrator notices one or more Authentications report failure messages like "Authentication failed: 22056 Subject not found in the applicable identity store(s)" for a given user ID.
Conditions	Click the magnifying glass icon in Authentications to view the messages in the Authentication Report. You should see a short series like the following: • 24210 Looking up User in Internal Users IDStore - test-radius • 24216 The user is not found in the internal users identity store • 22056 Subject not found in the applicable identity store(s)

Possible Causes	This message appears any time an authentication fails. In all cases, it's because the user is unknown to Cisco ISE. The subject could be a guest user who has not been added to the local database, a new employee who has not yet been appropriately provisioned in the network, or even a hacker. In addition, it is possible that the administrator did not configure the user ID in Cisco ISE.
Resolution	Check the local and external identity sources to verify whether the user ID exists, and if it does, ensure that both Cisco ISE and the associated access switch are configured to accept that user.

Connectivity Issues Between the Network Access Device (Switch) and Cisco ISE

Symptoms or Issue	Authentications report failure reason: “Authentication failed: 22040 Wrong password or invalid shared secret”
Conditions	Click the magnifying glass icon in Authentications to display authentication report entries like the following: • 24210 Looking up User in Internal Users IDStore - test-radius • 24212 Found User in Internal Users IDStore • 22040 Wrong password or invalid shared secret
Possible Causes	The network administrator may not have specified the correct password to enable the switch (or other NAD) to authenticate with Cisco ISE.
Resolution	Verify that the password that is configured on the NAD is correct to authenticate with Cisco ISE.

Active Directory Disconnected

Symptoms or Issue	The connection between Cisco ISE and the Active Directory server has been terminated, resulting in user authenticating failure.
Conditions	This issue is pertinent to any Active Directory domain topology that is connected to Cisco ISE.
Possible Causes	This scenario is most commonly caused by clock drift due to not syncing time via NTP[1] on VMware. This issue can also arise if the Cisco ISE FQDN[2] changes and/or the name of the certificate imported on the client machine has changed.
Resolution	Ensure that your Active Directory domain and Cisco ISE are aligned to the same NTP server source. Shut down or pause your Active Directory server and try to authenticate an employee to the network.

1. NTP = Network Time Protocol
2. FQDN = fully-qualified domain name

Cisco ISE Node Not Authenticating with Active Directory

Symptoms or Issue	The administrator receives “authentication failure” messages in the Authentication Failure Report on the Administration ISE node.
Conditions	This issue applies to Cisco ISE policy enforcement nodes added to an existing AD domain.
Possible Causes	• The administrator may not have changed the AD password on after joining the Cisco ISE node to the AD domain. • The account used to join Cisco ISE to the Active Directory domain may have an expired password.
Resolution	Change the account password that was used to join the AD domain after adding Cisco ISE to Active Directory.

RADIUS Server Error Message Entries Appearing in Cisco ISE

Symptoms or Issue	• Unsuccessful RADIUS or AAA[1] functions on Cisco ISE • Error messages in the **Operations > Authentication** event entries
Conditions	This scenario can become an issue in a system where Cisco ISE is configured to perform user authentication via an external identity source on the network.
Possible Causes	The following are possible causes for losing connectivity with the external identity source: • Subject not found in the applicable identity source • Wrong password or invalid shared secret • Could not locate network device or AAA client

Resolution	Check the Cisco ISE dashboard (**Operations > Authentications**) for any indication regarding the nature of RADIUS communication loss. (Look for instances of your specified RADIUS usernames and scan the system messages that are associated with any error message entries.) Log into the Cisco ISE CLI[2] and enter the following command to produce RADIUS attribute output that may aid in debugging connection issues: **test aaa group radius** <*username*> <*password*> **new-code** If this test command is successful, you should see the following attributes: • Connect port • Connect NAD IP address • Connect Policy Service ISE node IP address • Correct server key • Recognized username or password • Connectivity between the NAD and Policy Service ISE node You can also use this command to help narrow the focus of the potential problem with RADIUS communication by deliberately specifying incorrect parameter values in the command line and then returning to the administrator dashboard (**Operations > Authentications**) to view the type and frequency of error message entries that result from the incorrect command line. For example, to test whether or not user credentials may be the source of the problem, enter a username and or password that you *know* is incorrect, and then go look for error message entries that are pertinent to that username in the **Operations > Authentications** page to see what Cisco ISE is reporting.) **Note** This command does not validate whether or not the NAD is configured to use RADIUS, nor does it verify whether the NAD is configured to use the new AAA model.

1. AAA = authentication, authorization, and accounting
2. CLI = command-line interface

RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE)

Symptoms or Issue	• Unsuccessful RADIUS or AAA functions in Cisco ISE • The NAD is unable to ping the Policy Service ISE node
Conditions	This scenario is applicable in a system in which Cisco ISE is configured to perform user authentication via an external RADIUS server on the network.
Possible Causes	The following are possible causes for losing connectivity with the RADIUS server: • Network connectivity issue or issues • Bad server IP address • Bad server port

Resolution	If you are unable to ping the Policy Service ISE node from the NAD, try any or all of these possible solutions: • Verify the NAD IP address • Try using Traceroute and other appropriate "sniffer"-type tools to isolate the source of disconnection. (In a production environment, be cautious of overusing debug functions, because they commonly consume large amounts of available bandwidth and CPU, which can impact normal network operation.) Check the Cisco ISE "TCP Dump" report for the given Policy Service ISE node to see if there are any indications.

Client Access, Authentication, and Authorization

- Cannot Authenticate on Profiled Endpoint, page D-17
- Quarantined Endpoints Do Not Renew Authentication Following Policy Change, page D-18
- Endpoint Does Not Align to the Expected Profile, page D-19
- User is Unable to Authenticate Against the Local Cisco ISE Identity Store, page D-19
- Certificate-Based User Authentication via Supplicant Failing, page D-20
- 802.1X Authentication Fails, page D-21
- Users Are Reporting Unexpected Network Access Issues, page D-22
- Authorization Policy Not Working, page D-23
- Switch is Dropping Active AAA Sessions, page D-24
- URL Redirection on Client Machine Fails, page D-24
- Agent Download Issues on Client Machine, page D-26
- Agent Login Dialog Not Appearing, page D-27
- Agent Fails to Initiate Posture Assessment, page D-27
- Agent Displays “Temporary Access”, page D-28
- Cisco ISE Does Not Issue CoA Following Authentication, page D-28

Cannot Authenticate on Profiled Endpoint

Symptoms or Issue	• The IP phone was profiled but was not authorized properly. Therefore, it was not assigned to the voice VLAN. • The IP phone was profiled and authorized properly, but was not assigned to the correct voice VLAN. • The endpoint has been successfully profiled in Cisco ISE, but user authentication fails.
Conditions	The administrator will see the Authentications Log Error message: “22056 Subject not found in the applicable identity store(s)” containing the following entries: • 24210 Looking up User in Internal Users IDStore - 00:03:E3:2A:21:4A • 24216 The user is not found in the internal users identity store • 22056 Subject not found in the applicable identity store(s)
Possible Causes	• This could be either a MAB[1] or 802.1X authentication issue. • The authorization profile could be missing the Cisco av-pair=”device-traffic-class=voice” attribute. As a result, the switch does not recognize the traffic on the voice VLAN. • The administrator did not add the endpoint as static identity, or did not allow an unregistered endpoint to pass (create a policy rule to “Continue/Continue/Continue” upon failure).

Resolution	• Verify that the Authorization Policy is framed properly for groups and conditions, and check to see whether the IP phone is profiled as an "IP phone" or as a "Cisco-device." • Verify the switch port configuration for multidomain and voice VLAN configuration. • Add the continue/continue/continue to allow the endpoint to pass: **a.** Choose **Policy > Policy Elements > Results > Authentication > Allowed Protocols** to create a Protocol Policy. MAC authentications use PAP[2]/ASCII and EAP-MD5[3] protocols. Enable the following MAB_Protocols settings: – Process Host Lookup – PAP/ASCII – Detect PAP as Host Lookup – EAP-MD5 – Detect EAP-MD5 as Host Lookup **b.** From the main menu, choose **Policy > Authentication**. **c.** Change the authentication method from Simple to Rule-Based **d.** Use the action icon to create new Authentication Method entries for MAB: – Name: MAB – Condition: IF MAB RADIUS:Service-Type == Call Check – Protocols: allow protocols MAB_Protocols and use – Identity Source: Internal – Hosts: Continue/Continue/Continue

1. MAB = MAC authentication bypass
2. PAP = Password Authentication Protocol
3. EAP = Extensible AUthentication Protocol; MD5 = Message Digest 5

Quarantined Endpoints Do Not Renew Authentication Following Policy Change

Symptoms or Issue	Authentication has failed following policy change or additional identity and no reauthentication is taking place. The endpoint in question remains unable to connect or authentication fails.
Conditions	This issue often occurs on client machines that are failing posture assessment per the posture policy that is assigned to the user role.
Possible Causes	The authentication timer may not be set correctly on the client machine, or the authentication interval may not be set correctly on the switch.

Resolution	There are several possible resolutions for this issue: 1. Check the Session Status Summary report in Cisco ISE for the specified NAD or switch, and ensure that the interface has the appropriate authentication interval configured. 2. Enter "show running configuration" on the NAD/switch and ensure that the interface is configured with an appropriate "authentication timer restart" setting. (For example, "authentication timer restart 15," and "authentication timer reauthenticate 15.") 3. Try entering "interface shutdown" and "no shutdown" to bounce the port on the NAD/switch and force reauthentication following a potential configuration change in Cisco ISE.



