



Cisco Identity Services Engine User Guide, Release 1.2

December 5, 2013

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Text Part Number: OL-26134-01

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 1.2
© 2013 Cisco Systems, Inc. All rights reserved.



Preface xxxv

Audience xxxv

Document Organization Map xxxvi

Document Conventions xxxvii

Documentation Updates xxxviii

Related Documentation xxxviii

Release-Specific Documents xxxix

Platform-Specific Documents xxxix

Notices xl

OpenSSL/Open SSL Project xl

License Issues xl

Obtaining Documentation and Submitting a Service Request xlii

PART 1

Introducing Cisco ISE

CHAPTER 1

Cisco ISE Features 1-1

Identity-Based Network Access 1-2

Support for Multiple Deployment Scenarios 1-2

Support for UCS Hardware 1-3

Basic User Authentication and Authorization 1-3

Policy Sets 1-4

FIPS 140-2 Implementation 1-4

Support for Common Access Card Functions 1-5

Client Posture Assessment 1-6

Network Access for Guests 1-6

Support for Personal Devices 1-6

Mobile Device Manager Interoperability with Cisco ISE 1-7

Wireless and VPN Traffic with Inline Posture Nodes 1-7

Profiled Endpoints on the Network 1-7

Support for SAnet Devices 1-7

Support for Installation on Multiple Hardware and VMware Platforms 1-8

CHAPTER 2

Navigating the Admin portal 2-1

- Admin Portal 2-1
 - Cisco ISE Dashboard 2-2
- Setup Assistant and Task Navigators 2-3
 - Setup Assistant 2-3
 - Cisco ISE Licensing Impact on Setup Assistant 2-3
 - Running the Setup Assistant 2-4
 - Setup Assistant Overwrites Previous Configurations 2-4
 - Identify Policy Requirements Page in Setup Assistant 2-4
 - Configure Network Access Service Page in Setup Assistant 2-5
 - Select Network Device Types Page in Setup Assistant 2-7
 - Review and Confirm Your Choices Page in Setup Assistant 2-7
 - Task Navigators 2-8
- Filtering Data on Listing Pages 2-8
 - Data Filters in Listing Pages 2-8
 - Customizing the Displayed Field Attributes 2-9
 - Filtering Data by Field Attributes Using the Quick Filter 2-9
 - Filtering Data by Conditions Using the Advanced Filter 2-9
 - Creating Custom Filters 2-10
- Cisco ISE Internationalization and Localization 2-10
 - Supported Languages 2-10
 - End-User Web Portal Localization 2-11
 - Support for UTF-8 Character Data Entry 2-11
 - UTF-8 Credential Authentication 2-12
 - UTF-8 Policies and Posture Assessment 2-12
 - Cisco NAC and MAC Agent UTF-8 Support 2-12
 - UTF-8 Support for Messages Sent to Supplicant 2-12
 - Reports and Alerts UTF-8 Support 2-13
 - UTF-8 Character Support in the Portals 2-13
 - UTF-8 Support Outside the User Interface 2-15
 - Support for Importing and Exporting UTF-8 Values 2-15
 - UTF-8 Support on REST 2-15
 - UTF-8 Support for Identity Stores Authorization Data 2-16
 - Admin Features Limited by Role-Based Access Control Policies 2-16

PART 2

Deploying Cisco ISE Nodes

CHAPTER 3

Setting Up Cisco ISE in a Distributed Environment 3-1

- Cisco ISE Deployment Terminology 3-1

Personas in Distributed Cisco ISE Deployments	3-2
Administration Node	3-2
High Availability in Administration Nodes	3-3
Policy Service Node	3-3
High Availability in Policy Service Nodes	3-3
Session Failover in Policy Service Nodes	3-4
Machine Access Restriction in Policy Service Nodes	3-4
Number of Nodes in a Policy Service Node Group	3-4
Monitoring Node	3-5
Automatic Failover in Monitoring Nodes	3-5
Inline Posture Node	3-6
Inline Posture Node Installation	3-7
Cisco ISE Distributed Deployment	3-7
Cisco ISE Deployment Setup	3-8
Data Replication from Primary to Secondary ISE Nodes	3-8
Cisco ISE Node Deregistration	3-8
Automatic Restart of the Cisco ISE Application Server	3-9
Guidelines for Setting Up a Distributed Deployment	3-9
Menu Options Available on Primary and Secondary Nodes	3-10
Configuring a Cisco ISE Node	3-11
Configuring a Primary Administration Node	3-12
Registering a Secondary Cisco ISE Node	3-12
Registering an Inline Posture Node	3-14
Viewing Nodes in a Deployment	3-15
Synchronizing Primary and Secondary Cisco ISE Nodes	3-15
Creating a Policy Service Node Group	3-16
Changing Node Personas and Services	3-17
Promoting Secondary Administration Node To Primary	3-17
Configuring Monitoring Nodes for Automatic Failover	3-18
Removing a Node from Deployment	3-19
Changing the Hostname or IP Address of a Standalone Cisco ISE Node	3-19
Replacing the Cisco ISE Appliance Hardware	3-20

CHAPTER 4

Setting Up Inline Posture 4-1

Role of Inline Posture Node in a Cisco ISE Deployment	4-1
Inline Posture Policy Enforcement	4-2
Inline Posture Policy Enforcement Flow	4-2
Trusted and Untrusted Interfaces	4-4

Dedicated Nodes Required for Inline Posture	4-4
Standalone Inline Posture Node in a Cisco ISE Deployment	4-4
Inline Posture High Availability	4-4
Automatic Failover in Inline Posture Nodes	4-5
Inline Posture Operating Modes	4-6
Inline Posture Routed Mode	4-6
Inline Posture Bridged Mode	4-7
Inline Posture Maintenance Mode	4-8
Inline Posture High Availability in Routed and Bridged Modes	4-8
Best Practices for Inline Posture Deployment	4-9
Inline Posture Node Guidelines	4-11
Inline Posture Node Authorization	4-12
Deploying an Inline Posture Node	4-13
Configuring an Inline Posture Node	4-13
Creating Inline Posture Downloadable Access Control Lists	4-16
Creating Inline Posture Node Profiles	4-17
Creating an Inline Posture Authorization Policy	4-18
Configuring a High-Availability Pair	4-19
Synchronizing an Inline Posture Node	4-20
Configuring Inline Posture Node as RADIUS Client in Administration Node	4-20
Removing an Inline Posture Node from Deployment	4-21
Health of an Inline Posture Node	4-22
Remote Access VPN Use Case	4-22
Configuring an Inline Posture Node with a VPN Device	4-23
Collecting Inline Posture Node Logs	4-24
Kclick process in Inline Posture Node	4-24

PART 4

Setting Up Cisco ISE Management Access

CHAPTER 5

Administering Cisco ISE 5-1

Logging in to Cisco ISE	5-1
Administrator Login Browser Support	5-2
Administrator Lockout Following Failed Login Attempts	5-2
Specifying Proxy Settings in Cisco ISE	5-2
Ports Used by the Admin Portal	5-3
Specifying System Time and NTP Server Settings	5-3
Changing the System Time Zone	5-4

Configuring the SMTP Server to Support Notifications	5-5
Installing a Software Patch	5-5
Cisco ISE Software Patches	5-6
Software Patch Installation Guidelines	5-6
Rolling Back Software Patches	5-7
Software Patch Rollback Guidelines	5-8
Viewing Patch Install and Rollback Changes	5-8
Enabling FIPS Mode in Cisco ISE	5-8
FIPS Mode Support	5-9
FIPS Mode Operational Parameters	5-9
Cisco NAC Agent Requirements when FIPS Mode is Enabled	5-10
Configuring Cisco ISE for Administrator CAC Authentication	5-10
Supported Common Access Card Standards	5-12
Common Access Card Operation in Cisco ISE	5-12
Securing SSH Key Exchange Using Diffie-Hellman Algorithm	5-13
Configuring Cisco ISE to Send Secure Syslog for Common Criteria Compliance	5-13
Configuring Secure Syslog Remote Logging Target	5-13
Enabling Logging Categories to Send Auditable Events to the Secure Syslog Target	5-14
Disabling the TCP Syslog and UDP Syslog Collectors	5-15

CHAPTER 6

Managing Administrators and Admin Access Policies 6-1

Cisco ISE Administrators	6-1
Privileges of a CLI Administrator Vs. a Web-Based Administrator	6-2
Creating a New Cisco ISE Administrator	6-2
Cisco ISE Administrator Groups	6-3
Creating Admin Groups	6-6
Administrative Access to Cisco ISE	6-7
Role-Based Access Control in Cisco ISE	6-8
Role-Based Permissions	6-8
RBAC Policies	6-8
Default Menu Access Permissions	6-8
Configuring Menu Access Permissions	6-10
Default Data Access Permissions	6-10
Configuring Data Access Permissions	6-11
Configuring Admin Access Policies	6-12
Administrator Access Settings	6-12
Configuring the Maximum Number of Concurrent Administrative Sessions and Login Banners	6-13
Allowing Administrative Access to Cisco ISE from Select IP Addresses	6-13

Configuring a Password Policy for Administrator Accounts	6-14
Configuring Session Timeout for Administrators	6-15
Terminating an Active Administrative Session	6-15
Changing Administrator Name	6-16
Administrative Access to Cisco ISE Using an External Identity Store	6-16
External Authentication and Authorization	6-17
Configuring a Password-Based Authentication Using an External Identity Store	6-17
Creating an External Administrator Group	6-18
Configuring Menu Access and Data Access Permissions for the External Administrator Group	6-18
Creating an RBAC Policy for External Administrator Authentication	6-19
Configuring Admin Access Using an External Identity Store for Authentication with Internal Authorization	6-19
External Authentication Process Flow	6-20

CHAPTER 7

Cisco ISE Licenses 7-1

Cisco ISE Licensing	7-1
90-Day Evaluation License	7-2
Base License	7-3
Advanced License	7-3
Wireless and Wireless Upgrade Licenses	7-4
Obtaining a Cisco ISE License from Cisco.com	7-4
Determining Your Hardware ID Using the CLI	7-5
Determining Your Hardware ID Using the Admin Portal	7-5
Adding or Upgrading a License	7-5
Removing a License	7-6

CHAPTER 8

Managing Certificates 8-1

HTTPS Communication Using the Cisco ISE Certificate	8-1
EAP Communication Using the Cisco ISE Certificate	8-2
Certificates Enable Cisco ISE to Provide Secure Access	8-2
Enabling PKI in Cisco ISE	8-3
Local Certificates	8-4
Wildcard Certificates	8-4
Wildcard Certificates for HTTPS and EAP Communication	8-5
Wildcard Certificate Support in Cisco ISE 1.2	8-6
Fully Qualified Domain Name in URL Redirection	8-6
Advantages of Using Wildcard Certificates	8-7
Disadvantages of Using Wildcard Certificates	8-7

Wildcard Certificate Compatibility	8-8
Creating a Wildcard Certificate	8-8
Installing Wildcard Certificates in Cisco ISE	8-10
Creating a Certificate Signing Request for Wildcard Certificates	8-10
Exporting the Certificate Signing Request	8-11
Submitting the CSR to a Certificate Authority	8-11
Importing the Root Certificates to the Certificate Store	8-12
Binding the CSR With the New Public Certificate	8-13
Exporting the CA-Signed Certificate and Private Key	8-13
Importing the CA-Signed Certificate to the Policy Service Nodes	8-13
Installing a CA-Signed Certificate in Cisco ISE	8-13
Viewing Local Certificates	8-15
Adding a Local Certificate	8-16
Importing a Local Certificate	8-16
Generating a Self-Signed Certificate	8-18
Generating a Certificate Signing Request	8-19
Binding a CA-Signed Certificate	8-20
Editing a Local Certificate	8-21
Exporting a Local Certificate	8-22
Certificate Signing Requests	8-23
Exporting Certificate Signing Requests	8-23
Certificate Store	8-24
Expiration of X.509 Certificates	8-25
CA Certificate Naming Constraint	8-25
Viewing Certificate Store Certificates	8-27
Changing the Status of a Certificate in Certificate Store	8-27
Adding a Certificate to Certificate Store	8-27
Editing a Certificate Store Certificate	8-28
Exporting a Certificate from the Certificate Store	8-28
Importing Certificate Chains	8-28
Installation of CA Certificates for Cisco ISE Inter-node Communication	8-29
Importing a CA-Signed Certificate from a Secondary Node into the Primary Node's CTL	8-29
Importing a Self-Signed Certificate from a Secondary Node into the CTL of the Primary Node	8-30
Simple Certificate Enrollment Protocol Profiles	8-30
Adding Simple Certificate Enrollment Protocol Profiles	8-30
OCSP Services	8-31
OCSP Certificate Status Values	8-32
OCSP High Availability	8-32

OCSP Failures	8-32
Adding OCSP Services	8-33
OCSP Statistics Counters	8-34
Monitoring OCSP	8-35