Note Since CoA requires a MAC address or session ID, Cisco recommends that you do not bounce the port that is shown in the Network Device SNMP report.

Endpoint Does Not Align to the Expected Profile

Symptoms or Issue	An IP phone is plugged in and the profile appears as a "Cisco-Device."
Conditions	Launch the Endpoint Profiler/Endpoint Profiler Summary report and click **Details** for the MAC address that corresponds to the profiled endpoint in question.
Possible Causes	• There could be an SNMP configuration issue on Cisco ISE, the switch, or both. • The profile is likely not configured correctly, or contains the MAC address of the endpoint already.
Resolution	• Verify the SNMP version configuration on both Cisco ISE and the switch for SNMP trap and SNMP server settings. • The Profiler profile needs to be updated. Navigate to **Administration > Identity Management > Identities > Endpoints**, select the endpoint by MAC address and click **Edit**.

User is Unable to Authenticate Against the Local Cisco ISE Identity Store

Symptoms or Issue	User cannot authenticate from supplicant.

Conditions	Authentications report failure reason: "Authentication failed: 22056 Subject not found in the applicable identity store(s)" Click the magnifying glass in Authentications to launch the Authentication report that displays the following: • 24210 Looking up User in Internal Users IDStore - ACSXP-SUPP2\Administrator • 24216 The user is not found in the internal users identity store
Possible Causes	The supplicant is providing a name and password to authenticate against the local Cisco ISE user database, but those credentials are not configured in the local database.
Resolution	Verify that the user credentials are configured in the Cisco ISE local identity store.

Certificate-Based User Authentication via Supplicant Failing

Symptoms or Issue	User authentication is failing on the client machine, and the user is receiving a "RADIUS Access-Reject" form of message.

Conditions	(This issue occurs with authentication protocols that require certificate validation.) Possible Authentications report failure reasons: • "Authentication failed: 11514 Unexpectedly received empty TLS message; treating as a rejection by the client" • "Authentication failed: 12153 EAP-FAST failed SSL/TLS handshake because the client rejected the Cisco ISE local-certificate" Click the magnifying glass icon from Authentications to display the following output in the Authentication Report: • 12305 Prepared EAP-Request with another PEAP challenge • 11006 Returned RADIUS Access-Challenge • 11001 Received RADIUS Access-Request • 11018 RADIUS is re-using an existing session • 12304 Extracted EAP-Response containing PEAP challenge-response • 11514 Unexpectedly received empty TLS message; treating as a rejection by the client • 12512 Treat the unexpected TLS acknowledge message as a rejection from the client • 11504 Prepared EAP-Failure • 11003 Returned RADIUS Access-Reject • 11006 Returned RADIUS Access-Challenge • 11001 Received RADIUS Access-Request • 11018 RADIUS is re-using an existing session • 12104 Extracted EAP-Response containing EAP-FAST challenge-response • 12815 Extracted TLS Alert message • 12153 EAP-FAST failed SSL/TLS handshake because the client rejected the Cisco ISE local-certificate • 11504 Prepared EAP-Failure • 11003 Returned RADIUS Access-Reject **Note** This is an indication that the client does not have or does not trust the Cisco ISE certificates.
Possible Causes	The supplicant or client machine is not accepting the certificate from Cisco ISE. The client machine is configured to validate the server certificate, but is not configured to trust the Cisco ISE certificate.
Resolution	The client machine must accept the Cisco ISE certificate to enable authentication.

802.1X Authentication Fails

Symptoms or Issue	The user logging in via the client machine sees an error message from the supplicant that indicates that 802.1X authentication has failed.

Conditions	Troubleshooting Steps: 1. Choose **Operations > Authentications**. 2. Scroll over and look for the "Failure reason."
Possible Causes	Look for the details of the failed authentication record and click on the failure reason link under **Details > Resolution for the Authentication**. The failure reason should be listed.
Resolution	• Correct the failure reason per the findings that are defined in the Possible Causes. • Click on details icon of any active sessions, which takes you to the **AAA Protocol > RADIUS Authentication Details** report where you can find the **Authentication Summary > Radius Status** field stating failure reasons along with message code hyperlinks.

Note If authentication fails and there are no Authentications entries to search (assuming monitoring and troubleshooting is running properly), complete the following steps:

1. Ensure that the RADIUS server configuration on the switch is pointing to Cisco ISE.
2. Check network connectivity between the switch and Cisco ISE.
3. Verify that the Policy Service ISE node is running on Cisco ISE to ensure that it can receive RADIUS requests.

Users Are Reporting Unexpected Network Access Issues

Symptoms or Issue	Several symptoms for this issue could be taking place, including the following: • Users are being asked to download an agent other than what they expect. • Users who should have full network access are only allowed limited network access. • Although users are passing posture assessment, they are not getting the appropriate level of network access. • Users who should be allowed into the corporate (Access) VLAN are being left in the Authentication VLAN following authentication.
Conditions	Users are successfully authenticated, but are unable to get network access.
Possible Causes	• The administrator may not have specified the correct authorization profile. • The administrator did not define the appropriate policy conditions for the user access level. • The authorization profile, itself, might not have been framed properly.

Resolution	Ensure that the Identity Group Conditions are defined appropriately to support the authorization profile that is required for the user groups in question. 1. Choose **Operations > Authentication**. 2. Look for the identity group to which the user belongs. 3. Look at the authorization profile that is selected for that identity group. 4. Choose **Policy > Authorization** and verify that the correct rule is matching for that identity group. 5. If not, debug for the reason why the correct authorization policy is not matching.

Authorization Policy Not Working

Symptoms or Issue	The authorization policy that is specified by the administrator is the correct one, but the endpoint is not receiving the configured VLAN IP.
Conditions	This issue applies to standard user authorization sessions in a wired environment.
Possible Causes	The preauthorization ACL could be blocking DHCP traffic.

Resolution	• Ensure that the Cisco IOS release on the switch is equal to or more recent than the Cisco IOS Release 12.2.(53)SE.
	• Ensure that the identity group conditions are defined appropriately.
	• Check for the client machine port VLAN by using **show vlan** on the access switch. If the port is not showing the correct authorization profile VLAN, ensure that VLAN enforcement is appropriate to reach out to the DHCP server. If the VLAN is correct, the preauthorization ACL could be blocking DHCP traffic. Ensure that the preauthorization DACL is as follows:
	`remark Allow DHCP`
	`permit udp any eq bootpc any eq bootps`
	`remark Allow DNS`
	`permit udp any any eq domain`
	`remark ping`
	`permit icmp any any`
	`permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect`
	`permit tcp any host 80.0.80.2 eq www`
	`permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal port`
	`permit tcp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8906 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`deny ip any any`
	• Ensure the session is created on the switch by entering **show epm session summary**. If the IP address of the session shown is “not available,” ensure that the following configuration lines appear on the switch:
	`ip dhcp snooping vlan 30-100`
	`ip device tracking`

Switch is Dropping Active AAA Sessions

Symptoms or Issue	802.1X and MAB authentication and authorization are successful, but the switch is dropping active sessions and the **epm session summary** command does not display any active sessions.
Conditions	This applies to user sessions that have logged in successfully and are then being terminated by the switch.
Possible Causes	• The preauthentication ACL (and the subsequent DACL enforcement from Cisco ISE) on the NAD may not be configured correctly for that session. • The preauthentication ACL is configured and the DACL is downloaded from Cisco ISE, but the switch brings the session down. • Cisco ISE may be enforcing a preposture VLAN assignment rather than the (correct) postposture VLAN, which can also bring down the session.

Resolution	• Ensure the Cisco IOS release on the switch is equal to or more recent than Cisco IOS Release 12.2.(53)SE.
	• Check to see whether or not the DACL name in Cisco ISE contains a blank space (possibly around or near a hyphen "-"). There should be no space in the DACL name. Then ensure that the DACL syntax is correct and that it contains no extra spaces.
	• Ensure that the following configuration exists on the switch to interpret the DACL properly (if not enabled, the switch may terminate the session):
	`radius-server attribute 6 on-for-login-auth`
	`radius-server attribute 8 include-in-access-req`
	`radius-server attribute 25 access-request include`
	`radius-server vsa send accounting`
	`radius-server vsa send authentication`

URL Redirection on Client Machine Fails

Symptoms or Issue	The URL redirection page in the client machine's browser does not correctly guide the end user to the appropriate URL.
Conditions	This issue is most applicable to 802.1X authentication sessions that require URL redirection and Guest Centralized Web Authentication (CWA) login sessions.
Possible Causes	(There are multiple causes for this issue. See the **Resolutions** descriptions that follow for explanation.)