CHAPTER 9

Managing Network Devices 9-1

Network Devices Definitions in Cisco ISE	9-1
Default Network Device Definition in Cisco ISE	9-2
Creating a Network Device Definition in Cisco ISE	9-3
Importing Network Devices into Cisco ISE	9-4
Exporting Network Devices from Cisco ISE	9-4
Network Device Groups	9-5
Network Device Attributes Used By Cisco ISE in Policy Evaluation	9-5
Importing Network Device Groups in to Cisco ISE	9-6
Exporting Network Device Groups from Cisco ISE	9-6
Import Templates in Cisco ISE	9-7
Network Devices Import Template Format	9-7
Network Device Groups Import Template Format	9-10
Mobile Device Manager Interoperability with Cisco ISE	9-11
Supported MDM Use Cases	9-12
Supported MDM Servers	9-13
Ports Used by the MDM Server	9-13
MDM Dictionary Attributes	9-14
MDM Integration Process Flow	9-14
Setting Up MDM Servers With Cisco ISE	9-15
Importing MDM Server Certificate into Cisco ISE	9-15
Creating Mobile Device Manager Definitions	9-16
Configuring an Authorization Profile for Redirecting Nonregistered Devices	9-16
Configuring Authorization Policy Rules for the MDM Use Cases	9-17
Wiping or Locking a Device	9-18
Viewing Mobile Device Manager Reports	9-18
Viewing Mobile Device Manager Logs	9-19

CHAPTER 10

Managing Resources 10-1

Dictionaries and Dictionary Attributes	10-1
System Defined Dictionaries and Dictionary Attributes	10-1
Displaying System Dictionaries and Dictionary Attributes	10-2
User-Defined Dictionaries and Dictionary Attributes	10-2

Creating User-Defined Dictionaries	10-2
Creating User Defined Dictionary Attributes	10-3
RADIUS-Vendor Dictionaries	10-3
Creating RADIUS Vendor Dictionaries	10-4
Creating RADIUS-Vendor Dictionary Attributes	10-4

CHAPTER 11

Logging 11-1

Cisco ISE Logging Mechanism	11-1
Configuring Local Log Purge Settings	11-2
Cisco ISE System Logs	11-2
Local Store Syslog Message Format	11-2
Configuring Remote Syslog Collection Locations	11-4
Remote Syslog Message Format	11-4
Cisco ISE Message Codes	11-6
Setting Severity Levels for Message Codes	11-6
Cisco ISE Message Catalogs	11-7
Debug Log Configuration Options	11-7
Configuring Debug Log Severity Levels	11-7
Collection Filters	11-8
Configuring Collection Filters	11-8

CHAPTER 12

Managing Backup and Restore Operations 12-1

Backup Data Type	12-1
Backup and Restore Repositories	12-2
Creating Repositories	12-2
On-Demand and Scheduled Backups	12-3
Performing an On-Demand Backup	12-4
Scheduling a Backup	12-5
Performing a Backup from the CLI	12-6
Backup History	12-6
Backup Failures	12-6
Cisco ISE Restore Operation	12-6
Data Restoration Guidelines	12-7
Restoration of Configuration or Monitoring Backup from the CLI	12-8
Restoring Configuration Backups from the GUI	12-10
Restoration of Monitoring Database	12-10
Restoring a Monitoring Backup in a Standalone Environment	12-10
Restoring a Monitoring Backup with Administration and Monitor Personas	12-11

Restoring a Monitoring Backup with a Monitoring Persona	12-12
Restore History	12-12
Synchronizing Primary and Secondary Nodes in a Distributed Environment	12-13
Recovery of Lost Nodes in Standalone and Distributed Deployments	12-14
Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment	12-14
Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment	12-15
Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment	12-15
Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment	12-16
Configuration Rollback	12-16
Recovery of Primary Node in Case of Failure in a Distributed Deployment	12-17
Recovery of Secondary Node in Case of Failure in a Distributed Deployment	12-17

CHAPTER 13

Setting Up Endpoint Protection Service 13-1

Configuring Endpoint Protection Service	13-1
Creating Authorization Profiles for Network Access through EPS	13-2
Creating Exception Policies for Network Access through EPS	13-2
Configuring Network Access Settings	13-3
EPS Operations Fail when IP Address or MAC Address is not Found	13-3
Externally Authenticated Administrator Cannot Perform EPS Operations	13-4
Endpoint Protection Service	13-4
EPS Quarantine and Unquarantine Flow	13-5
EPS NAS Port Shutdown Flow	13-5

PART 4

Managing Users and End-User Portals

CHAPTER 14

Managing Users and External Identity Sources 14-1

Cisco ISE Users	14-1
User Identity	14-2
User Groups	14-2
User Identity Groups	14-2
Default User Identity Groups	14-2
User Role	14-2
User Account Custom Attributes and Password Policies	14-2
Custom User Attributes	14-3
User Password Policy Settings	14-3
Adding Users	14-3
Exporting Cisco ISE User Data	14-4

Importing Cisco ISE User Data	14-4
Creating a User Identity Group	14-5
Exporting User Identity Groups	14-5
Importing User Identity Groups	14-6
Identity Sources	14-6
Internal Identity Sources	14-7
External Identity Sources	14-7
Certificate Authentication Profiles	14-8
Adding a Certificate Authentication Profile	14-8
Active Directory as an External Identity Source	14-9
User and Machine Authentication in Active Directory	14-9
Active Directory Supported Authentication Protocols and Features	14-9
Active Directory Attribute and Group Retrieval for Use in Authorization Policies	14-10
Active Directory Certificate Retrieval for Certificate-Based Authentication	14-10
Active Directory User Authentication Process Flow	14-10
Support for Active Directory Multidomain Forests	14-11
Guidelines for Setting Up Active Directory as an External Identity Source	14-11
Configuring Active Directory as an External Identity Source	14-12
Connecting to the Active Directory Domain	14-13
Enabling Password Changes, Machine Authentications, and Machine Access Restrictions	14-13
Configuring Active Directory User Groups	14-14
Configuring Active Directory User Attributes	14-14
Leaving the Active Directory Domain	14-15
Deleting Active Directory Configurations	14-16
Enabling Active Directory Debug Logs	14-16
Obtaining Active Directory Log File for Troubleshooting	14-17
Supplemental Information for Setting Up Cisco ISE with Active Directory	14-17
Configuring Group Policies in Active Directory	14-17
Configuring Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory	14-18
AnyConnect Agent for Machine Authentication	14-19
LDAP	14-19
LDAP Directory Service	14-19
Multiple LDAP Instances	14-20
LDAP Failover	14-20
LDAP Connection Management	14-20
LDAP User Authentication	14-21
LDAP Group and Attribute Retrieval for Use in Authorization Policies	14-21
LDAP Group Membership Information Retrieval	14-22

LDAP Attributes Retrieval	14-22
LDAP Certificate Retrieval	14-23
Errors Returned by the LDAP Server	14-23
LDAP User Lookup	14-24
LDAP MAC Address Lookup	14-24
Adding LDAP Identity Sources	14-24
Configuring Primary and Secondary LDAP Servers	14-25
Enabling Cisco ISE to Obtain Attributes from the LDAP Server	14-25
Retrieving Group Membership Details from the LDAP Server	14-26
Retrieving User Attributes From the LDAP Server	14-26
RADIUS Token Identity Sources	14-27
RADIUS Token Server Supported Authentication Protocols	14-27
Ports Used By the RADIUS Token Servers for Communication	14-27
RADIUS Shared Secret	14-28
Failover in RADIUS Token Servers	14-28
Configurable Password Prompt in RADIUS Token Servers	14-28
RADIUS Token Server User Authentication	14-28
User Attribute Cache in RADIUS Token Servers	14-29
RADIUS Identity Source in Identity Sequence	14-29
RADIUS Server Returns the Same Message for All Errors	14-29
Safeword Server Supports Special Username Format	14-30
Authentication Request and Response in RADIUS Token Servers	14-30
Adding a RADIUS Token Server	14-31
Deleting a RADIUS Token Server	14-32
RSA Identity Sources	14-32
Cisco ISE and RSA SecurID Server Integration	14-33
RSA Configuration in Cisco ISE	14-33
RSA Agent Authentication Against the RSA SecurID Server	14-33
RSA Identity Sources in a Distributed Cisco ISE Environment	14-33
RSA Server Updates in a Cisco ISE Deployment	14-34
Override Automatic RSA Routing	14-34
RSA Node Secret Reset	14-34
RSA Automatic Availability Reset	14-34
Adding RSA Identity Sources	14-35
Importing the RSA Configuration File	14-35
Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files	14-35
Configuring Authentication Control Options for RSA Identity Source	14-36
Configuring RSA Prompts	14-37
Configuring RSA Messages	14-37

Identity Source Sequences	14-38
Creating Identity Source Sequences	14-38
Deleting Identity Source Sequences	14-39
Identity Source Details in Reports	14-39
Authentications Dashlet	14-40
Identity Source Reports	14-40

CHAPTER 15

Setting Up and Customizing End-User Web Portals	15-1
Available End-User Portals	15-1
End-User Portals in Distributed Environment	15-1
Enabling Policy Services for End-User Portals	15-2
Specifying Ports and Ethernet Interfaces for End-User Portals	15-2
Tips for Assigning Ports and Ethernet Interfaces	15-3
Specifying the Fully Qualified Domain Name for Sponsor and My Devices Portals	15-3
Customizing the Portal Language, Text, and Error Messages	15-4
Adding a Custom Language Template	15-4
Customizing Portal UI Fields and Error Messages	15-5
Customizing the Web Portal Images and Color Scheme	15-5
Displaying Banner Messages to Users When Logging In or Out of Portals	15-6
Enabling Banner Messages	15-6
Customizing the Sponsor Portal Banner Messages	15-6
Customizing the My Devices Portal Banner Messages	15-7
Customizing the Guest Portal Login Banner Message	15-7

CHAPTER 16

Supporting Authorized Network Access for Guests	16-1
Cisco ISE Guest Services	16-1
Guest Services End-User Portals	16-1
Sponsor Portal	16-2
Guest Portal	16-2
Support for Multiple Guest Portals	16-2
Mobile Guest Portal	16-2
Device Registration Web Authentication Portal	16-3
Client Provisioning Portal	16-3
Managing Sponsor and Guest Accounts	16-3
Guest Accounts	16-3
Guest Role and Identity Groups	16-3
Configuring Guest Roles	16-4
Sponsor Accounts and Identity Groups	16-4

Sponsor Groups	16-5
Creating Sponsor Groups	16-5
Sponsor Group Policies	16-6
Creating a Sponsor Group Policy	16-6
Mapping Active Directory Groups to Sponsor Groups	16-7
Configuring the Sponsor Portal	16-8
Sponsor Identity Source Sequence	16-8
Specifying the Identity Source Sequence for Sponsors	16-8
Customizing Guest Notifications	16-9
Customizing E-mail Notifications	16-9
Customizing SMS Text Message Notifications	16-9
Customizing Print Notifications	16-10
Configuring the Guest Portal	16-10
Adding a New Guest Portal	16-10
Providing a Mobile-Optimized Guest Portal	16-11
Customized Guest Portal	16-12
HTML Pages Required for Custom Guest Portals	16-12
Sequence of Customized HTML Pages Used by Guest Portal	16-13
Creating Custom HTML Files for Guest Portal	16-13
Uploading HTML Files for Guest Portal	16-14
Mapping HTML Files to Guest Portal Pages	16-15
Configuring the Guest Username and Password Policies	16-15
Configuring the Guest Username Policy Based on Names or E-mail Accounts	16-15
Configuring the Username Policy for Random Guest Accounts	16-16
Configuring the Guest Password Policy	16-16
Setting the Guest Password Expiration Time	16-16
Requiring Guests to Change Password	16-17
Specifying the Maximum Failed Login Attempts	16-17
Defining Guest Features	16-17
Specifying the Required Data for Guest Accounts	16-18
Limiting the Number of Supported Devices per Guest	16-18
Restricting Guests to One Active Network Session	16-18
Requiring an Acceptable Use Policy for Guests	16-19
Customizing the Acceptable Use Policy for Guests	16-19
Creating New Guest Time Profiles	16-20
Default Guest Time Profiles	16-20
Enabling Posture for Guest Users	16-21
Specifying the Identity Source Sequence for Guests	16-21
Allowing Guest Users to Create Own Accounts and Add Devices	16-22
Allowing Guests to Create Accounts	16-22

Allowing Guests to Add Devices	16-22
Setting the Guest Role for Self Registration	16-23
Setting the Time Profile for Self Registration	16-23
Monitoring Sponsor and Guest Activity	16-23
Suspended and Expired Guest Accounts	16-24
Purging Expired Guest Accounts	16-24
Metric Meter	16-24
Guest Activity Report	16-25
Guest Accounting Report	16-25
Guest Sponsor Summary	16-25
Audit Logging for Guest and Sponsor Portals	16-26
Guest Deployment Scenarios	16-26
NAD with Central WebAuth Process Flow	16-26
Wireless LAN Controller with Local WebAuth	16-27
Wired NAD with Local WebAuth	16-28
IP Address and Port Values Required for the Login.html Page	16-29
HTTPS Server Enabled on the NAD	16-29
Support for Customized Authentication Proxy Web Pages on the NAD	16-29
Configuring Web Authentication on the NAD	16-29
Device Registration WebAuth	16-30
Device Registration Web Authentication Process	16-31
Creating the Device Registration WebAuth Guest Portal	16-31
Creating a DRW Authorization Profile	16-32
Creating a DRW Authorization Policy Rule	16-32

CHAPTER 17

Supporting Personal Devices 17-1

Personal Devices on a Corporate Network	17-1
Personal Devices Portals	17-1
Self-Provisioning Portal	17-2
My Devices Portal	17-2
Blacklist Portal	17-2
Employee Accounts	17-3
Supporting Device Registration Using Native Supplicants	17-3
Operating Systems Supported by Native Supplicants	17-3
Allowing Employees to Register Personal Devices Using Native Supplicants	17-3
Supporting the My Devices Portal	17-4
Specifying the Identity Store Sequence Used for Employee Authentication	17-4
Enabling the My Devices Portal	17-4
Implementing an Acceptable Use Policy for Employees	17-5

Customizing the Acceptable Use Policy for Employees	17-5
Requiring an Acceptable Use Policy for Employees	17-5
Limiting the Number of Personal Devices Registered by Employees	17-6
Customizing Help Desk Contact Details	17-6
Managing Personal Devices Added by Employees	17-6
Displaying Devices Added by an Employee	17-7
Registered Endpoints Report	17-7
Errors When Adding Devices to My Devices Portal	17-7
Devices Deleted from My Devices Portal Remain in Endpoints Database	17-8
Deployment Scenarios for Personal Devices Using Native Suppliants	17-8

PART 5

Enabling and Configuring Cisco ISE Services

CHAPTER 18

Setting Up Policy Conditions 18-1

Simple and Compound Conditions	18-1
Policy Evaluation	18-2
Creating Simple Conditions	18-2
Creating Compound Conditions	18-3
Profiler Conditions	18-4
Creating a Profiler Condition	18-4
Posture Conditions	18-5
Simple Posture Conditions	18-5
Creating Simple Posture Conditions	18-6
Compound Posture Conditions	18-6
Cisco-Predefined Condition for Enabling Automatic Updates in Windows Clients	18-7
Cisco-Preconfigured Antivirus and Antispyware Conditions	18-7
Antivirus and Antispyware Support Chart	18-7
Creating Compound Posture Conditions	18-7
Creating Time and Date Conditions	18-8

CHAPTER 19

Managing Authentication Policies 19-1

Cisco ISE Authentication Policies	19-1
Policy Condition Evaluation	19-2
Supported Authentication Protocols	19-2
Supported Authentication Types and Database	19-3
Types of Authentication Failures	19-3
Authentication Policy Terminology	19-4
Simple Authentication Policies	19-4

Simple Authentication Policy Flow	19-5
Guidelines for Configuring Simple Authentication Policies	19-6
Rule-Based Authentication Policies	19-6
Rule-Based Authentication Policy Flow	19-7
Supported Dictionaries for Rule-Based Authentication Policies	19-8
Attributes Supported by Dictionaries	19-8
Protocol Settings for Authentication	19-10
Guidelines for Using EAP-FAST as Authentication Protocol	19-11
Configuring EAP-FAST Settings	19-11
Generating the PAC for EAP-FAST	19-12
Configuring EAP-TLS Settings	19-12
Configuring PEAP Settings	19-13
Configuring RADIUS Settings	19-13
Network Access Service	19-14
Defining Allowed Protocols for Network Access	19-14
Enabling MAB from Non-Cisco Devices	19-16
Enabling MAB from Cisco Devices	19-17
Cisco ISE Acting as a RADIUS Proxy Server	19-18
Configuring External RADIUS Servers	19-18
RADIUS Server Sequence	19-19
Defining RADIUS Server Sequences	19-19
Policy Modes	19-19
Guidelines for Changing Policy Modes	19-20
Changing Policy Modes	19-21
Configuring a Simple Authentication Policy	19-21
Configuring a Rule-Based Authentication Policy	19-22
Policy Sets	19-23
Policy Set Evaluation Flow	19-24
Guidelines for Creating Policy Sets	19-25
Global Authorization Exception Policy	19-25
Configuring Policy Sets	19-25
Authentication Policy Built-In Configurations	19-26
Viewing Authentication Results	19-28
Authentication Dashlet	19-30
Authentication Reports and Troubleshooting Tools	19-30

CHAPTER 20

Managing Authorization Policies and Profiles 20-1

Cisco ISE Authorization Policies	20-1

Cisco ISE Authorization Profiles	20-2
Authorization Policy Terminology	20-2
Network Authorization	20-2
Policy Elements	20-3
Authorization Profile	20-3
Authorization Policy	20-3
Access Control Lists	20-4
Authorization Policies and Supported Dictionaries	20-4
Guidelines for Configuring Authorization Policies and Profiles	20-4
Default Authorization Policy, Rule, and Profile Configuration	20-5
Configuring Authorization Policies	20-8
Time and Date Conditions	20-10
Permissions for Authorization Profiles	20-10
Configuring Permissions for New Standard Authorization Profiles	20-10
Downloadable ACLs	20-11
Supported DACL Format	20-11
Configuring Permissions for Downloadable ACLs	20-13
Machine Access Restriction for Active Directory User Authorization	20-13

CHAPTER 21

Cisco ISE Endpoint Profiling Policies 21-1

Cisco ISE Profiling Service	21-1
Endpoint Inventory Using Profiling Service	21-2
Cisco ISE Profiler Queue Limit Configuration	21-2
Configuring Profiling Service in Cisco ISE Nodes	21-3
Network Probes Used by Profiling Service	21-4
NetFlow Probe	21-4
DHCP Probe	21-5
Wireless LAN Controller Configuration in DHCP Bridging Mode	21-6
DHCP SPAN Probe	21-6
HTTP Probe	21-6
HTTP SPAN Probe	21-7
Unable to Collect HTTP Attributes in Cisco ISE Running on VMware	21-7
RADIUS Probe	21-7
Network Scan Probe	21-7
Limitations of NMAP Manual Subnet Scan	21-8
NMAP Manual Subnet Scan Command	21-8
Network Mapper Integration with Cisco ISE	21-8
SNMP Read Only Community Strings for NMAP Manual Subnet Scan	21-9
IP Address and MAC Address Binding	21-9

DNS Probe	21-10
DNS FQDN Lookup	21-10
DNS Lookup with an Inline Posture Node Deployment in Bridged Mode	21-10
Configuring Call Station ID Type in the WLC Web Interface	21-11
SNMP Query Probe	21-11
Cisco Discovery Protocol Support with SNMP Query	21-12
Link Layer Discovery Protocol Support with SNMP Query	21-12
SNMP Trap Probe	21-13
Configuring Probes per Cisco ISE Node	21-13
Setting up COA, SNMP RO Community and Endpoint Attribute Filter	21-15
Global Configuration of Change of Authorization for Authenticated Endpoints	21-15
Use Cases for Issuing Change of Authorization	21-16
Exemptions for Issuing a Change of Authorization	21-17
Change of Authorization Issued for Each Type of CoA Configuration	21-18
Attribute Filters for ISE Database Persistence and Performance	21-18
Global Setting to Filter Endpoint Attributes with Whitelist	21-19
Attributes Collection from IOS Sensor Embedded Switches	21-20
IOS Sensor Embedded Network Access Devices	21-20
Configuration Checklist for IOS Sensor-Enabled Network Access Devices	21-21
Endpoint Profiling Policy Rules	21-22
Creating Endpoint Profiling Policies	21-22
Change of Authorization Configuration per Endpoint Profiling Policy	21-24
Importing Endpoint Profiling Policies	21-24
Exporting Endpoint Profiling Policies	21-25
Predefined Endpoint Profiling Policies	21-25
Predefined Endpoint Profiling Policies Overwritten During Upgrade	21-26
Unable to Delete Endpoint Profiling Policies	21-26
Predefined Profiling Policies for Draeger Medical Devices	21-27
Endpoint Profiling Policy for Unknown Endpoints	21-27
Endpoint Profiling Policy for Statically Added Endpoints	21-27
Endpoint Profiling Policy for Static IP Devices	21-28
Endpoint Profiling Policy Matching	21-28
Endpoint Profiling Policies Used for Authorization	21-28
Endpoint Profiling Policies Grouped into Logical Profiles	21-28
Creating Logical Profiles	21-29
Profiling Exception Actions	21-29
Creating Exception Actions	21-30
Profiling Network Scan Actions	21-30
Creating Network Scan Actions	21-31

Operating System Scan	21-31
SNMP Port Scan	21-32
Common Ports Scan	21-32
Common Ports	21-33
Cisco ISE Integration with Cisco NAC Appliance	21-33
Cisco Clean Access Manager Configuration in Administration Nodes	21-34
Cisco ISE Profiler and Cisco Clean Access Manager Communication	21-34
Adding Cisco Clean Access Managers	21-35
Creating Endpoints with Static Assignments of Policies and Identity Groups	21-36
Importing Endpoints from CSV Files	21-36
Default Import Template Available for Endpoints	21-37
Unknown Endpoints Reprofiled During Import	21-37
Static Assignments of Policies and Identity Groups for Endpoints Retained During Import	21-38
Endpoints with Invalid Profiles Not Imported	21-38
Importing Endpoints from LDAP Server	21-39
Exporting Endpoints with Comma-Separated Values File	21-39
Identified Endpoints	21-40
Identified Endpoints Locally Stored in Policy Service Nodes Database	21-40
Policy Service Nodes in Cluster	21-41
Creating Endpoint Identity Groups	21-42
Identified Endpoints Grouped in Endpoint Identity Groups	21-42
Default Endpoint Identity Groups Created for Endpoints	21-43
Endpoint Identity Groups Created for Matched Endpoint Profiling Policies	21-43
Adding Static Endpoints in Endpoint Identity Groups	21-44
Dynamic Endpoints Reprofiled After Adding or Removing in Identity Groups	21-44
Endpoint Identity Groups Used in Authorization Rules	21-44
Profiler Feed Service	21-44
OUI Feed Service	21-45
Configuring Profiler Feed Service	21-46
Removing Updates to Endpoint Profiling Policies	21-47
Profiler Reports	21-47

CHAPTER 22
Configuring Client Provisioning 22-1

Client Provisioning Resource Types	22-1
Enabling and Disabling Client Provisioning	22-2
Adding Client Provisioning Resources from Remote Sources	22-3
Adding Client Provisioning Resources from a Local Machine	22-3
Downloading Client Provisioning Resources Automatically	22-4

Client Login Session Criteria	22-5
Cisco ISE Agents	22-5
Cisco NAC Agent for Windows Clients	22-5
Uninstalling Cisco NAC Agent for Windows Clients	22-6
Windows 8 Metro and Metro App Support —Toast Notifications	22-6
Cisco NAC Agent for Macintosh Clients	22-7
Uninstalling Cisco NAC Agent for Macintosh Clients	22-7
Cisco NAC Web Agent	22-7
Agent Login Screen Customization	22-8
Custom nac_login.xml File Template	22-9
Using a Custom Corporate/Company Logo	22-10
Custom nacStrings_xx.xml File Template	22-11
Sample Extended nacStrings_xx.xml File	22-11
UpdateFeed.xml Descriptor File Template	22-12
Creating an Agent Customization File	22-13
Agent XML File Installation Directories	22-14
Agent Profile Configuration Guidelines	22-14
Agent Profile Parameters and Applicable Values	22-15
Example XML File Generated Using the Create Profile Function	22-23
Creating Windows Agent Profiles	22-23
Creating Mac OS X Agent Profiles	22-24
Creating Native Supplicant Profiles	22-25
Allowed Protocol Settings	22-26
Configuring Personal Device Registration Behavior	22-26
Provisioning Client Machines with the Cisco NAC Agent MSI Installer	22-27
Configuring Client Provisioning Resource Policies	22-28
Viewing Client Provisioning Reports	22-30
Viewing Client Provisioning Requests	22-30
Viewing Client Access Sessions	22-30
Viewing Client Provisioning Resource Configuration Changes	22-30
Viewing Supplicant Provisioning Requests	22-31
Viewing Client Provisioning Event Logs	22-31
Collecting Cisco NAC Agent Logs	22-31

CHAPTER 23

Configuring Client Posture Policies 23-1

Posture Service	23-1
Components of Posture Services	23-2
Posture and Client-Provisioning Policies Workflow	23-3