Resolution

- The two Cisco av-pairs that are configured on the authorization profile should exactly match the example below. (Note: Do *not* replace the "IP" with the actual Cisco ISE IP address.)
  - url-redirect=https://ip:8443/guestportal/gateway?...lue&action=cpp
  - url-redirect-acl=ACL-WEBAUTH-REDIRECT (ensure that this ACL is also defined on the access switch)
- Ensure that the URL redirection portion of the ACL have been applied to the session by entering the **show epm session ip** <*session IP*> command on the switch. (Where the session IP is the IP address that is passed to the client machine by the DHCP server.)

```
Admission feature : DOT1X
AAA Policies : #ACSACL#-IP-Limitedaccess-4cb2976e
URL Redirect ACL : ACL-WEBAUTH-REDIRECT
URL Redirect :
https://node250.cisco.com:8443/guestportal/gateway?sessionId=0A000A72
0000A45A2444BFC2&action=cpp
```

- Ensure that the preposture assessment DACL that is enforced from the Cisco ISE authorization profile contains the following command lines:

```
remark Allow DHCP
permit udp any eq bootpc any eq bootps
remark Allow DNS
permit udp any any eq domain
remark ping
permit icmp any any
permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect
permit tcp any host 80.0.80.2 eq www --> Provides access to internet
permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal
port
permit tcp any host 80.0.80.2 eq 8905 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
permit udp any host 80.0.80.2 eq 8905 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
permit udp any host 80.0.80.2 eq 8906 --> This is for posture
communication between NAC agent and ISE (Swiss ports)
deny ip any any
```

Note Ensure that the above URL Redirect has the proper Cisco ISE FQDN.

Resolution (continued)	• Ensure that the ACL with the name "ACL-WEBAUTH_REDIRECT" exists on the switch as follows:
	`ip access-list extended ACL-WEBAUTH-REDIRECT`
	` deny ip any host 80.80.80.2`
	` permit tcp any any eq www`
	` permit tcp any any eq 443`
	` permit tcp any any eq 8443`
	• Ensure that the HTTP and HTTPS servers are running on the switch:
	`ip http server`
	`ip http secure-server`
	• Ensure that, if the client machine employs any kind of personal firewall, it is disabled.
	• Ensure that the client machine browser is not configured to use any proxies.
	• Verify connectivity between the client machine and the Cisco ISE IP address.
	• If Cisco ISE is deployed in a distributed environment, make sure that the client machines are aware of the Policy Service ISE node FQDN.
	• Ensure that the Cisco ISE FQDN is resolved and reachable from the client machine.

Agent Download Issues on Client Machine

Symptoms or Issue	Client machine browser displays a "no policy matched" error message after user authentication and authorization.
Conditions	This issue applies to user sessions during the client provisioning phase of authentication.
Possible Causes	The client provisioning resource policy could be missing required settings.
Resolution	• Ensure that a client provisioning policy exists in Cisco ISE. If yes, verify the policy identity group, conditions, and type of agent(s) defined in the policy. (Also ensure whether or not there is any agent profile configured under **Policy > Policy Elements > Results > Client Provisioning > Resources > Add > ISE Posture Agent Profile**, even a profile with all default values.) • Try reauthenticating the client machine by bouncing the port on the access switch.

Note Remember that the client provisioning agent installer download requires the following:

- The user must allow the ActiveX installer in the browser session the first time an agent is installed on the client machine. (The client provisioning download page prompts for this.)
- The client machine must have Internet access.

Agent Login Dialog Not Appearing

Symptoms or Issue	The agent login dialog box does not appear to the user following client provisioning.
Conditions	This issue can generally take place during the posture assessment phase of any user authentication session.
Possible Causes	There are multiple possible causes for this type of issue. See the following **Resolution** descriptions for details.

Resolution	• Ensure that the agent is running on the client machine.
	• Ensure that the Cisco IOS release on the switch is equal to or more recent than Cisco IOS Release 12.2.(53)SE.
	• Ensure that the discovery host address on the Cisco NAC agent or Mac OS X agent is pointing to the Cisco ISE FQDN. (Right-click on the NAC agent icon, choose **Properties**, and check the discovery host.)
	• Ensure that the access switch allows Swiss communication between Cisco ISE and the end client machine. Limited access ACL applied for the session should allow Swiss ports:
	`remark Allow DHCP`
	`permit udp any eq bootpc any eq bootps`
	`remark Allow DNS`
	`permit udp any any eq domain`
	`remark ping`
	`permit icmp any any`
	`permit tcp any host 80.0.80.2 eq 443 --> This is for URL redirect`
	`permit tcp any host 80.0.80.2 eq www --> Provides access to internet`
	`permit tcp any host 80.0.80.2 eq 8443 --> This is for guest portal port`
	`permit tcp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`permit udp any host 80.0.80.2 eq 8905 --> This is for posture communication between NAC agent and ISE (Swiss ports)`
	`deny ip any any`
	• If the agent login dialog still does not appear, it could be a certificate issue. Ensure that the certificate that is used for Swiss communication on the end client is in the Cisco ISE certificate trusted list.
	• Ensure that the default gateway is reachable from the client machine.

Agent Fails to Initiate Posture Assessment

Symptoms or Issue	The user is presented with a “Clean access server not available” message.
Conditions	This issue applies to any agent authentication session from Cisco ISE.
Possible Causes	This error could mean that either the session has terminated or Cisco ISE is no longer reachable on the network.

Resolution	• The user can try to ping the default gateway or the RADIUS server IP address or FQDN supplied by the network administrator. • The user can try to log into the network again. • The administrator can check network access attributes for the user (like the assigned VLAN, ACLs, routing, execute the **nslookup** command on the client, client machine DNS connection, etc.).

Agent Displays "Temporary Access"

Symptoms or Issue	A client machine is granted "Temporary Access" following login and authentication, but administrator and user expect full network access.
Conditions	This issue is applicable to any client machine login session using an agent to connect.
Possible Causes	If the NAC Agent is running on the client and: • The interface on the client machine goes down • The session is terminated
Resolution	The user must try to verify network connectivity and then try to log in again (and pass through posture assessment, as well) to attempt to re-establish the connection.

Cisco ISE Does Not Issue CoA Following Authentication

Symptoms or Issue	CoA is not issued following client machine login and authentication.
Conditions	This specific issue is only applicable in a wired environment where CoA is required on the client machine to complete authentication.
Possible Causes	The access switch may not have the required configuration to support CoA for the client machine.

Resolution	• Ensure that the Cisco IOS release on the switch is equal to or more recent than Cisco IOS Release 12.2.(53)SE.
	• Ensure that the switch configuration features the following commands necessary to enable CoA:
	`aaa server radius dynamic-author`
	`client 80.0.80.2 server-key cisco456 --> ISE ip.`
	`server-key cisco456`

Error Messages

- ACTIVE_DIRECTORY_USER_INVALID_CREDENTIALS, page D-29
- ACTIVE_DIRECTORY_USER_AUTH_FAILED, page D-29
- ACTIVE_DIRECTORY_USER_PASSWORD_EXPIRED, page D-30
- ACTIVE_DIRECTORY_USER_WRONG_PASSWORD, page D-30
- ACTIVE_DIRECTORY_USER_ACCOUNT_DISABLED, page D-30
- ACTIVE_DIRECTORY_USER_RESTRICTED_LOGON_HOURS, page D-30
- ACTIVE_DIRECTORY_USER_NON_COMPLIANT_PASSWORD, page D-30
- ACTIVE_DIRECTORY_USER_UNKNOWN_DOMAIN, page D-31
- ACTIVE_DIRECTORY_USER_ACCOUNT_EXPIRED, page D-31
- ACTIVE_DIRECTORY_USER_ACCOUNT_LOCKED_OUT, page D-31
- ACTIVE_DIRECTORY_GROUP_RETRIEVAL_FAILED, page D-31
- ACTIVE_DIRECTORY_MACHINE_AUTHENTICATION_DISABLED, page D-31
- ACTIVE_DIRECTORY_ATTRIBUTE_RETRIEVAL_FAILED, page D-32
- ACTIVE_DIRECTORY_PASSWORD_CHANGE_DISABLED, page D-32
- ACTIVE_DIRECTORY_USER_UNKNOWN, page D-32
- ACTIVE_DIRECTORY_CONNECTION_FAILED, page D-32
- ACTIVE_DIRECTORY_BAD_PARAMETER, page D-32
- ACTIVE_DIRECTORY_TIMEOUT, page D-33

ACTIVE_DIRECTORY_USER_INVALID_CREDENTIALS

Description	This Authentication Failure message indicates that the user's credentials are invalid.
Resolution	Check if the Active Directory user account and credentials that are used to connect to the Active Directory domain are correct.

ACTIVE_DIRECTORY_USER_AUTH_FAILED

Description	This Authentication Failure message indicates that the user authentication has failed. You will see this message when the user or machine password is not found in Active Directory.
Resolution	Check if the Active Directory user account and credentials that are used to connect to the Active Directory domain are correct.

ACTIVE_DIRECTORY_USER_PASSWORD_EXPIRED

Description	This Authentication Failure message appears when the user's password has expired.
Resolution	If the Active Directory user account is valid, then reset the account in Active Directory. If the user account has expired, but if it is still needed, then renew it. If the user account has expired and is no longer valid, investigate the reasons for the attempts.

ACTIVE_DIRECTORY_USER_WRONG_PASSWORD

Description	This Authentication Failure message appears when the user has entered an incorrect password.
Resolution	Check if the Active Directory user account and credentials that are used to connect to the Active Directory domain are correct.

ACTIVE_DIRECTORY_USER_ACCOUNT_DISABLED

Description	This Authentication Failure message appears when the user account is disabled in Active Directory.
Resolution	If the Active Directory user account is valid, then reset the account in Active Directory. If the user account has expired, but if it is still needed, then renew it. If the user account has expired and is no longer valid, investigate the reasons for the attempts.