Posture Service Licenses	23-3
Posture Service Deployment	23-4
Deploying Posture Session Service	23-4
Running Posture Reports	23-5
Posture Administration Settings	23-5
Timer Settings for Clients	23-5
Setting Timer for Users to Remediate	23-6
Setting Timer for Users to Transition	23-6
Setting Timer to Automatically Close the Login Window	23-7
Setting Posture Status for Non-Agent Devices	23-7
Periodic Reassessments	23-7
Configuring Periodic Reassessments	23-8
Downloading Posture Updates	23-9
Downloading Posture Updates Automatically	23-9
Configuring Acceptable Use Policies for Posture Assessment	23-10
Configuring Posture Policies	23-11
Posture Assessment Options	23-12
Posture Remediation Options	23-12
Custom Conditions for Posture	23-13
Custom Posture Remediation Actions	23-13
Adding a File Remediation	23-15
Adding a Link Remediation	23-15
Adding an Antivirus Remediation	23-15
Adding an Antispyware Remediation	23-16
Adding a Launch Program Remediation	23-16
Windows Update Remediation	23-17
Adding a Windows Update Remediation	23-17
Adding a Windows Server Update Services Remediation	23-18
Posture Assessment Requirements	23-18
Client System Stuck in Noncompliant State	23-19
Creating Client Posture Requirements	23-19
Custom Permissions for Posture	23-20
Configuring Standard Authorization Policies	23-21

CHAPTER 24

Configuring Cisco Security Group Access Policies 24-1

Security Group Access Architecture	24-1
SGA Features	24-2
SGA Terminology	24-3

Supported Switches for SGA	24-4
Components Required for SGA	24-5
Enable SGA Solution	24-5
Configure SGA Settings on the Switches	24-6
Configuring SGA Devices	24-6
Configuring Security Group Access Settings	24-7
Configuring Security Group Access AAA Servers	24-8
Configure Security Groups	24-8
Adding Security Groups	24-9
Configure Security Group Access Control Lists	24-10
Adding Security Group Access Control Lists	24-10
Map Security Groups to Devices	24-11
Adding Security Group Mappings	24-11
Configuring SGA Policy by Assigning SGTs to Devices	24-12
Assigning Security Groups to Users and Endpoints	24-13
Egress Policy	24-13
View the Egress Policy	24-14
Source Tree	24-14
Destination Tree	24-14
Matrix View	24-14
Configure Egress Policy Table Cells	24-15
Adding the Mapping of Egress Policy Cells	24-15
Configuring SGT from Egress Policy	24-16
Configuring SGACL from Egress Policy	24-16
Push Button	24-16
Monitor Mode	24-17
Features of Monitor Mode	24-17
Running Top N RBACL Drops by User	24-17
The Unknown Security Group	24-18
Default Policy	24-18
OOB SGA PAC	24-18
SGA PAC Provisioning	24-19
Generating an SGA PAC from the Settings Screen	24-19
Generating an SGA PAC from the Network Devices Screen	24-19
Generating an SGA PAC from the Network Devices List Screen	24-20
Monitoring SGA PAC	24-20
SGA CoA	24-21
CoA Supported Network Devices	24-21
Environment CoA	24-22

Initiate Environment CoA	24-23
Per Policy CoA	24-24
Update RBACL Named List CoA	24-24
Update SGT Matrix CoA	24-25
Policies Update CoA	24-26
SGA CoA Summary	24-27
Monitor SGA CoA	24-27
SGA CoA Alarms	24-28
Running SGA CoA Report	24-28

PART 6

Monitoring and Troubleshooting Cisco ISE

CHAPTER 25

Monitoring and Troubleshooting 25-1

Monitoring and Troubleshooting Service in Cisco ISE	25-1
Cisco ISE Dashboard	25-2
User Roles and Permissions for Monitoring and Troubleshooting Capabilities	25-2
Data Stored in Monitoring Database	25-3
Device Configuration for Monitoring	25-3
Monitoring Network Process Status	25-3
Monitoring Network Authentications	25-4
Determining Profiler Activity and Profiled Endpoints	25-4
Checking Posture Compliance	25-4
Cisco ISE Alarms	25-5
Enabling and Configuring Alarms	25-11
Monitoring Alarms	25-11
Log Collection	25-12
Alarm Syslog Collection Location	25-12
Live Authentications	25-13
Monitoring Live Authentications	25-13
Global Search for Endpoints	25-14
Session Trace for an Endpoint	25-15
Session Removal from the Directory	25-17
Troubleshooting Network Access Issues	25-17
Diagnostic Troubleshooting Tools	25-18
Troubleshooting Unexpected RADIUS Authentication Results	25-18
Executing IOS Show Commands to Check Configuration	25-19
Troubleshooting Network Device Configuration Issues	25-20
Troubleshooting Endpoint Posture Failure	25-20

TCP Dump Utility to Validate the Incoming Traffic	25-21
Using TCP Dump to Monitor Network Traffic	25-21
Saving a TCP Dump File	25-22
Comparing Unexpected SGACL for an Endpoint or User	25-22
Egress Policy Diagnostic Flow	25-23
Troubleshooting Connectivity Issues in an SGA-Enabled Network with SXP-IP Mappings	25-23
Troubleshooting Connectivity Issues in an SGA-Enabled Network with IP-SGT Mappings	25-24
Troubleshooting Connectivity Issues in an SGA-Enabled Network by Comparing Device SGT Mappings	25-24
Obtaining Additional Troubleshooting Information	25-25
Cisco ISE Support Bundle	25-25
Downloading Support Bundles	25-26
Cisco ISE Debug Logs	25-27
Cisco ISE Components and the Corresponding Debug Logs	25-27
Downloading Debug Logs	25-28
Monitoring Database	25-29
Back Up and Restore of the Monitoring Database	25-29
Monitoring Database Purge	25-30
Guidelines for Purging the Monitoring Database	25-30
Purging Older Monitoring Data	25-30

CHAPTER 26
Reporting 26-1

Cisco ISE Reports	26-1
Running and Viewing Reports	26-2
Reports Navigation	26-2
Exporting Reports	26-2
Scheduling and Saving ISE Reports	26-3
Adding Favorite Reports	26-4
Cisco ISE Active RADIUS Sessions	26-4
Changing Authorization for RADIUS Sessions	26-5
Available Reports	26-6

PART 7
Reference

APPENDIX A
Administration User Interface Reference A-1

System Administration	A-1
Deployment Settings	A-1
Deployment Nodes List Page	A-1

General Node Settings	A-2
Profiling Node Settings	A-5
Inline Posture Node Settings	A-6
License Page Parameters	A-9
Certificate Store Settings	A-10
Certificate Store Page	A-11
Certificate Store Import Settings	A-11
Certificate Store Edit Settings	A-12
Logging Settings	A-13
Remote Logging Target Settings	A-13
Logging Category Settings	A-14
Maintenance Settings	A-15
Repository Settings	A-15
On-Demand Backup Settings	A-16
Scheduled Backup Settings	A-16
Admin Access Settings	A-17
Administrator Password Policy Settings	A-17
Session Timeout and Session Info Settings	A-18
Settings	A-19
Posture General Settings	A-19
Posture Reassessment Configuration Settings	A-19
Posture Acceptable Use Policy Configuration Settings	A-20
EAP-FAST Settings	A-22
Generate PAC for EAP-FAST Settings	A-22
EAP-TLS Settings	A-23
PEAP Settings	A-23
RADIUS Settings	A-24
Security Group Access Settings	A-24
Identity Management	A-25
Endpoints	A-25
Endpoint Settings	A-25
Endpoint Import from LDAP Settings	A-27
Groups	A-28
Endpoint Identity Group Settings	A-28
External Identity Sources	A-29
LDAP Identity Source Settings	A-29
RADIUS Token Identity Sources Settings	A-32
RSA SecurID Identity Source Settings	A-34
Identity Management Settings	A-35
User Password Policy Settings	A-35

Network Resources	A-35
Network Devices	A-35
Network Device Definition Settings	A-36
Default Network Device Definition Settings	A-41
Network Device Import Settings	A-41
Network Device Groups	A-42
Network Device Group Settings	A-42
Network Device Group Import Settings	A-43
External RADIUS Server Settings	A-43
RADIUS Server Sequences	A-44
NAC Manager Settings	A-45
Web Portal Management	A-46
Sponsor Group Policy Settings	A-46
Sponsor Group Settings	A-47
Web Portal Management Settings	A-48
General Portal Theme Settings	A-49
Port Settings for Web Portals	A-50
Guest Purge Settings	A-52
Sponsor Language Template Settings	A-52
My Devices Portal Language Template Settings	A-53
My Devices Portal Settings	A-54
Guest Portal Language Template Settings	A-55
Multi-Portal Configuration Settings	A-56
Guest Portal Policy Settings	A-59
Guest Time Profile Settings	A-60
Guest Username Policy Settings	A-61

APPENDIX B

Policy User Interface Reference B-1

Authentication	B-1
Simple Authentication Policy Configuration Settings	B-1
Rule-Based Authentication Policy Configuration Settings	B-2
Authorization Policy Settings	B-5
Endpoint Profiling Policies Settings	B-5
Dictionaries	B-8
RADIUS Vendor Dictionary Attribute Settings	B-8
Conditions	B-9
Profiler Condition Settings	B-9
Posture Conditions Settings	B-10
File Condition Settings	B-10

Registry Condition Settings	B-11
Application Condition Settings	B-12
Service Conditions Settings	B-13
Posture Compound Condition Settings	B-13
Antivirus Compound Condition Settings	B-13
Antispyware Compound Condition Settings	B-15
Dictionary Simple Conditions Settings	B-16
Dictionary Compound Condition Settings	B-16
Time and Date Condition Settings	B-17
Results	B-18
Allowed Protocols Services Settings	B-19
PAC Options	B-22
Authorization Profile Settings	B-23
Profiling Exception Action Settings	B-25
File Remediation	B-26
Link Remediation	B-26
Antivirus Remediation	B-26
Antispyware Remediation	B-27
Launch Program Remediation	B-27
Windows Update Remediation	B-28
Windows Server Update Services Remediation	B-29
Client Posture Requirements	B-30

APPENDIX C

Operations User Interface Reference C-1

Recent RADIUS Authentications	C-1
Show Live Sessions	C-2
Live Authentication Details	C-3
Diagnostic Tools	C-4
RADIUS Authentication Troubleshooting Settings	C-4
Execute Network Device Command Settings	C-5
Evaluate Configuration Validator Settings	C-5
Posture Troubleshooting Settings	C-6
TCP Dump Settings	C-6
SXP-IP Mappings	C-7
IP User SGT	C-8
Device SGT Settings	C-9
Progress Details Settings	C-10
Results Summary	C-10

APPENDIX D**Sample Code for Sponsor and Guest Portal Customizations D-1**

Sample Code for Custom Guest Notifications from Sponsor Portal D-1

E-Mail Notification Template D-1

SMS Text Message Notification Template D-2

Print Notification Template D-3

Sample HTML for Custom Pages for the Guest Portal D-3

Fields Used on Custom HTML Pages D-4

Login Page Sample HTML D-5

Detect Cookies at Login Sample HTML D-8

Successful Guest Login Page Sample HTML D-9

Error Page Sample HTML D-10

Acceptable Use Policy (AUP) Page Sample HTML D-11

Change Password Page Sample HTML D-13

Self-Registration Page Sample HTML D-14

Self-Registration Result Page Sample HTML D-17

Device Registration Page Sample HTML D-18

Sample style.css for Custom Guest Portal HTML Pages D-19

APPENDIX E**Network Access Flows E-1**

Password-Based Authentication E-1

Secure Authentication Using Encrypted Passwords and Cryptographic Techniques E-1

Authentication Methods and Authorization Privileges E-1

RADIUS Protocol Support in Cisco ISE E-2

Network Access for Users E-2

RADIUS-Based Protocols Without EAP E-2

RADIUS-Based Non-EAP Authentication Flow E-3

Password Authentication Protocol E-3

RADIUS-Based PAP Authentication in Cisco ISE E-3

Challenge Handshake Authentication Protocol E-4

Microsoft Challenge Handshake Authentication Protocol Version 1 E-4

Microsoft Challenge Handshake Authentication Protocol Version 2 E-5

RADIUS-Based EAP Protocols E-5

RADIUS-Based EAP Authentication Flow E-6

Extensible Authentication Protocol-Message Digest 5 E-6

Lightweight Extensible Authentication Protocol E-7

Protected Extensible Authentication Protocol E-7

Advantages of Using PEAP E-8

Supported Supplicants for the PEAP Protocol E-8

PEAP Protocol Flow E-9

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling	E-10
Benefits of EAP-FAST	E-10
EAP-FAST Flow	E-11

APPENDIX F

Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions F-1

Enable Your Switch to Support Standard Web Authentication	F-2
Define a Local Username and Password for Synthetic RADIUS Transactions	F-2
Set the NTP Server to Ensure Accurate Log and Accounting Timestamps	F-2
Enable AAA Functions	F-3
Configure a RADIUS Server	F-3
Configure the Switch to Send RADIUS Accounting Start/Stop to Inline Posture Nodes	F-4
Enable RADIUS Change of Authorization (CoA)	F-4
Enable Device Tracking and DHCP Snooping	F-4
Enable 802.1X Port-Based Authentication	F-4
Use EAP for Critical Authentications	F-4
Throttle AAA Requests Using Recovery Delay	F-5
Define VLANs Based on Enforcement States	F-5
Define Local (Default) ACLs on the Switch	F-5
Enable Cisco Security Group Access Switch Ports	F-6
Enable EPM Logging	F-8
Enable SNMP Traps	F-8
Enable SNMP v3 Query for Profiling	F-8
Enable MAC Notification Traps for Profiler to Collect	F-9
Configure the RADIUS Idle-Timeout	F-9
Set Up the Wireless LAN Controller for iOS Supplicant Provisioning	F-9
Configure the Wireless LAN Controller to Support Apple Devices	F-9
Configure ACLs on the Wireless LAN Controller for MDM Interoperability	F-10

APPENDIX G

Troubleshooting Cisco ISE G-1

Installation and Network Connection Issues	G-2
Unknown Network Device	G-3
CoA Not Initiating on Client Machine	G-3
Users Are Assigned to Incorrect VLAN During Network Access Sessions	G-4
Client Machine URL Redirection Function Not Working	G-5
Cisco ISE Profiler is Not Able to Collect Data for Endpoints	G-5
RADIUS Accounting Packets (Attributes) Not Coming from Switch	G-6
Policy Service Node Not Passing Traffic	G-7

Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation	G-7
Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working	G-8
Cisco SNS-3415 Appliance RAID Configuration Cleared Inadvertently	G-8
Cisco SNS-3495 Appliance RAID Configuration Cleared Inadvertently	G-9
Licensing and Administrator Access	G-11
Certificate Expired	G-11
Configuration and Operation (Including High Availability)	G-12
Client Machines Are Unable to Authenticate	G-12
Users Are Not Appropriately Redirected to URL	G-13
Cannot Download Remote Client Provisioning Resources	G-13
Lost Monitoring and Troubleshooting Data After Registering Policy Service Node to Administration Node	G-13
Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8	G-14
Data Out of Sync Between Primary And Secondary ISE Nodes	G-14
External Authentication Sources	G-16
User Authentication Failed	G-16
Missing User for RADIUS-Server Test Username in Cisco ISE Identities	G-16
Connectivity Issues Between the Network Access Device (Switch) and Cisco ISE	G-17
Active Directory Disconnected	G-17
Cisco ISE Node Not Authenticating with Active Directory	G-18
RADIUS Server Error Message Entries Appearing in Cisco ISE	G-18
RADIUS Server Connectivity Issues (No Error Message Entries Appearing in Cisco ISE)	G-19
Client Access, Authentication, and Authorization	G-21
Cannot Authenticate on Profiled Endpoint	G-21
Quarantined Endpoints Do Not Renew Authentication Following Policy Change	G-22
Endpoint Does Not Align to the Expected Profile	G-23
User is Unable to Authenticate Against the Local Cisco ISE Identity Store	G-24
Sponsor Users Cannot Log in to Sponsor Portal	G-24
Certificate-Based User Authentication via Supplicant Failing	G-25
802.1X Authentication Fails	G-26
Users Are Reporting Unexpected Network Access Issues	G-26
Authorization Policy Not Working	G-27
Switch is Dropping Active AAA Sessions	G-28
URL Redirection on Client Machine Fails	G-29
Agent Download Issues on Client Machine	G-31
Agent Login Dialog Not Appearing	G-32
Agent Fails to Initiate Posture Assessment	G-32
Agent Displays "Temporary Access"	G-33
Cisco ISE Does Not Issue CoA Following Authentication	G-33

Non-Guest Users Do Not Go Through Guest Flow for Network Access	G-34
Guest Devices Keep Losing Network Access	G-34
Error Messages	G-35
ACTIVE_DIRECTORY_USER_INVALID_CREDENTIALS	G-35
ACTIVE_DIRECTORY_USER_AUTH_FAILED	G-35
ACTIVE_DIRECTORY_USER_PASSWORD_EXPIRED	G-36
ACTIVE_DIRECTORY_USER_WRONG_PASSWORD	G-36
ACTIVE_DIRECTORY_USER_ACCOUNT_DISABLED	G-36
ACTIVE_DIRECTORY_USER_RESTRICTED_LOGON_HOURS	G-36
ACTIVE_DIRECTORY_USER_NON_COMPLIANT_PASSWORD	G-36
ACTIVE_DIRECTORY_USER_UNKNOWN_DOMAIN	G-37
ACTIVE_DIRECTORY_USER_ACCOUNT_EXPIRED	G-37
ACTIVE_DIRECTORY_USER_ACCOUNT_LOCKED_OUT	G-37
ACTIVE_DIRECTORY_GROUP_RETRIEVAL_FAILED	G-37
ACTIVE_DIRECTORY_MACHINE_AUTHENTICATION_DISABLED	G-37
ACTIVE_DIRECTORY_ATTRIBUTE_RETRIEVAL_FAILED	G-38
ACTIVE_DIRECTORY_PASSWORD_CHANGE_DISABLED	G-38
ACTIVE_DIRECTORY_USER_UNKNOWN	G-38
ACTIVE_DIRECTORY_CONNECTION_FAILED	G-38
ACTIVE_DIRECTORY_BAD_PARAMETER	G-38
ACTIVE_DIRECTORY_TIMEOUT	G-38
Configure NADs for ISE Monitoring	G-39
Troubleshooting APIs	G-40
Contacting the Cisco Technical Assistance Center	G-41



Preface

Revised: December 5, 2013, OL-26134-01

This preface introduces the *Cisco Identity Services Engine User Guide, Release 1.2* and contains the following sections:

- [Audience, page xxxv](#)
- [Document Organization Map, page xxxvi](#)
- [Document Conventions, page xxxvii](#)
- [Documentation Updates, page xxxviii](#)
- [Related Documentation, page xxxviii](#)
- [Notices, page xl](#)
- [Obtaining Documentation and Submitting a Service Request, page xlii](#)

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 Map

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	
	Cisco ISE Features
	Navigating the Admin portal
Part 2: Deploying Cisco ISE Nodes	
	Setting Up Cisco ISE in a Distributed Environment
	Setting Up Inline Posture
Part 3: Setting Up Cisco ISE Management Access	
	Administering Cisco ISE
	Managing Administrators and Admin Access Policies
	Cisco ISE Licenses
	Managing Certificates
	Managing Network Devices
	Managing Resources
	Logging
	Managing Backup and Restore Operations
	Setting Up Endpoint Protection Service
Part 4: Managing Users and End-User Portals	
	Managing Users and External Identity Sources
	Setting Up and Customizing End-User Web Portals
	Supporting Authorized Network Access for Guests
	Supporting Personal Devices
Part 5: Enabling and Configuring Cisco ISE Services	
	Setting Up Policy Conditions
	Managing Authentication Policies
	Managing Authorization Policies and Profiles
	Cisco ISE Endpoint Profiling Policies
	Configuring Client Provisioning
	Configuring Client Posture Policies
	Configuring Cisco Security Group Access Policies
Part 6: Monitoring and Troubleshooting Cisco ISE	
	Monitoring and Troubleshooting
	Reporting

Part	Chapter
Part 7: Reference	
	Appendix A, “Administration User Interface Reference”
	Appendix B, “Policy User Interface Reference”
	Appendix C, “Operations User Interface Reference”
	Appendix D, “Sample Code for Sponsor and Guest Portal Customizations”
	Appendix E, “Network Access Flows”
	Appendix F, “Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions”
	Appendix G, “Troubleshooting Cisco ISE”
	Appendix H, “Supported Management Information Bases in Cisco ISE”

**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

Throughout this guide, the term Admin portal, refers to the user interface of the primary Administration node.

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:

1. Option > Option: Used to select a series of menu options.
2. Variables for which you must supply a value are shown in *italic* font.
3. 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.

Examples use these conventions:

- Terminal sessions and sample console screen displays are in *screen* font.
- Information you enter is in **boldface screen** font.
- 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 (|).
- 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

[Table 1](#) lists the creation and update history of this guide.

Table 1 **Updates to Cisco Identity Services Engine User Guide, Release 1.2**

Date	Description
12/5/2013	Resolved CSCul77700
12/5/2013	Resolved CSCul37345
12/3/2013	Resolved CSCul12780
11/6/2013	Resolved CSCul22203
10/14/13	Resolved CSCuj53930
10/14/13	Resolved CSCuj58711
8/16/2013	Resolved CSCui61280
7/25/2013	Cisco Identity Services Engine, Release 1.2

Related Documentation

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

- [Release-Specific Documents, page xxxix](#)
- [Platform-Specific Documents, page xxxix](#)

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
<i>Release Notes for the Cisco Identity Services Engine, Release 1.2</i>	http://www.cisco.com/en/US/products/ps11640/prod_release_notes_list.html
<i>Cisco Identity Services Engine Network Component Compatibility, Release 1.2</i>	http://www.cisco.com/en/US/products/ps11640/products_device_support_tables_list.html
<i>Cisco Identity Services Engine User Guide, Release 1.2</i>	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
<i>Cisco Identity Services Engine Hardware Installation Guide, Release 1.2</i>	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
<i>Cisco Identity Services Engine Upgrade Guide, Release 1.2.</i>	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
<i>Cisco Identity Services Engine, Release 1.2 Migration Tool Guide</i>	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
<i>Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2.</i>	http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html
<i>Cisco Identity Services Engine CLI Reference Guide, Release 1.2.</i>	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
<i>Cisco Identity Services Engine API Reference Guide, Release 1.2.</i>	http://www.cisco.com/en/US/products/ps11640/prod_command_reference_list.html
<i>Cisco Identity Services Engine Troubleshooting Guide, Release 1.2.</i>	http://www.cisco.com/en/US/products/ps11640/prod_troubleshooting_guides_list.html
<i>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</i>	http://www.cisco.com/en/US/products/ps11640/prod_installation_guides_list.html
<i>Cisco Identity Services Engine In-Box Documentation and China RoHS Pointer Card</i>	http://www.cisco.com/en/US/products/ps11640/products_documentation_roadmaps_list.html
<i>My Devices Portal FAQs, Release 1.2</i>	http://www.cisco.com/en/US/products/ps11640/products_user_guide_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 notices in this section 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.



PART 1

Introducing Cisco ISE



Cisco ISE Features

Cisco Identity Services Engine (Cisco 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 Cisco ISE administrators, sanctioned sponsor administrators, or both
- Enforces endpoint compliance by providing comprehensive client provisioning measures and assessing the 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

Related Topics

- [*Cisco Identity Services Engine Hardware Installation Guide, Release 1.2.*](#)

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

- [Identity-Based Network Access, page 1-2](#)
- [Support for Multiple Deployment Scenarios, page 1-2](#)
- [Basic User Authentication and Authorization, page 1-3](#)
- [Policy Sets, page 1-4](#)
- [FIPS 140-2 Implementation, page 1-4](#)
- [Support for Common Access Card Functions, page 1-5](#)
- [Client Posture Assessment, page 1-6](#)
- [Network Access for Guests, page 1-6](#)
- [Support for Personal Devices, page 1-6](#)
- [Wireless and VPN Traffic with Inline Posture Nodes, page 1-7](#)
- [Profiled Endpoints on the Network, page 1-7](#)
- [Support for SAnet Devices, page 1-7](#)
- [Support for Installation on Multiple Hardware and VMware Platforms, page 1-8](#)

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.

Related Topics

[Chapter 6, “Managing Administrators and Admin Access Policies.”](#)

Support for Multiple 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 standalone 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.

Related Topics

- [Chapter 3, “Setting Up Cisco ISE in a Distributed Environment”](#)
- [Chapter 4, “Setting Up Inline Posture”](#)

Support for UCS Hardware

In addition to Cisco ISE 3300 Series appliance, Cisco ISE 1.2 supports the UCS C220 M3 hardware and is available on the following platforms:

- SNS-3415 (small)
- SNS-3495 (large)

Related Topics

[Cisco Identity Services Engine Installation Guide, Release 1.2.](#)

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 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 “AuthenticationStatus” 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.

Related Topics

- [Chapter 19, “Managing Authentication Policies”](#)
- [Chapter 20, “Managing Authorization Policies and Profiles”](#)

Policy Sets

Cisco ISE supports policy sets, which let you group sets of authentication and authorization policies. As opposed to the basic authentication and authorization policy model, which is a flat list of authentication and authorization rules, policy sets let you logically define the organization’s IT business use cases into policy groups or services, such as VPN and 802.1x, such that it is easier for configuration, deployment, and troubleshooting.