ACTIVE_DIRECTORY_USER_RESTRICTED_LOGON_HOURS

Description	This Authentication Failure message appears when the user logs in during restricted hours.
Resolution	If the user access is valid, then update the user access policy in Active Directory. If the user access is invalid (restricted at this time), then investigate the reasons for the attempts.

ACTIVE_DIRECTORY_USER_NON_COMPLIANT_PASSWORD

Description	This Authentication Failure message appears if the user has a password that is not compliant with the password policy.
Resolution	Reset the password in Active Directory such that it is compliant with the password policy in Active Directory.

ACTIVE_DIRECTORY_USER_UNKNOWN_DOMAIN

Description	This Authentication Failure message appears if Active Directory is unable to locate the specified domain.
Resolution	Check the configuration of Active Directory in the Administration ISE node user interface and the DNS[1] configuration in the Cisco ISE CLI.

1. DNS = domain name service

ACTIVE_DIRECTORY_USER_ACCOUNT_EXPIRED

Description	This message appears when the user account in Active Directory has expired.
Resolution	If the user account has expired, but is still needed, then renew the user account. If the user account has expired and is no longer valid, investigate the reasons for the attempts.

ACTIVE_DIRECTORY_USER_ACCOUNT_LOCKED_OUT

Description	This Authentication Failure message appears if the user account has been locked out.
Resolution	If the user attempts to log in with correct credentials, reset the user's password. Otherwise, investigate the attempts that caused the lock out.

ACTIVE_DIRECTORY_GROUP_RETRIEVAL_FAILED

Description	This Authentication Failure message appears if Active Directory is unable to retrieve the groups.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct.

ACTIVE_DIRECTORY_MACHINE_AUTHENTICATION_DISABLED

Description	This Authentication Failure message appears if machine authentication is not enabled in Active Directory.
Resolution	Enable Machine Authentication in Active Directory, if required.

ACTIVE_DIRECTORY_ATTRIBUTE_RETRIEVAL_FAILED

Description	This Authentication Failure message appears if Active Directory is unable to retrieve the attributes that you have specified.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct.

ACTIVE_DIRECTORY_PASSWORD_CHANGE_DISABLED

Description	This Authentication Failure message appears if the password change option is disabled in Active Directory.
Resolution	Enable Password Change in Active Directory, if required.

ACTIVE_DIRECTORY_USER_UNKNOWN

Description	This Invalid User message appears if the user information is not found in Active Directory.
Resolution	Check for the origin of the invalid attempts. If it is from a valid user, ensure that the user account is configured correctly in Active Directory.

ACTIVE_DIRECTORY_CONNECTION_FAILED

Description	This External Error message appears when Cisco ISE is unable to establish a connection with Active Directory.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct.

ACTIVE_DIRECTORY_BAD_PARAMETER

Description	This External Error message appears when you have provided an invalid input.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct.

ACTIVE_DIRECTORY_TIMEOUT

Description	This External Error message appears when a timeout event has occurred.
Resolution	Check if the Active Directory configuration in the Administration ISE node user interface is correct

Configure NADs for ISE Monitoring

To help troubleshoot failures with endpoint authentication and authorization, network access devices (NADs) can be configured to send syslog messages to the ISE Monitoring node. The logs can be correlated to authentication and authorization events and will be displayed in the details of the RADIUS authentication logs.

Note Sending syslog from NADs to ISE should be used for troubleshooting purposes only as this additional logging increases the load on the Monitoring node. Logging should only be enabled on specific NADs where endpoint is connected and should be disabled when the troubleshooting session is completed. If possible, it is recommended to filter the logs sent to ISE to those listed in Syslog Messages Collected, page D-33.

To enable a switch in your network to send syslog messages for ISE troubleshooting purposes, use the following commands.

```
epm logging
logging monitor informational
logging origin-id ip
logging source-interface <interface_id>
logging host <syslog_server_IP_address_x> transport udp port 20514
```

Note The origin-id ip address should be set to match source-interface IP address. The interface_id is the interface that will send syslog messages. Syslog messages will be sourced from the IP address configured for this interface. The syslog_server_IP_address should be the Primary MnT node.

Syslog Messages Collected

The following NAD syslog messages are collected:

AP-6-AUTH_PROXY_AUDIT_START

AP-6-AUTH_PROXY_AUDIT_STOP

AP-1-AUTH_PROXY_DOS_ATTACK

AP-1-AUTH_PROXY_RETRIES_EXCEEDED

AP-1-AUTH_PROXY_FALLBACK_REQ

AP-1-AUTH_PROXY_AAA_DOWN

AUTHMGR-5-MACMOVE

AUTHMGR-5-MACREPLACE

AUTHMGR-5-START/SUCCESS/FAIL

AUTHMGR-SP-5-VLANASSIGN/VLANASSIGNERR

DOT1X-5-SUCCESS/FAIL

DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND

EPM-6-POLICY_REQ

EPM-6-POLICY_APP_SUCCESS/FAILURE

EPM-6-IPEVENT:

MAB-5-SUCCESS/FAIL

MKA-5-SESSION_START

MKA-5-SESSION_STOP

MKA-5-SESSION_REAUTH

MKA-5-SESSION_UNSECURED

MKA-5-SESSION_SECURED

MKA-5-KEEPALIVE_TIMEOUT

RADIUS-4-RADIUS_DEAD

Troubleshooting APIs

You can use the following troubleshooting APIs to query information from Cisco ISE that could aid in general troubleshooting processes.

- **Get Version and Type of Node (Version)**
  https://{hostname}/ise/mnt/api/Version
- **Get Failure Reasons Mapping (FailureReasons)**
  https://{hostname}/ise/mnt/api/FailureReasons
- **Get Session Authentication Status (AuthStatus)**
  https://{hostname}/ise/mnt/api/AuthStatus/MACAddress/{mac}/{seconds}/{number of records per MAC Address}/All
- **Get Session Accounting Status (AcctStatusTT)**
  https://{hostname}/ise/mnt/api/AcctStatusTT/MACAddress/{mac}/{seconds}

Active Session List/Count APIs

APIs to Get Active Session Count

- **Get Active Session Count in Session Directory (ActiveCount)**
  https://{mnt-node}/ise/mnt/api/Session/ActiveCount
- **Get Active Session Count in Session Directory Using Posture Service (PostureCount)**
  https://{mnt node}/ise/mnt/api/Session/PostureCount
- **Get Active Session Count in Session Directory Using Profiler Service (ProfilerCount)**
  https://{mnt node}/ise/mnt/api/Session/ProfilerCount

APIs to Get Active Session List

- **Get Active Session Key Information in Session Directory (ActiveList)**
  https://{mnt node}/ise/mnt/api/Session/ActiveList

- **Get Active Session Key Information in Session Directory Authenticated within a Specified Period of Time (AuthList)**
  https://{mnt node}/ise/mnt/api/Session/AuthList/{start time}/{end time}

For more information:

- For more information about using the troubleshooting APIs in this release, see the *Cisco Identity Services Engine API Reference Guide, Release 1.1*.

Note The *Cisco Identity Services Engine API Reference Guide, Release 1.1*, also provides information about the supported session management and CoA APIs.

Contacting the Cisco Technical Assistance Center

If you cannot locate the source and potential resolution for a problem in the above sections, contact a Cisco customer service representative for information on how to best proceed with resolving the issue. For Cisco Technical Assistance Center (TAC), see the *Cisco Information Packet* publication that is shipped with your appliance or visit the following website:

http://www.cisco.com/tac/

Before you contact Cisco TAC, make sure that you have the following information ready:

- The appliance chassis type and serial number.
- The maintenance agreement or warranty information (see the *Cisco Information Packet*).
- The name, type of software, and version or release number (if applicable).
- The date you received the new appliance.
- A brief description of the problem or condition you experienced, the steps you have taken to isolate or re-create the problem, and a description of any steps you took to resolve the problem.

Note Be sure to provide the customer service representative with any upgrade or maintenance information that was performed on the Cisco ISE 3300 Series appliance after your initial installation. For site log information, see the "Creating a Site Log" section in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.



GLOSSARY

0-9

802.1X Also known as dot1X, 802.1X is an IEEE standard for port-based network access control. Per this standard, the Extensible Authentication Protocol (EAP) protocol is used for communication between the client and the authenticator (switches, wireless access points).

802.1X-REV 802.1X-REV is a revision of the 802.1X standard that contains security encryption and secure key exchange, allowing secure communication between authenticated and authorized devices. The 802.1X-REV feature includes the 802.1AE MAC Security (MACSec) encryption as well as 802.1af MACSec Key Agreement (MKA) protocol.

A

AAA Combined authentication, authorization, and accounting processes that are found in a management framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information that is necessary to bill for services. These three processes are considered essential for effective network management and security. Typically, a server-based system in IP-based networking, AAA controls what computer resources users have access to, and manages and audits the activity of users over a network.

AAA client IP address An IP address of the AAA client, used to configure the AAA client in the Cisco Identity Services Engine (ISE) to interact with the network device. To represent multiple network devices, specify multiple IP addresses. Separate each IP address by pressing the **Enter** key.