Related Topics

- [Chapter 19, “Managing Authentication Policies”](#)
- [Chapter 20, “Managing Authorization Policies and Profiles”](#)

FIPS 140-2 Implementation

Cisco ISE, supports 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.
- Turning on FIPS mode also automatically disables PAP and CHAP protocols, which the Guest login function of Cisco ISE requires. For information on addressing this issue with Layer-3 Guest login implementation, see [Chapter 16, “Supporting Authorized Network Access for Guests.”](#)
- You might have to get your certificates re-issued if the encryption method used in the certificates is not supported by FIPS.

- 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

Related Topics

- [Chapter 5, “Administering Cisco ISE”](#) (Enabling FIPS Mode in Cisco ISE, page 5-8)
- [Chapter 8, “Managing Certificates”](#)
- [Chapter 9, “Managing Network Devices”](#)
- [Chapter 19, “Managing Authentication Policies”](#)

Support for 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 Admin portal. 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.

Related Topics

[Chapter 5, “Administering Cisco ISE.”](#)

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 occurs.

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

- Cisco NAC Web Agent—A temporal agent that the users install on their system at the time of login and 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 security compliance functions.

Related Topics

- [Chapter 22, “Configuring Client Provisioning”](#)
- [Chapter 23, “Configuring Client Posture Policies”](#)
- [Cisco Identity Services Engine Network Component Compatibility, Release 1.2](#)

Network Access for Guests

Cisco ISE administrators and employees who 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.

Related Topics

- [Chapter 16, “Supporting Authorized Network Access for Guests”](#)
- [Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2](#)

Support for Personal Devices

Cisco ISE allows employees to connect their personal devices, such as laptop computers, mobile phones, tablets, printers, and other network devices on the enterprise network.

Supporting these devices presents difficulties in protecting network services and enterprise data, so you must ensure that both the employees and their devices are authenticated and authorized for network access. With an advanced license, Cisco ISE provides you with the tools you need to allow employees to securely use their personal devices on your corporate network.

Related Topics

[Chapter 17, “Supporting Personal Devices.”](#)

Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM servers consist of a policy server and an inline enforcement point that controls the use of some applications on a mobile device (for example, an e-mail application) in the deployed environment. However, the network is the only entity that can provide granular access to endpoints based on ACLs, SGTs.

Related Topics

[Mobile Device Manager Interoperability with Cisco ISE, page 1-7.](#)

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. Consequently, 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.

Related Topics

[Chapter 4, “Setting Up Inline Posture.”](#)

Profiled 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 device types, 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 identity groups.

Related Topics

[Chapter 21, “Cisco ISE Endpoint Profiling Policies.”](#)

Support for SAnet Devices

Cisco ISE provides limited support for Session Aware Networking (SAnet), a session management framework on the switches that provides more consistent and flexible management of access-sessions, including visibility, authentication, and authorization. SAnet defines the notion of a service template which is an authorization object accepted both by ISE as well as by the device. This is in contradistinction to Cisco ISE authorization profiles which are containers of RADIUS authorization attributes that are merged and flattened into a list of attributes before they are sent to the device. Similarly, SAnet service templates are also containers of RADIUS authorization attributes but they are not flattened into a list before sending to the device. Instead, Cisco ISE sends the name of the service template and the device downloads the content (RADIUS attributes) if it does not already have a cached

or statically defined version of it. In addition, Cisco ISE sends CoA notifications to the device if the definition of a service template has changed, that is, if a RADIUS attribute was added, removed or changed.

Cisco ISE implements service templates as authorization profiles that contain a special flag that marks them as “Service Template” compatible. This way the service template, which is also an authorization profile, can be used in a single policy statement that will support sessions connecting from SANet capable devices as well as legacy devices.

Related Topics

[Chapter 20, “Managing Authorization Policies and Profiles.”](#)

Support for Installation on Multiple 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 either on a dedicated SNS-3400 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.

Related Topics

[Cisco Identity Services Engine Hardware Installation Guide, Release 1.2.](#)



Navigating the Admin portal

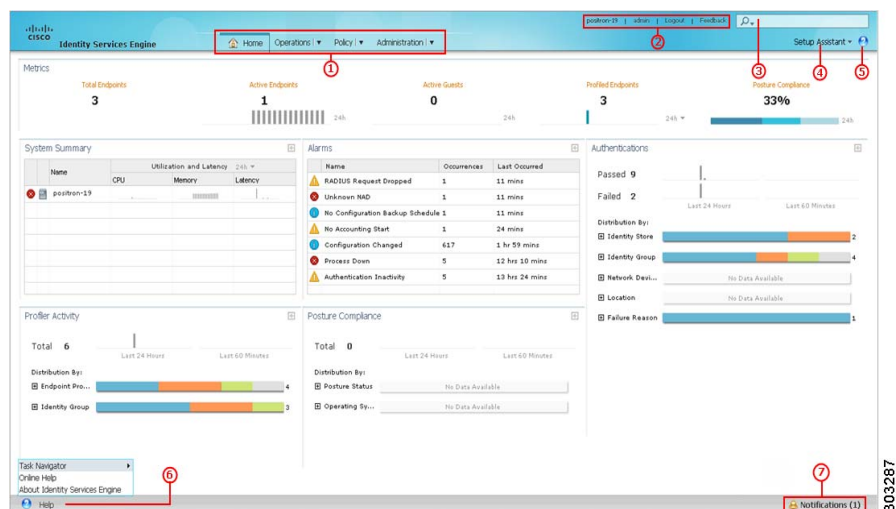
This chapter introduces the Cisco Identity Services Engine (ISE) Admin portal and contains the following topics:

- [Admin Portal, page 2-1](#)
- [Setup Assistant and Task Navigators, page 2-3](#)
- [Filtering Data on Listing Pages, page 2-8](#)
- [Cisco ISE Internationalization and Localization, page 2-10](#)
- [Admin Features Limited by Role-Based Access Control Policies, page 2-16](#)

Admin Portal

The Admin portal is an administration console from which you can manage various identity services. [Figure 2-1](#) shows the main elements of this portal.

Figure 2-1 Admin portal

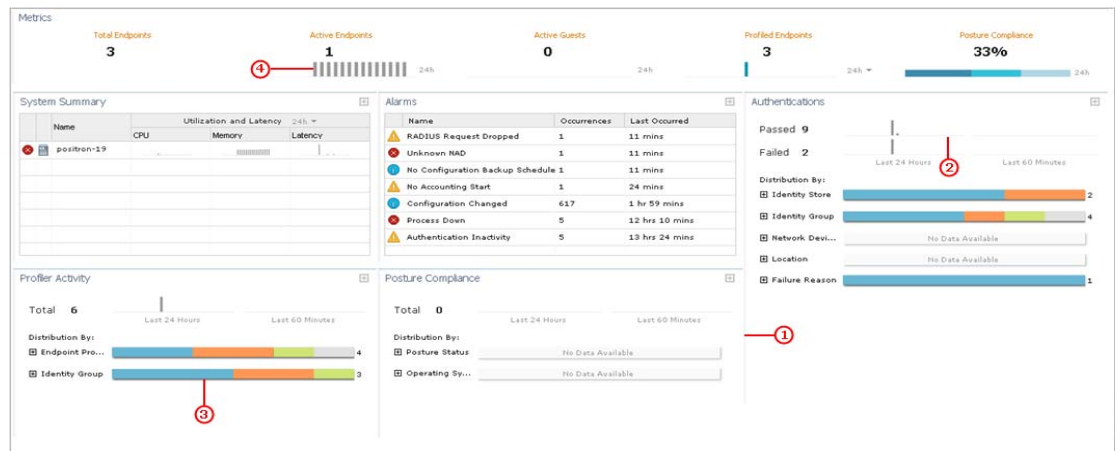


1	Menu Bar	Access tools for viewing, monitoring, and managing different Cisco ISE options: • Home: Access the dashboard, which is a real-time view of all the services running in the Cisco ISE network. • Operations: Access tools for monitoring real-time alarms and live authentications, querying historical data through reports, and troubleshooting network services. • Policy: Access tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning. • Administration: Access tools for managing Cisco ISE nodes, licenses, certificates, network devices, users, endpoints, and guest services.
2	Top Right Panel	View the connected Cisco ISE node. Click the appropriate options to edit account information, log out, and provide feedback to Cisco.
3	Search	Search for endpoints and display their distribution by profiles, failures, identity stores, location, device type, and so on.
4	Setup Assistant	Access wizard to create a basic configuration to demonstrate Cisco ISE feature functionality in your network.
5	Context-Sensitive Help	Access help for the currently displayed page.
6	Help	Access the complete Cisco ISE online Help system and the Task Navigator, which provides visual guides for navigating through procedures whose tasks span multiple screens.
7	Notifications	Hover the mouse cursor over this option to view a summary of notifications.

Cisco ISE Dashboard

The Cisco ISE Dashboard displays live consolidated and correlated statistical data that is essential for effective monitoring and troubleshooting. Dashboard elements show activity over 24 hours, unless otherwise noted. [Figure 2-2](#) shows some of the information available on the Cisco ISE Dashboard.

Figure 2-2 Cisco ISE User Dashboard



1	Dashlets	Dashboard element that displays statistical summaries about the devices and user accessing the network. In some dashlets, colored icons are displayed prior to the device names to convey the system health: • Green = Healthy • Yellow = Warning • Red = Critical • Gray = No information
2	Sparklines	Depict trends over time.
3	Stacked bar charts	Display the distribution of parameters using color as the dividing element, so you can see where one parameter ends and another begins. Display is limited to the top 10 distributions. In general, stacked bar charts use color to mark the boundary points between one data measurement and another.
4	Metric meters	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. You can click the number displayed above the metrics meter to view more information about the devices.

Setup Assistant and Task Navigators

The Setup Assistant and Task Navigators provide efficient configuration of Cisco ISE on your network. The Setup Assistant provides a basic Cisco ISE configuration based on your network settings and policies, and Task Navigators provide a visual path through the configuration tasks.

Setup Assistant

The Setup Assistant guides you through a series of questions in a wizard-like interface retaining your responses and using them to configure Cisco ISE directly. It enables you to set up a basic working Cisco ISE configuration as a proof-of-concept for your network. Your answers to the questions impact these Cisco ISE features: authentication, authorization, profiling, posture, client provisioning, guest services, and support for personal devices.

Cisco ISE Licensing Impact on Setup Assistant

Setup Assistant functionality depends on the Cisco ISE license that you have applied to your configuration.

Cisco ISE License	Identify Policy Requirements	Configure Network Access Services	Select Network Device Types
Basic	—	The posture, endpoint profiling, and personal devices options are not available.	—
Advanced	If you choose wired + monitor, the guest and posture choices are disabled on the next page. If you choose wireless and wired + monitor, the guest and posture choices on the next page impact wireless only.	The guest and posture choices are not available if you select wired + monitor on the previous page.	If you choose wired only on the first page, the wireless LAN controller (WLC) information does not appear. If you choose wireless only on the first page, switch information does not appear.
Wireless	The wired option is not available.	—	Switch information does not appear.

Running the Setup Assistant

When you start Cisco ISE 1.2 for the first time, you are prompted to run the Setup Assistant. If you choose not to run it then, you can run it again later.

Before You Begin

To perform this task, you must be a Super Admin. You can only run the Setup Assistant on the standalone or primary Administration node.

-
- Step 1** Click **Setup Assistant** in the upper-right corner of the Admin portal.
- Step 2** Follow the on-screen instructions to complete the configuration.
-

Setup Assistant Overwrites Previous Configurations

Each time you run the Setup Assistant, Cisco ISE overwrites previous settings, which can critically impact on your configuration in the following ways:

- All authentication, authorization, client provisioning, and posture policies are deleted and replaced, including any that you added without using the Setup Assistant.
- Other settings, such as policy elements and web portal customizations, are overwritten with any newly specified values. If you do not enter anything for the optional settings, the Setup Assistant resets them to their default values.

Identify Policy Requirements Page in Setup Assistant

Wired or Wireless

You must indicate whether you want to support wired or wireless connections, or both. If you are using a Cisco ISE Wireless License, the wired option is unavailable.

These choices impact the policies that Cisco ISE creates, and also dictate other required responses. For example, if you choose wired, you can also indicate whether your network supports IP phones.

You must also indicate whether or not the wired connections are monitored or if network access must be enforced based on compliance:

- Monitor generates non-compliance logs and reports, but does not require that users or devices comply with the defined policies.

In monitoring mode, posture and guest policies are ignored. If you support wired connections in monitoring mode, the Setup Assistant disables the guest and posture choices on the next page to prevent unauthorized computer and guest access.

If you support wired and wireless connections, you can enable the guest and posture features, but they will apply only to the wireless connections. The wireless connections always runs in enforcement mode.

- Enforce requires compliance with the defined policies.

Protected Subnets

You must indicate which subnets should be inaccessible by guests or noncompliant endpoints. This information is used when creating the downloadable ACLs.

Configure Network Access Service Page in Setup Assistant

User Authentication

Users belonging to these groups will be granted network access as employees and be allowed to create guest accounts using the Sponsor portal.

- Internal users—If you choose to create an internal user, Cisco ISE creates a single user using the name you enter and assigns the user to the default Employee and SponsorAllAccount user identity groups. You can verify this in the **Administration > Identity Management > Identities > Users** page after setup completes.

Because the Setup Assistant provides only the basic Cisco ISE configuration to demonstrate its functionality in your network, you cannot use it to import additional users into the internal user database. You can add additional internal users using the Admin portal after you complete the Setup Assistant.

- Active Directory—If you choose to join the Active Directory domain, Cisco ISE adds the indicated AD domain and joins to it. After joining the domain, you must choose an Active Directory group. All users belonging to this group will be able to authenticate using Dot1x and create guests using the Sponsor portal. You can verify this from the **Administration > Identity Management > External Identity Sources > Active Directory** page after setup completes.

Posture Compliance

When you enable posture using the Setup Assistant, Cisco ISE checks for antispymware and antivirus definitions and installations on connected endpoints.

You must indicate whether you want to assess or assess and enforce posture compliance for employees and guests:

- Assess generates reports about noncompliant users, but allows them to be authenticated.
- Enforce prevents authentication.

If you want to force Cisco ISE to redirect noncompliant endpoints to a remediation server before granting network access, enter the proxy server IP address.

If you enable posture compliance, Cisco ISE will:

- Download the Cisco NAC agents and update the **Policy > Policy Elements > Results > Client Provisioning > Resources** page.
- Create the downloadable ACLs on the **Policy > Policy Elements > Results > Authorization > Downloadable ACLs** page. All DACLs created by the Setup Assistant include the prefix AutoGen, such as: `AutoGen_DACL_PrePostureWired`.
- Create authorization profiles on the **Policy > Policy Elements > Results > Authorization > Authorization Profiles** page. Authorization profiles created by the Setup Assistant include the prefix AutoGen, such as: `AutoGen_profile_Byod_CWA`.
- Create authorization conditions on the **Policy > Policy Elements > Conditions > Simple Conditions** and **Policy > Policy Elements > Conditions > Compound Conditions** pages. Authorization conditions created by the Setup Assistant include the prefix AutoGen, such as: `AutoGen_condition_Android_Devices` or `AutoGen_condition_GuestWired`.
- Create client provisioning policies on the **Policy > Client Provisioning** page. Client provisioning policies created by the Setup Assistant include the prefix AutoGen, such as: `AutoGen_Provisioning`.
- Download posture updates from the **Administration > System > Settings > Posture > Updates** page.
- Create posture policies on the **Policy > Posture** page. Posture policies created by the Setup Assistant include the prefix AutoGen, such as: `AutoGen_Policy_Check_For_AS_Definition_Mac_Employee`.
- Create authorization policies on the **Policy > Authorization** page. Authorization policies created by the Setup Assistant include the prefix AutoGen, such as: `AutoGen_policy_Registered_Wireless_Devices`.
- Create authentication policies on the **Policy > Authentication** page. Authorization policies created by the Setup Assistant include the prefix AutoGen, such as: `AutoGen_AuthNPolicy_MAB`.

Endpoint Profiling

Endpoint profiling discovers, identifies, and determines the capabilities of all attached endpoints on your network. If you enable endpoint profiling, Cisco ISE will:

- Enable these endpoint profiling features on the **Administration > System > Deployment > Edit Node > Profiling Configuration** page.
 - DHCP
 - RADIUS
 - Network Scan (NMAP)
 - SNMP Query Probes
- Configure SNMP on the **Administration > Network Resources > Network Devices** page.

Proxy Settings

Cisco ISE uses the proxy server to download Cisco-defined posture checks and client provisioning resources required for assessing posture of endpoints and allowing personal devices on the network. If you configure these proxy settings, Cisco ISE will update the settings on the **Administration > System > Settings > Proxy** page.

Guest User Support

To support guest users, you must create a sponsor user. Cisco ISE creates a single user using the name you enter and assigns the user to the default SponsorAllAccount user identity group, which defines the user as a sponsor user. You can verify this from the **Administration > Identity Management > Identities > Users** page after setup completes.

If you add a simplified URL, Cisco ISE updates the **Portal URL** settings on the **Administration > Web Portal Management > Settings > General > Ports** page.

Support for Personal Devices

You can add a simplified URL for employees to use to access the My Devices portal, and Cisco ISE updates the **Portal URL** settings on the **Administration > Web Portal Management > Settings > General > Ports** page.

Web Portal Customizations

You can upload an image to use as a custom logo for the Sponsor, Guest, and My Devices portals. Cisco ISE also will upload the image to the **Administration > Web Portal Management > Settings > General > Portal Theme** page.

Select Network Device Types Page in Setup Assistant

Switches and Wireless Controllers

Cisco ISE adds the switches and wireless controllers to the **Administration > Network Resources > Network Devices** page, updates the SNMP settings, and adds the RADIUS shared secret to the Authentication Settings option.

Depending on the choices you made previously, you must configure the switches and wireless controllers. Click the **Wired** or **Wireless Network Diagram** links to display sample network topologies that illustrate the required configuration details.

Review and Confirm Your Choices Page in Setup Assistant

Review Your Selection

You can verify your responses to each of the questions.

Network Device Configuration

Configuration details for each configured switch and WLC display separately. Cisco ISE does not automatically update these configurations on the devices. If you want to completely replace the current device configuration, copy and paste the entire configuration. Alternatively, you can just copy the specific sections with the configuration changes you need. You can access the most current copy of the settings after exiting the Setup Assistant by choosing **Setup Assistant > View network device configuration**.

ISE Configuration

The ISE Configuration tab displays details about each setting, policy, profile, DACL, and network device added to Cisco ISE.

Task Navigators

Task Navigators provide a visual path through the configuration tasks, which span multiple pages. The linear presentation visually outlines the order in which the tasks should be completed and provides direct links to the screens where the tasks are performed. It is purely a visual map that does not retain any information about the tasks as you complete them.

You can choose from the following Task Navigators:

- 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.
- Device Registration—Configure users' devices.

Filtering Data on Listing Pages

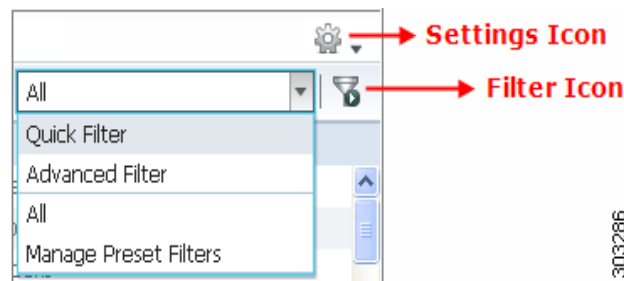
Listing pages include tools that enable you to filter and customize the displayed information:

- [Data Filters in Listing Pages, page 2-8](#)
- [Customizing the Displayed Field Attributes, page 2-9](#)
- [Filtering Data by Field Attributes Using the Quick Filter, page 2-9](#)
- [Filtering Data by Conditions Using the Advanced Filter, page 2-9](#)
- [Creating Custom Filters, page 2-10](#)

Data Filters in Listing Pages

You can customize and filter the information that displays in the listing pages using the settings and filter icons.

Figure 2-3 Data Filters Example



Customizing the Displayed Field Attributes

You can customize the field attributes displayed in the listing pages. The available and default options vary based on the specific listing page.

-
- Step 1** Click the Settings icon and choose **Columns**.
 - Step 2** Select the items to add or remove. A checkmark displays next to the selected items.
 - Step 3** Click **Close**.
-

Related Topics

[Data Filters in Listing Pages, page 2-8](#)

Filtering Data by Field Attributes Using the Quick Filter

The Quick Filter allows you to enter a value for any of the field attributes displayed in the listing page, refreshes the page, and lists only those records that match your filter criteria.

-
- Step 1** Click the **Show** drop-down list and choose **Quick Filter**.
 - Step 2** Enter search criteria in one or more of the attribute fields, and the entries that match the specified attributes display automatically.
-

Related Topics

[Data Filters in Listing Pages, page 2-8](#)

Filtering Data by Conditions Using the Advanced Filter

The Advanced Filter allows you to filter information based on specified conditions, such as, First Name = Mike and User Group = Employee. You can specify more than one condition.

-
- Step 1** Click the **Show** drop-down list and choose **Advanced Filter**.
 - Step 2** Specify search the search attributes, such as fields, operators, and values from the Filter menus.
 - Step 3** Click + to add additional conditions.
 - Step 4** Click **Go** to display the entries that match the specified attributes.
-

Related Topics

[Data Filters in Listing Pages, page 2-8](#)

Creating Custom Filters

You can create and save custom filters and modify the filter criteria in preset filters. Custom filters are not saved in the Cisco ISE database. You can only access them using the same computer and browser used to create them.

-
- Step 1** Click the **Show** drop-down list and choose **Advanced Filter**.
 - Step 2** Specify the search attributes, such as fields, operators, and values from the Filter menus.
 - Step 3** Click **+** to add additional conditions.
 - Step 4** Click **Go** to display the entries that match the specified attributes.
 - Step 5** Click the **Save** icon to save the filter.
 - Step 6** Enter a name and click **Save**. The filter now appears in the Show drop-down list.
-

Related Topics

- [Filtering Data by Conditions Using the Advanced Filter, page 2-9](#)
- [Data Filters in Listing Pages, page 2-8](#)

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, internationalization and localization support focuses on support for non-English text in UTF-8 encoding to the end-user facing portals and on selective fields in the Admin portal.

This section contains the following topics:

- [Supported Languages, page 2-10](#)
- [End-User Web Portal Localization, page 2-11](#)
- [Support for UTF-8 Character Data Entry, page 2-11](#)

Supported Languages

Cisco ISE, provides localization and internationalization support for the following languages and browser locales:

Language	Browser Locale
Chinese traditional	zh-tw
Chinese simplified	zh-cn
Czech	cs-cz
Dutch	nl-nl
English	en

Language	Browser Locale
French	fr-fr
German	de-de
Hungarian	hu-hu
Italian	it-it
Japanese	ja-jp
Korean	ko-kr
Polish	pl-pl
Portuguese (Brazil)	pt-br
Russian	ru-ru
Spanish	es-es

End-User Web Portal Localization

The Guest, Sponsor, My Devices, and Client Provisioning portals are localized into all supported languages and locales. This includes text, labels, messages, field names, and button labels. If the client browser requests a locale that is not mapped to a template in Cisco ISE, the portals display content using the English template.

Using the Admin portal, you can modify the fields used for the Guest, Sponsor, and My Devices portals for each language individually, and you can add additional languages. Currently, you cannot customize these fields for the Client Provisioning portal.

You can further 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. Cisco ISE provides the ability to upload, store, and render custom internationalized HTML pages.

**Note**

NAC and MAC agent installers and WebAgent pages are not localized.

Related Topics

- [Supported Languages, page 2-10](#)
- [Adding a Custom Language Template, page 15-4](#)
- [Customized Guest Portal, page 16-12](#)
- [Sample HTML for Custom Pages for the Guest Portal, page D-3](#)

Support for UTF-8 Character Data Entry

Cisco ISE fields that are exposed to the end user (through the Cisco NAC agent, or supplicants, or through the Sponsor, Guest, My Devices, and Client Provisioning portals) support UTF-8 character sets for all languages. UTF-8 is a multibyte-character encoding for the unicode character set, which includes many different language character sets, such as Hebrew, Sanskrit, and Arabic.

Character values are stored in UTF-8 in the administration configuration database, and the UTF-8 characters display correctly in reports and user interface components.

Related Topics

[UTF-8 Character Support in the Portals, page 2-13.](#)

UTF-8 Credential Authentication

Network access authentication supports UTF-8 username and password credentials. This includes RADIUS, EAP, RADIUS proxy, RADIUS token, and web authentication from the Guest and Administrative portal login authentications. 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 does not support UTF-8 users, hence UTF-8 authentication with RSA is not supported. Likewise, RSA servers, which are compatible with Cisco ISE 1.2, 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 Cisco 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.
- WebAgent does not support UTF-8 based rules and requirements.
- 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. You are 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.

Cisco ISE prompts and messages may not be in sync with the locale of the client operating system on which the supplicant is running. You must 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 detailed pages of report records
- Exporting and saving reports
- Viewing the Cisco ISE dashboard
- Viewing alert information
- Viewing tcpdump data

UTF-8 Character Support in the Portals

Many more character sets are supported in Cisco ISE fields (UTF-8) than are currently supported for localizations in portals and end-user messages. For example, Cisco ISE does not support right-to-left languages, such as Hebrew or Arabic, even though the character sets themselves are supported.