AAA server A server program that manages user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers, as well as with databases and directories that contain user information. The current standard by which devices or applications communicate with a AAA server is the RADIUS.

access The capability to get to what you need. Data access is being able to get to (usually having permission to use) particular data on a computer.

access control Ensures that resources are only granted to those users who are entitled to them.

access control list (ACL) A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

access control service A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

access control system (ACS) An AAA server that performs authentication, authorization, and accounting to manage devices in a network.

access policies The policies that limit access to the Cisco ISE web interface by IP address, TCP port range, and Secure Socket Layer (SSL).

accounting The capability of ISE to record user sessions in a log file.

Active Directory Active Directory is a Microsoft implementation of LDAP directory services for use in Windows-based environments. Active Directory provides administrators with the means for assigning network wide policies, deploying programs to many computer systems concurrently, and applying critical updates to an entire organization. Active Directory stores information and settings related to an organization in a centralized and accessible database.

Administration Persona Administrative service running on ISE that allows you to administer and maintain ISE.

administrative operations A set of operations that you must perform to effectively deploy and manage the ISE servers in your network.

ADR Accessibility design requirements. Provides detail on how to design accessible products, websites, and documentation.

AES Advanced encryption standard. A Federal Information Processing Standard (FIPS) publication that specifies a cryptographic algorithm for use by U.S. government organizations to protect sensitive (unclassified) information. This standard specifies Rijndael as a FIPS-approved symmetric encryption algorithm that may be used by U.S. government organizations (and others) to protect sensitive information.

allowed protocols access service Allowed protocols access service is a configurable object that contains a set of protocols that Cisco ISE uses to communicate with the device that requests access to your network resources.

anchored overlay A stationary pop-up dialog that simplifies specifying multiple options for a particular function. An anchored overlay is typically linked to a specific user interface function-related element.

anonymous (LDAP) An LDAP session is described as anonymous if no user distinguished name or secret is supplied when initiating the session (sending the bind).

anti virus A software program that is designed to identify and remove a known or potential computer virus.

AP Access point. The hub of a wireless network. Wireless clients connect to the access point, and traffic between two clients must travel through the access point.

API Application programming interface. The specific methodology by which a programmer writing an application program may make requests of the operating system or another application.

applet Java programs; an application program that uses the client web browser to provide a user interface.

ARP Address resolution protocol. A protocol for mapping an IP address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

ARPANET Advanced Research Projects Agency Network. A pioneer packet-switched network that was built in the early 1970s under contract with the US government. It led to the development of the modern Internet, and was decommissioned in June 1990.

Asymmetric Key Exchange Asymmetric or public key cryptography is based on the concept of a key pair. Each half of the pair (one key) can encrypt information so that only the other half (the other key) can decrypt it. One part of the key pair, the private key, is known only by the designated owner; the other part, the public key, is published widely but is still associated with the owner.

attribute (LDAP) The data in an entry is contained in attribute-value pairs. Each attribute has a name (and sometimes a short form of the name) and belongs to an objectClass. The attributes characteristics are fully described by an ASN.1 definition. One or more objectClasses may be included in a Schema. Depending on the ASN.1 definition of the attribute, there can be more that one attribute-value pair of the same named attribute in an entry. One (or more) attribute (or attributes), the naming attribute, or RDN will always uniquely identify an entry.

auditing The information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

authenticated (LDAP) A session is described as authenticated if a user distinguished name and secret are supplied when initiating the session (sending the bind).

authentication The process of confirming the correctness of the claimed identity.

Authenticator (AT) A device that is already part of a trusted network.

authenticity The validity and conformance of the original information.

authorization The approval, permission, or empowerment for someone or something to do something.

authorization profile The basic "permissions container" for a RADIUS-based network access service. The authorization profile is where you define all permissions to be granted for a network access request. VLANs, ACLs, URL redirects, session timeout or reauthorization timers, or any other RADIUS attributes to be returned in a response are defined in the authorization profile.

Authorization Server (AS) AAA server, such as Cisco ISE that provides authentication and authorization services.

B

basic authentication The simplest web-based authentication scheme that works by sending the username and password with each request.

BIND Berkeley Internet Name Domain. An implementation of DNS. DNS is used for domain-name-to-IP-address resolution.

bind (LDAP) When connection is made to an LDAP server, the first operation of the sequence is called a bind. The bind operation sends the distinguished name of the entry that will be used for authentication and the password to be used. In the case of an anonymous bind, both values will be NULL.

block cipher Encrypts one block of data at a time.

bridge A product that connects a LAN to another LAN that uses the same protocol (for example, Ethernet or Token Ring).

broadcast To simultaneously send the same message to multiple recipients. One host to all hosts on network.

broadcast address An address that is used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

browser A client computer program that can retrieve and display information from servers on the World Wide Web.

C

CA Certificate authority. An authority in a network that issues and manages security credentials and public keys for message encryption and decryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information that is provided by the requestor of a digital certificate. If the RA verifies the information of the requestor, the CA can then issue a certificate.

CA signature A digital code that vouches for the authenticity of a digital certificate. The CA signature is provided by the certificate authority (CA) that issued the certificate.

cache A special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

certificate Digital representation of user or device attributes, including a public key, which is signed with an authoritative private key.

certificate authentication profile Certificate authentication profiles are identity sources that are used in certificate-based authentications to verify the authenticity of users.

certificate-based authentication The use of Secure Sockets Layer (SSL) and certificates to authenticate and encrypt HTTP traffic.

CGI Common gateway interface. This mechanism is used by HTTP servers (web servers) to pass parameters to executable scripts in order to generate responses dynamically.

CHAP Challenge-Handshake Authentication Protocol. A protocol that uses a challenge-response authentication mechanism where the response varies every challenge to prevent replay attacks.

CHAP is an authentication technique where after a link is established, a server sends a challenge to the requestor. The requestor responds with a value that is obtained by using a one-way hash function. The server checks the response by comparing it its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is usually terminated.

challenge-response A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.

checksum A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

cipher A cryptographic algorithm for encryption and decryption. The method is used to transform a readable message (called plaintext or cleartext) into an unreadable, scrambled, or hidden message (called ciphertext).

ciphertext The encrypted form of the message being sent. Ciphertext is data that has been encrypted. It is the output of the encryption process and can be transformed back into a readable form (plaintext) with the appropriate decryption key.

client A system entity that requests and uses a service that is provided by another system entity, called a server. In some cases, the server may itself be a client of some other server.

client/server Describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although the client/server idea can be used by programs within a single computer, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations.

CN Common name is one of the attributes listed in an LDAP directory entry.

CoA RADIUS Change of Authorization provides a mechanism to change the attributes of a session after it is authenticated. When there is a change in policy for a user or user group in AAA, you can send the RADIUS CoA packets from the AAA server such as Cisco ISE to reinitialize authentication and apply the new policies.

collision Occurs when multiple systems transmit simultaneously on the same wire.

community string A character string that is used to identify valid sources for Simple Network Management Protocol (SNMP) requests, and to limit the scope of accessible information. Ravlin units use a community string, such as a password, allowing only a limited set of management stations to access its MIB.

computer network A collection of host computers together with the subnetwork or internetwork through which they can exchange data.

confidentiality The need to ensure that information is disclosed only to those who are authorized to view it.

configuration management The process of establishing a known baseline condition and managing it.

cookie Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections.

corruption A threat action that undesirably alters system operation by adversely modifying system functions or data.

CoS Class of service. A way of managing traffic in a network by grouping similar types of traffic (for example, email, streaming video, voice, large document file transfer) and treating each type as a class with its own level of service priority.

countermeasure Reactive methods that is used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion prevention systems (IPSs) commonly employ countermeasures to prevent intruders form gaining further access to a computer network. Other countermeasures are patches, access control lists and malware filters.

covert channels The means by which information can be communicated between two parties in a covert fashion by using normal system operations. For example, by changing the amount of hard-drive space that is available on a file server can be used to communicate information.

CRC Cyclic redundancy check. Sometimes called cyclic redundancy code. A type of checksum algorithm that is not a cryptographic hash, but is used to implement data integrity service where accidental changes to data are expected.

CRL Certificate revocation list. A list of certificates (more accurately: their serial numbers) that have been revoked and are no longer valid, and should not be relied upon by any system user.

CRUD Create, read, update, and delete. The basic management operations that are performed on managed data.

cryptanalysis The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge that is needed to break or circumvent the protection that the system is designed to provide. In other words, to convert the cipher text to plaintext without knowing the key.

cryptographic algorithm or hash An algorithm that employs the science of cryptography, including encryption algorithms, cryptographic algorithm or hash, Digital Signature Algorithm (DSA), and key agreement algorithms.

cryptography Garbles a message in such a way that anyone who intercepts the message cannot understand it.

CSS Cascading style sheet. A web page that is derived from multiple sources with a defined order of precedence where the definitions of any style element conflict.

CSV Comma-separated value. This file format is a delimited data format that has fields separated by the comma character and records separated by new lines.

CUE Common user experience

cut-through A method of switching where only the header of a packet is read before it is forwarded to its destination.

D

daemon A program that is often started at the time when the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. Daemons are supported by many operating systems, even if the original UNIX term is not. Windows, for example, refers to daemons as system agents and services.

dashlet A subwindow on the Cisco ISE dashboard that contains unique, independent functions, and displays information using widgets, or small components that access data from outside the application.

datagram Request for Comment 1594 says, “a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.” The term has been generally replaced by the term “packet.” Datagrams or packets are the message units that the IP processes with and that the Internet transports. A datagram or packet needs to be self-contained without reliance on earlier exchanges because there is no connection of fixed duration between the two communicating points as there is, for example, in most voice telephone conversations. (This kind of protocol is referred to as connectionless.)

decapsulation The process of stripping off the headers of one layer and passing the rest of the packet up to the next, higher layer on the protocol stack.

decryption The process of transforming an encrypted message into its original plaintext.

deep-drill The ability to click a sparkline on the Cisco ISE dashboard to automatically display a granular report of that data.

denial of service The prevention of authorized access to a system resource, or the delaying of system operations and functions.

DES Data Encryption Standard. A widely used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

device administration Capability to control and audit the administration operations that are performed on network devices. The network device administrator role has full access to perform the administrative operations on network devices.

dictionaries A store to configure attributes of the RADIUS protocol, internal users, and internal hosts.

dictionary attack An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words, compared to a brute force attack that tries all possible combinations.

Diffie-Hellman A key agreement algorithm that was published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

Digest Authentication Allows a web client to compute MD5 hashes of the password to prove it has the password.

digital certificate An electronic “credit card” that establishes your credentials when doing business or other transactions on the web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the public key of the certificate holder (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

digital envelope An encrypted message with the encrypted session key.

digital signature A hash of a message that uniquely identifies the sender of the message and proves the message has not changed since transmission.

disassembly The process of taking a binary program and deriving the source code from it.

disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.

DIT Directory information tree (also known as the naming context). The hierarchy of objects that make up the local directory structure. More than one DIT may be supported by an LDAP server. The Root DSE will provide this information.

DLL Dynamic link library. A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

DN Distinguished name. A DN is composed of a series of RDNs that uniquely describe the naming attributes on the path up the DIT from the required entry to the directory root. A DN is written left to right.

DNS Domain Name System. The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember “handle” for an Internet address.

domain A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Domain Name System (DNS) of the Internet, a domain is a name with which name server records are associated that describe subdomains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so on) for a group of users. The user only needs to log into the domain to gain access to the resources, which may be located on many different servers in the network.

domain name Locates an organization or other entity on the Internet. For example, the domain name “www.sans.org” locates an Internet address for “sans.org” at Internet point 199.0.0.2 and a particular host server named “www.” The “org” part of the domain name reflects the purpose of the organization or entity (in this example, “organization”) and is called the top-level domain name. The “sans” part of the domain name defines the organization or entity and, together with the top-level name, is called the second-level domain name.

DSA Digital Signature Algorithm. An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

DSA Directory System Agent X.500 term for any DAP- or LDAP-enabled directory service; for example, an LDAP server.

DSE DSA Specific Entry An entry in a local directory server.

DSS Digital Signature Standard. The U.S. government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

due diligence The requirement that organizations must develop and deploy a protection plan to prevent fraud and abuse, and a means to detect them if they occur.

dumpsec A security tool that dumps various information about the users, file system, registry, permissions, password policy, and services of a system.

E

EAP Extensible Authentication Protocol. A protocol for wireless networks that expands on Authentication methods used by the PPP (Point-to-Point Protocol), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and Public Key Encryption authentication.

EAP-FAST Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling. EAP-FAST is compliant with IEEE 802.1X and IEEE 802.11i. Like all EAP types, EAP-FAST can be used with WPA and WPA2 networks.

EAP-MD5 Extensible Authentication Protocol-Message Digest 5. An EAP security algorithm developed by RSA Security that uses a 128-bit generated number string, or hash, to verify the authenticity of a data communication.

EAP-TLS Extensible Authentication Protocol-Translation Layer Security. A high-security version of EAP that requires authentication from both the client and the server. If one of them fails to offer the appropriate authenticator, the connection is terminated. Used to create a secured connection for 802.1X by preinstalling a digital certificate on the client computer. EAP-TLS is the protocol that serves for mutual authentication and integrity-protected cipher suite negotiation and key exchange between a client and server. Both the client and the server use X.509 certificates to verify their identities to each other.

eavesdropping Listening to a private conversation which may reveal information which can provide access to a facility or network.

EditorAdmin A user role with privileges to edit all parts of the Cisco ISE user interface, with the exception of delete privileges for network resources.

egress Egress is the point at which a data packet leaves a trusted network, where the security group tag (SGT) is removed from the packet and the egress policy is applied.

egress filtering Filtering outbound traffic.

encapsulation The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

encryption Cryptographic transformation of data (called “plaintext”) into a form (called “cipher text”) that conceals the data's original meaning to prevent it from being known or used.

endpoint An endpoint is a network capable device connecting to your enterprise network that can use the resources on your network.

entry (LDAP) The name given to a stored object in a LDAP enabled directory. Each entry has one parent entry (object) and zero or more child entries (objects). The data content of an entry consist of one or more attributes one (or more) of which is (are) used as the naming attribute (more correctly the RDN) to uniquely identify this object in the DIT.

equality (LDAP) Equality defines the comparison rule of an attribute when used in a search filter that contains no wildcards, and both the content and length must be exactly the same. When wildcards are used, this is called a substring and the SUBSTR rule is used.

Ethernet The most widely-installed LAN technology. Specified in a standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Devices are connected to the cable and compete for access using a CSMA/CD protocol.

event An observable occurrence in a system or network.

exception action A single configurable action triggered if a set of conditions do not match.

Exponential Backoff Algorithm Used to adjust TCP timeout values on the fly so that network devices don't continue to timeout sending data over saturated links.

exposure A threat action whereby sensitive data is directly released to an unauthorized entity.

expression builder A pop-up dialog that simplifies creating expressions by allowing you to make selections from menus and other pop-up dialogs.

extended ACLs A more powerful form of standard ACLs on Cisco routers. They can make filtering decisions based on IP addresses (source or destination), Ports (source or destination), protocols, and whether a session is established.

external identity source External databases that ISE accesses to perform credential and authentication validations for internal and external users (as defined by you within a policy).

external user A user defined in an external identity source.

F

false rejects When an authentication system fails to recognize a valid user.

filter Used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

filtering router An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.

firewall A TCP/IP Fragmentation Attack that is possible because IP allows packets to be broken down into fragments for more efficient transport across various media. The TCP packet (and its header) are carried in the IP packet. In this attack the second fragment contains incorrect offset. When packet is reconstructed, the port number will be overwritten.

fragmentation The process of storing a data file in several “chunks” or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

frames Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that “frame” the data. (Some control frames contain no data.)

FTP File Transfer Protocol . A TCP/IP protocol specifying the transfer of text or binary files across the network.

full duplex A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.

fully qualified domain name A server name with a hostname followed by the full domain name.

G

gateway A network point that acts as an entrance to another network.

global system options Configuring EAP-TTLS, PEAP, and EAP-FAST run-time characteristics and generating EAP-FAST PAC.

guest user A guest user is the person who needs a guest user account to access the network temporarily.

H

hash functions Used to generate a one way “check sum” for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

header The extra information in a packet that is needed for the protocol stack to process the packet.

HelpDeskAdmin A user role with privileges for read-only the Cisco ISE Dashboard, as well as Alarms within Monitor and Report.

host Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

Host-Based ID Host-based intrusion detection systems use information from the operating system audit records to watch all operations occurring on the host that the intrusion detection software has been installed upon. These operations are then compared with a pre-defined security policy. This analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must be utilized by the intrusion detection system. Depending on the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

HTML Hypertext Markup Language. The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

HTTP Hypertext Transfer Protocol. The protocol in the Internet Protocol (IP) family used to transport hypertext documents across an internet.

HTTPS Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL. HTTPS is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL. HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP and an additional encryption/authentication layer between HTTP and TCP.

hub A network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub. The central device in a star network, whether wired or wireless. Wireless access points act as hubs in wireless networks.

hybrid attack Builds on the dictionary attack method by adding numerals and symbols to dictionary words.

hybrid encryption An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

I

I18N Internationalization and localization are means of adapting software for non-native environments, especially other nations and cultures. Internationalization is the adaptation of products for potential use virtually everywhere, while localization is the addition of special features for use in a specific locale.

identity Whom someone or what something is, for example, the name by which something is known.

IdentityAdmin A user role with privileges to add, update, and delete entries in the internal ISE identity stores, including internal users and hosts.

identity groups A logical entity that is associated with all types of users and hosts.

identity source A database such as internal users, AD, LDAP, and so on that Cisco ISE uses to obtain user information for authentication.

identity source sequence An object that contains a set of identity sources that Cisco ISE will look up for user information for authentication. Cisco ISE searches these identity sources in the order in which they are defined in this sequence.

IETF Internet Engineering Task Force . The body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership.

incremental backup A scheduled job that allows users to take smaller, periodic backups of the Monitoring & Report Viewer database.

ingress Ingress is the point at which a data packet encounters the first security group access (SGA)-capable device on its path to the destination, where it is tagged with a security group tag (SGT).

inline PEP Inline Policy Enforcement Point (IPEP) is a gatekeeping node that is positioned behind wireless LAN controllers (WLC) and virtual private network (VPN) concentrators on the network.

integrity The need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

internal identity sources A database that contains the internal user attributes and credential information used to authenticate internal users and endpoints.

internal user A user defined in the internal identity source.

Interrupt A signal that informs the OS that something has occurred.

intrusion detection A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Internet Protocol. The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP address A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP flood A denial of service attack that sends a host more echo request (“ping”) packets than the protocol implementation can handle.

IP forwarding An Operating System option that allows a host to act as a router. A system that has more than 1 network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP poofing The technique of supplying a false IP address.

IPsec Internet Protocol Security. A developing standard for security at the network or packet processing layer of network communication.

ISO International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

ISP Internet Service Provider. A business or organization that provides to consumers access to the Internet and related services. In the past, most ISPs were run by the phone companies.

J

Java An object oriented programming language developed by Sun Microsystems. The Java language was designed to be elegantly concise, allowing it to be portable across platforms and operating systems at both source and binary levels.

JRE Java Runtime Environment. A software bundle that allows a computer system to run a Java application.

K

Kerberos — A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.

key — In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.

L

Layer 2 Forwarding Protocol (L2F) — An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user.

Layer 2 Tunneling Protocol (L2TP) — An extension of the Point-to-Point Tunneling Protocol used by an Internet service provider to enable the operation of a virtual private network over the Internet.

LDAP client — LDAP client describes a piece of software that provides access to an LDAP sever. Most standard web browsers provide limited LDAP client capabilities using LDAP URLs. LDAP browsers and web interfaces are both very common examples of LDAP clients. List of Open Source Clients.

Lightweight Directory Access Protocol (LDAP) — LDAP is a networking application protocol for querying and modifying data using directory services running over TCP/IP The LDAP protocol is used to locate organizations, individuals, and other resources such as files and devices in a network, on the public Internet or on a corporate Intranet.

Local Operations (secondary servers only) — The operations performed to register or deregister a secondary server, or to replicate a secondary server and a request for a local mode from the Join a Distributed System page.

Log Configuration — A system that uses logging categories and maintenance parameters that enable you to configure and store the logs generated for accounting messages, AAA audit and diagnostics messages, system diagnostics messages, and administrative audit messages.

M

MAC Address — A physical Media Access Control address which is a numeric value or identifier assigned by the manufacturer that acts to uniquely identify a network device from every other device of this type.

matchingRule (LDAP) — The method by which an attribute is compared in a search operation. A matchingRule is an ASN.1 definition that usually contains an OID a name (for example, caseIgnoreMatch [OID = 2.5.13.2]), and the data type it operates on (for example, DirectoryString).

MD5 — A one way cryptographic hash function.

metric meter — A type of widget that provides an at-a-glance view of data depicting network activity. Sparklines and stack bars convey the number of instances that have occurred over a designated period of time, such as the last 60 minutes or 24 hours.

MIB (Management Information Base) A MIB is a formal description of a set of network objects that can be managed using Simple Network Management Protocol (SNMP).

monitoring and reporting ISE features that allow you to monitor the state and health of the network and its devices, and generate reports of various types.

MPPE Microsoft Point-to-Point Encryption A protocol for encrypting data across PPP (Point-to-Point Protocol) and Virtual Private Network links.

N

name space (LDAP) Term used to describe all DNs that lie in (or are contained within or bounded by) a given directory information tree (DIT). If the DIT root is dc=example,dc=com, then cn=people,dc=example,dc=com is said to lie in the name space but ou=people,dc=example,dc=net does not; it lies in the dc=example,dc=net name space.

naming attribute (LDAP) A unique identifier for each entry in the directory information tree (DIT). Also known as the Relative Distinguished Name (RDN).

naming context (LDAP) A a unique name space starting from (and including) the root Distinguished Name (DN). Also known as namingContext or directory information tree (DIT).

NAS (network access server) A single point of access to a remote resource. The NAS is meant to act as a gateway to guard access to a protected resource. This can be anything from a telephone network, to printers, to the Internet.

NetworkDeviceAdmin A user role with privileges to manage the Cisco ISE network device repository, including adding, updating, and deleting devices. These permissions provide the administrator solely with read and write access to network devices.

network device groups Network device groups (NDGs) are a logical grouping of network devices by location and type.

network resources A location where you define all network devices in the device repository that access the ISE network, including Network Device Groups (NDGs), network devices, AAA clients, and external policy servers.

O

Object selector A pop-up dialog with items you can choose for a specific function. An object selector is often linked to another dialog, to provide input for a selected option.

P

PAP (Password Authentication Protocol.) PAP is a simple authentication protocol used to authenticate a user to a remote access server or Internet service provider (ISP).

PasswordAdmin A user role with privileges to change the password for internal users, and is intended for administrators who manage administrator accounts. An administrator with these privileges can change the password for other administrators.

Policy Service Persona Policy Service is the runtime service running on ISE that evaluates requests and processes them.

PI (Programmatic Interface) The ISE PI is a programmatic interface that provides external applications the ability to communicate with ISE to configure and operate ISE. PI allows for performing the following operations on ISE objects: create, update, delete, and read.

policy condition Rule-based single conditions that are based on policies, which are sets of rules used to evaluate an access request and return a decision.

policy element Global, shared object that defines policy conditions (for example, time and date, or custom conditions based on user-selected attributes) and permissions (for example, authorization profiles). Policy elements are referenced when you create policy rules.

port setting You can configure ISE to authenticate using different LDAP servers, or different databases on the same LDAP server, by creating more than one LDAP instance with different IP addresses or port settings.

posture Checking a host that accesses a protected network resource for compliance.

PPP (Point-to-Point Protocol) PPP is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet Protocol (IP) and is designed to handle others. It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

PRA Periodic Reassessment is reporting to the Cisco ISE server by periodically checking hosts for compliance.

profiling You can match identities like endpoints for the purpose of classifying them based on a set of conditions.

protocol A protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols at each layer in the telecommunication exchange that both ends of the exchange must recognize and observe. Protocols are often described in an industry or international standard.

Proxy An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

Public Key

In Cryptography a publicKey is a value provided by some designated authority as an Encryption Key that, combined with a private key derived from the public key, can be used to effectively encrypt messages andDigital Signatures.

The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).

Public Key Infrastructure (PKI)

A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The Public Key infrastructure provides for a Digital Certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

Q

Quick View

A pop-up dialog that provides information that is relevant to the location in the user interface.

R

RADIUS Servers

Any third-party server that supports the RADIUS interface.

RDN (LDAP)

The Relative Distinguished Name (frequently but incorrectly written as Relatively Distinguished Name) is an X.500 terminology. The name given to an attribute(s) that is unique at its level in the hierarchy. RDNs may be single valued or multi-valued in which case two or more attributes are combined using '+' (plus) to create the RDN e.g. cn+uid. The term RDN is only meaningful when used as part of a DN to uniquely describe the attributes on the path UP the DIT from a selected entry (or search start location) to the directory root (or more correctly the Root DSE).

referral (LDAP)

An operation in which the LDAP server returns to an LDAP client the name (typically in the form of an LDAP URL) of another LDAP server that might be able to provide the information requested by the LDAP client.

Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

Remediation

An operation that a host undergoes to get authenticated to access a protected network.

ReportAdmin

A user role with privileges for generating and viewing reports and monitoring data, with read-only access to logs.

RFC (Request for Comments)

A series of memoranda that encompass new research, innovations, and methodologies applicable to Internet technologies.

Role A set of typical administrator tasks, each with an associated set of permissions. An administrator can have more than one predefined role, and a role can apply to multiple administrators.

root (LDAP) The root entry (a.k.a base, suffix) is one of many terms used to describe the topmost entry in a DIT. The Root DSE is a a kind of super root.

Root DSE (LDAP) Conceptually the top most entry in a LDAP hierarchy - think of it as a super root and normally invisible i.e. not accessed in normal operations. Sometimes confused with root or base or suffix. DSE stands for DSA Specific Entry and DSA in turn stands for Directory System Agent (any directory enabled service providing DAP or LDAP access). Information about the rootDSE may be obtained in OpenLDAP by querying the OpenLDAProoDSE classobject and will provide information about protocol versions supported, services supported and the naming-context(s) or DIT(s) supported.

rootdn (LDAP) The rootdn is a confusingly named directive in the slapd.conf file which defines a superuser which can bypass normal directory access rules.

RPM (RedHat Package Manager) An RPM is a downloadable software package that is installable on Linux distributions that use RPM as their package management format.

S

SAN (Subject Alternative Name) Extension within certificate information.

Schema (LDAP) A package of attributes and object classes that are sometimes (nominally) related. The schema(s) in which the object classes and attributes that the application will use (reference) are packaged are identified to the LDAP server so that it can read and parse all that wonderful ASN.1 stuff. In OpenLDAP this done using the slapd.conf file.

search (LDAP) An operation that is carried out by defining a base directory name (DN), a scope, and a search filter.

Secure Sockets Layer(SSL) A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. SSL is a cryptographic protocol which provides secure communications on the Internet for such things as web browsing, email, Internet faxing, and other data transfers. There are slight differences between SSL 3.0 and TLS 1.0, but the protocol remains substantially the same. The term “TLS” as used here applies to both protocols unless clarified by context.

SecurityAdmin A user role with privileges to create, update, and delete administrator accounts, to assign administrative roles, and change the password policy.

Security Group Access (SGA) Security Group Access (SGA) is a solution that builds secure networks by establishing clouds of trusted networks. The Cisco SGA solution was previously known as Cisco TrustSec (CTS) solution.

Security Policy A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

server A system entity that provides a service in response to requests from other system entities called clients.

service provisioning Service provisioning refers to the "preparation beforehand" of IT systems' materials or supplies required to carry out a specific activity. This includes the provisioning of digital services such as user accounts and access privileges on systems, networks and applications, as well as the provisioning of non-digital or "physical" resources such as cell phones and credit cards.

service selection policy A set of rules that determines which access policy applies to an incoming request.

Session A session is a virtual connection between two hosts by which network traffic is passed.

session (LDAP) A session occurs between a LDAP client and a server when the client sends a **bind** command. A session may be either anonymous or authenticated.

session conditions Custom conditions, and date and time conditions.

Session Key In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

SGA device Any device that supports the Cisco Security Group Access solution.

SLA (Service Level Agreement) A SLA is that part of a service contract in which a certain level of service is agreed upon. A SLA is a formal negotiated agreement between two parties. It is a contract that exists between customers and their service provider, or between service providers. It transcripts the common understanding about services, priorities, responsibilities, guarantee, etc. It then specifies the levels of availability, serviceability, performance, operation or other attributes of the service like billing.

SMS Short Message Service.

SMTP (Simple Mail Transfer Protocol) SMTP is an Internet standard for electronic mail (email) transmission across Internet Protocol (IP) networks.

SNMP (Simple Network Management Protocol) A TCP/IP network protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SOAP A lightweight XML-based protocol for exchange of information in a decentralized, distributed environment. SOAP consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses.

sparkline A type of widget on the Cisco ISE Dashboard where vertical lines show trends over time. The height of a sparkline is based on a percentage of the maximum number of instances over a designated period of time, such as the last 60 minutes or the last 24 hours. Clicking a sparkline generates a deep-drill report showing granular data for a function.

SPML (Service Provisioning Markup Language) SPML is the open standard protocol for the integration and interoperation of service provisioning requests.

sponsor group A group of sponsor users who are assigned with the same set of privileges.

sponsor user A sponsor user is the person who creates the guest user account. This person is often an employee of the organization that provides the network access. Sponsors can be specific individuals with certain job roles, or can be any employee who can authenticate against a corporate directory such as Microsoft Active Directory (AD).

SSH (Secure Shell) A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

SSL (Secure Sockets Layer) SSL is a cryptographic protocols that provide security for communications over networks.

stack bar A type of widget on the Cisco ISE Dashboard comprised of horizontal color segments representing the distribution of a parameter over time.

subtype (LDAP) LDAPv3 defines a number of subtypes at this time two have been defined binary (in RFC 2251) and lang (in RFC 2596). subtypes may be used when referencing an attribute and qualify e.g. cn;lang-en-us=smith would perform a search using US english. The subtype does not affect the encoding since UTF-8 (used for cn) allows for all language types. lang subtypes are case insensitive.

suffix (LDAP) Also known as root, base, is one of many terms used to describe the topmost entry in a DIT. The term is typically used because this entry is usually defined in the suffix parameter in a OpenLDAP's slapd.conf file. The Root DSE is a kind of super root. Suffix Naming.

SuperAdmin A user role with privileges across the entire system, including monitoring and troubleshooting. SuperAdmin permissions allow the administrator to create, read, update, delete, and execute (CRUDX) all the Cisco ISE resources.

support bundle Support bundle contains ISE log messages, which can be used to prepare diagnostic information for TAC.

system administration The role-based administrative functions performed by a group of administrators.

system administrators Administrators with different access privileges defined in the Cisco ISE GUI. They administer and manage ISE deployments in your network.

system configuration The role-based administrative functions performed by a group of administrators to configure system performance.

System Health Dashboard The Monitoring & Report Viewer Dashboard that provides information about the health status of associated ISE instances.

T

TCP/IP Transmission Control Protocol/Internet Protocol is the basic communication language or protocol of the Internet. TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

Time profile Assign different levels of access time to a guest account.

TrustSec solution Cisco TrustSec is an identity-based access control solution that secures networks and networked resources through policy-based access control, identity-aware networking, data integrity, and confidentiality services.

U

UDP User Datagram Protocol. A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP)

URL Uniform Resource Locator. The unique address for a file that is accessible on the Internet.

user attribute configuration An administrative task consisting of configuring an internal user's identity attributes.

user roles User roles are sets of permissions that determine the tasks a user is allowed to perform on the Cisco ISE network. Due to associated permissions, user roles can affect what appears in the ISE user interface.

V

ViewerAdmin A user role with privileges for read-only all parts of the Cisco ISE user interface, and read-only access to all network resources.

VPN Virtual private network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VSA Vendor-specific attribute. A proprietary property or characteristic not provided by the standard Remote Authentication Dial-In User Service (RADIUS) attribute set. VSAs are defined by vendors of remote access servers to customize RADIUS for their servers.

W

WCS Cisco Wireless Control System us a platform designed to help enterprises design, control and monitor Cisco wireless LANs. WCS is the industry leading platform for wireless LAN planning, configuration, and management.

Web server A Web server is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests).

Web service A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. The web server interface is described in a machine-processable format, WSDL. Other systems interact with the Web service, typically using HTTP with an XML serialization in conjunction with other Web-related standards.

WLC (Wireless Lan Controller) WLC is a device that assumes a central role in the Cisco Unified Wireless Network (CUWN). Traditional roles of access points, such as association or authentication of wireless clients, are done by the WLC.

WSDL (Web Services Description Language) WSDL is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically.

X

X.509 A standard for public key infrastructure. X.509 specifies, amongst other things, standard formats for public key certificates and a certification path validation algorithm.

XML (eXtensible Markup Language) XML is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

Y

Z



INDEX

Symbols

! formatting symbol A-27

& formatting symbol A-27

< formatting symbol A-27

> formatting symbol A-27

@ formatting symbol A-27

A

adding

- data filters 24-26

advanced 20-5

antispyware remediations 20-130

antivirus remediations 20-125

application condition 20-68

authentication policies

- allowed protocols
  - authentication 16-15
- conditions
  - compound 16-33
- description 16-1
- rule-based 16-5
  - configuring 16-29
- simple 16-4
  - configuring 16-26
- supported authentication types, protocols, and databases 16-2
- supported dictionary attributes 16-7
- terminology 16-3
- UI elements 16-30

authentication results

- viewing 16-41

B

base 20-5

C

case conversions A-27

cautions

- description ii-xxxi

changing

- chart subtypes 24-30

changing chart subtypes

- chart types 24-30

character placeholder A-27

charts

- overview 24-29

CoA 18-8

columns

- sorting data in 24-25

compliance 20-1

compound condition

- av and as 20-88, 20-94

conditions

- filtering data and 24-26

conversions A-27

creating

- data filters 24-26

Currency format option A-26

Custom format option A-26

D

data
- plotting relationships for 24-29
- sorting 24-14

data filters 24-26

data rows 24-17

data sets 24-29

date data types A-26

date expressions 24-22

date formats A-26

displaying
- detail rows 24-17

dynamically
- statically 4-15

E

EAP-FAST
- PAC options 16-18

endpoints
- attribute 18-52
- identities 18-2

exception actions 18-58

expressions
- calculating data and 24-22
- filtering data and 24-26

F

file condition 20-44
- types 20-44

file remediation 20-115

filter conditions 24-26

filters 24-26

Fixed format option A-26

G

General Date format option A-26

General Number format option A-26

guest port 21-28

guest SSL setting 21-28

H

hiding
- detail rows 24-17

HTML codes
- AUP form 21-57
- change password form 21-59
- login form 21-54
- self registration form 21-60

I

identities
- endpoints 18-2

identity groups 4-71
- blacklist 4-70
- profiled 4-70
- unknown 4-70

identity store sequences 5-51

L

languages, supported 21-35

language template
- add and edit 21-38, 21-47
- create single guest account 21-40
- delete 21-40, 21-49

description 21-34

email notification 21-41

guest notification 21-41

print notification 21-44

SMS notification 21-43

licenses

evaluation

base 20-5

link remediation 20-119

Long Date format option A-26

Long Time format option A-26

Lowercase format option A-26

M

MAC address 18-2

Medium Date format option A-26

Medium Time format option A-26

monitor

sponsor and guest 21-74

multiple guest portals 21-49

N

network scan action 18-63

note, description of ii-xxxii

number formats A-26

numeric data types A-26

numeric expressions 24-22

P

Percent format option A-26

periodic reassessment

PRA 20-12

permission

authorization profile 20-167

posture 20-1

posture condition 20-42

posture policy 20-33

posture requirement 20-155

Posture services 20-1

probe 18-12

profiling

policies 18-37

profiling services 18-1

program remediation

launching 20-135

R

RADIUS

server, defining 16-22

registry condition 20-55

types 20-55

relationships 24-29

remediation 20-112

Windows updates 20-142

remediations

wsus 20-148

rows 24-17

S

Scientific format option A-26

service condition 20-74

Short Date format option A-26
Short Time format option A-26
SMTP setting 21-27
sorting data 24-14
sponsor
  authenticate 21-29
  customize
    background 21-33
    banner 21-32
    login page 21-32
  group
    create and edit 21-21
    delete 21-22
sponsor group policy
  description 21-16
sponsor SSL setting 21-28
statically
  dynamically 4-16
string conversions A-27
string data types A-26
subtypes (charts) 24-30

T

text
  converting case A-27
text formats A-26
time data types A-26
time formats A-26
time profiles
  add and edit 21-71
  delete 21-72
  description 21-70
timesaver, description of ii-xxxii

U

Unformatted format option A-26
updates
  dynamic
    offline 20-22
Uppercase format option A-26

V

values
  sorting highest or lowest 24-25
viewing
  detail rows 24-17