The following table lists the fields in the Admin and end-user portals that support UTF-8 characters for data entry and viewing, with the following limitations:

- Cisco ISE does not support administrator passwords with UTF-8 characters.
- Cisco ISE does not support UTF-8 characters in certificates.

Table 2-1 Admin Portal UTF-8 Character Fields

Admin Portal Element	UTF-8 Fields
Network access user configuration	• User name • First name • Last name • e-mail
User list	• All filter fields • Values shown on the User List page • Values shown on the left navigation quick view

Table 2-1 **Admin Portal UTF-8 Character Fields (continued)**

Admin Portal Element	UTF-8 Fields
User password policy	- Advanced > Password may not contain characters Some languages do not have uppercase or lower case alphabets. If your user password policy requires the user to enter a password with uppercase or lowercase characters, and if the user's language does not support these characters, the user cannot set a password. For the user password field to support UTF-8 characters, in the user password policy page (Administration > Identity Management > Settings > User Password Policy), you must uncheck the following options: - Lowercase alphabetic characters - Uppercase alphabetic 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 and My Devices settings	- Sponsor > Language Template: all supported languages, all fields - Guest > Language Template: all supported languages, all fields - My Devices > Language Template: all supported languages, all fields
System settings	SMTP Server > Default e-mail address
Operations > Alarms > Rule	- Criteria > User - Notification > e-mail Notification user list
Operations > Reports	- Operations > Live Authentications > Filter fields - Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	General Tools > RADIUS Authentication Troubleshooting > Username

Table 2-1 Admin Portal UTF-8 Character Fields (continued)

Admin Portal Element	UTF-8 Fields
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

UTF-8 Support Outside the User Interface

This section contains the areas outside the Cisco 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. You can download debug logs containing raw UTF-8 data that can be viewed with a UTF-8 supported viewer.

ACS Migration UTF-8 Support

Cisco ISE, allows for the migration of ACS UTF-8 configuration objects and values. Migration of some UTF-8 objects may not be supported by Cisco 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. You must convert unreadable UTF-8 values (that are migrated from ACS) into ASCII text.

Related Topics

[Cisco Identity Services Engine, Release 1.2 Migration Tool Guide.](#)

Support for Importing and Exporting UTF-8 Values

The Admin and Sponsor portals support plain text and .csv files with UTF-8 values to be used when importing user account details. Exported files are provided as csv files.

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.

Related Topics

[Cisco Identity Services Engine API Reference Guide, Release 1.2.](#)

UTF-8 Support for Identity Stores Authorization Data

Cisco ISE allows Active Directory and LDAP to use UTF- 8 data in authorization policies for policy processing.

Admin Features Limited by Role-Based Access Control Policies

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.

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.

Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any page that it can access. Read-only functionality is unavailable for any administrative access.

Related Topics

[Chapter 6, “Managing Administrators and Admin Access Policies”](#)



PART 2

Deploying Cisco ISE Nodes



Setting Up Cisco ISE in a Distributed Environment

Cisco ISE has a highly available and scalable architecture that supports standalone and distributed deployments. In a distributed environment, you configure one primary Administration node to manage the secondary ISE nodes that are deployed onto the network.

Cisco 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 personas, roles, and services that constitute Cisco ISE, and how to configure Cisco ISE nodes.

For information about the Cisco ISE deployment scenarios, refer to the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.2](#).

This chapter contains the following topics:

- [Cisco ISE Deployment Terminology, page 3-1](#)
- [Personas in Distributed Cisco ISE Deployments, page 3-2](#)
- [Cisco ISE Distributed Deployment, page 3-7](#)
- [Configuring a Cisco ISE Node, page 3-11](#)
- [Registering an Inline Posture Node, page 3-14](#)
- [Viewing Nodes in a Deployment, page 3-15](#)
- [Synchronizing Primary and Secondary Cisco ISE Nodes, page 3-15](#)
- [Creating a Policy Service Node Group, page 3-16](#)
- [Changing Node Personas and Services, page 3-17](#)
- [Promoting Secondary Administration Node To Primary, page 3-17](#)
- [Configuring Monitoring Nodes for Automatic Failover, page 3-18](#)
- [Removing a Node from Deployment, page 3-19](#)
- [Changing the Hostname or IP Address of a Standalone Cisco ISE Node, page 3-19](#)
- [Replacing the Cisco ISE Appliance Hardware, page 3-20](#)

Cisco ISE Deployment Terminology

The following terms are commonly used when discussing Cisco ISE deployment scenarios:

- **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.
- **Persona**—The persona or personas of a node determine the services provided by a node. An Cisco ISE node can assume any of the following personas: Administration, Policy Service, Monitoring, and Inline Posture. A Cisco ISE node can assume the Administration, Policy Service, and Monitoring personas. The Inline Posture persona requires a dedicated Cisco ISE node. The menu options that are available through the Admin portal are dependent on the role and personas that an Cisco ISE node assumes.
- **Deployment Model**—Determines if your deployment is distributed, standalone, or high availability in standalone, which is a basic two-node deployment.

Related Topics

[Menu Options Available on Primary and Secondary Nodes, page 3-10](#)

Personas in Distributed Cisco ISE Deployments

A Cisco ISE node can assume any of the following personas:

- [Administration Node](#)
- [Policy Service Node](#)
- [Monitoring Node](#)
- [Inline Posture Node](#)

A Cisco ISE node can provide various services based on the persona that it assumes. Each node in a deployment, with the exception of the Inline Posture node, can assume the Administration, Policy Service, and Monitoring personas. In a distributed deployment, you can have the following combination of nodes on your network:

- Primary and secondary Administration nodes for high availability
- A pair of Monitoring nodes for automatic failover
- One or more Policy Service nodes for session failover
- A pair of Inline Posture nodes for high availability

You need to add Canonical Name (CNAME) record of the ISE hostname to the DNS. Ensure that you create CNAME RR along with the A record for each Cisco ISE node. If CNAME record is not created, it might result in the alarm ‘DNS Resolution failed for CNAME <hostname of the node>’.

Administration Node

A Cisco ISE node with the Administration persona allows you to perform all administrative operations on Cisco ISE. It handles all system-related 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.

High Availability in Administration Nodes

In a high-availability configuration, the primary Administration node is in the active state to which all configuration changes are made. The secondary Administration node is in the standby state, and will receive all configuration updates from the primary Administration node. Therefore, it will always have a complete copy of the configuration from the primary Administration node.

If the primary Administration node goes down, you must log in to the user interface of the secondary Administration node and manually promote the secondary Administration node. There is no automatic failover for the Administration persona.

You can use Cisco ISE appliances (ISE 3300 series or SNS 3400 series) or virtual machines or a combination of both to set up a primary-secondary pair of Administration nodes. However, you must ensure that the virtual machine's hardware specification is comparable with the Cisco ISE appliance. See [VMware Appliance Specifications for a Production Environment](#) for more details.

When the primary Administration 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 in to the sponsor portal before the primary Administration node went offline, will not be able to log in to the sponsor portal until a secondary Administration node is promoted or the primary Administration node becomes available.

At least one node in your distributed setup should assume the Administration persona.

Policy Service Node

A Cisco ISE node with the Policy Service persona 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 node in a distributed deployment. All Policy Service nodes that reside behind a load balancer 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.

At least one node in your distributed setup should assume the Policy Service persona.

High Availability in Policy Service Nodes

In distributed deployments, you might have multiple Policy Service nodes located behind a load balancer to distribute the requests evenly. The load balancer distributes the requests to the functional nodes behind it. Also, to detect node failure and to reset sessions in pending state on the failed node, two or more Policy Service nodes can be placed in the same node group. When a node that belongs to a node group fails, another node in the same node group issues a Change of Authorization (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 node will not be automatically reset.

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 F-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 for all the nodes to be 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. 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 Nodes

The heartbeat functionality in Cisco ISE handles session failover in Policy Service nodes. When a Policy Service node that has a few active sessions fails, the endpoints are stuck in an intermediate state. Even if the posture agent detects that the Policy Service node that it has been communicating with has failed, it cannot re-initiate authorization.

If the Policy Service 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, the sessions are handled by another Policy Service node that is available using RADIUS load balancing. The session failover does not automatically move the sessions over from a Policy Service node that has gone down to one that is available, but issues a CoA to achieve that.

Machine Access Restriction in Policy Service Nodes

The Policy Service 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 nodes that fails, then another Policy Service node in the deployment handles the user authentication. However, the user authentication then fails because the second Policy Service node does not have the host authentication information in its MAR cache.

Number of Nodes in a Policy Service 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 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 node failures.

You can have a maximum of 10 Policy Service nodes in a node group cluster.

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.

Monitoring Node

A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the administration and Policy Service 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 nodes collect log messages. In case the primary Monitoring node goes down, the secondary Monitoring node automatically becomes the primary Monitoring node.

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.

You can access the Monitoring menu from the primary Administration node and the primary Monitoring node in your deployment.

Automatic Failover in Monitoring Nodes

The term automatic failover is used because high availability is not supported on Monitoring nodes in the true sense. For Monitoring nodes, operation audit data is duplicated by the Policy Service node(s), which then sends copies to both the primary and secondary Monitoring nodes.

**Note**

Monitoring is served from the primary (active) Monitoring node. Monitoring data is only served from the secondary (standby) Monitoring node when the active node is down. The secondary monitoring node is read-only.

Automatic Failover Process

When a primary Monitoring node goes down, the secondary Monitoring node takes over all monitoring and troubleshooting information. The secondary node provides read-only capabilities.

To convert the existing secondary node to an active primary 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 node will resume its role after it comes back up.

**Caution**

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.

Active-Standby Pair of Monitoring Nodes

You can specify two Monitoring nodes on an ISE network and create an active-standby pair. When you register a secondary Monitoring node, we recommend that you back up the primary Monitoring node and then restore the data to the new secondary Monitoring node. This ensures that the history of the primary Monitoring node is in sync with the new secondary node as new changes are replicated. Once the active-standby pair is defined, the following rules apply:

- All changes must be made on the primary Monitoring node. The secondary node is read-only.
- 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 Cisco ISE dashboard is the main entry point for monitoring and troubleshooting. Monitoring information is displayed on the dashboard from the primary Monitoring 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 Cisco ISE node backup process. You must configure repositories for backup and data purging on both the primary and secondary Monitoring nodes, and use the same repositories for each.

Monitoring Node Failover Scenarios

The following scenarios apply to the active-standby or single node configurations corresponding to the monitoring nodes:

- In an active-standby configuration of the monitoring nodes, the Administrative PAP always points to the active monitoring node to collect the monitoring data. After the active monitoring node fails, the Administrative PAP points to the standby monitoring node. The failover from the active monitoring node to the standby monitoring node happens within a time period of 1 to 10 seconds.
However, after the active node fails, the standby node does not become the active node. In case the active node comes back up, the Administrative node starts collecting the monitoring data again from the resumed active node.
- During the time that the active monitoring node is down, if you want to promote the standby monitoring node to active status, you must de-register the existing active monitoring node. When you de-register the existing active monitoring node, the standby node becomes the active monitoring node and the Administrative PAP automatically starts pointing to the newly promoted active node.
- In an active-standby pair, if you choose to de-register the standby monitoring node from the deployment or if the standby monitoring node goes down, the existing active monitoring node still retains the active node status. The Administrative PAP points to the existing active node for data collection.
- If there is only one monitoring node in the ISE deployment, then that node acts as the active monitoring node that provides monitoring data to the Administrative PAP. However, when you register a new monitoring node and make it the active node in the deployment, the existing active monitoring node automatically becomes the standby node. The Administrative PAP begins to point to the newly registered active monitoring node for collecting monitoring data.

Related Topics

- [Performing an On-Demand Backup, page 12-4](#)
- [Restoration of Monitoring Database, page 12-10](#)

Inline Posture Node

An Inline Posture node is a gatekeeping node that is positioned behind network access devices such as Wireless LAN Controllers (WLC) and VPN concentrators on the network. The Inline Posture node 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.

The Inline Posture node must be a dedicated node. It must be dedicated solely for inline posture service, and cannot operate concurrently with other Cisco 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 node that offers administration service, or a Policy Service node that offers network access, posture, profile, and guest services, or a Monitoring node that offers monitoring and troubleshooting services for a Cisco ISE network.

The Inline Posture persona is not supported on the Cisco ISE 3495 platform. Ensure that you install The Inline Posture persona on any one of the following supported platforms: Cisco ISE 3315, Cisco ISE 3355, Cisco ISE 3395, or Cisco ISE 3415.

Related Topics

[Chapter 4, “Setting Up Inline Posture”](#)

Inline Posture Node Installation

You must download the Inline Posture 1.2 ISO image from Cisco.com and install it on any of the supported platforms. You must then configure certificates through the command-line interface (CLI). You can then register this node from the Admin portal.



Note

You cannot access the web-based user interface of the Inline Posture nodes. You can configure them only from the primary Administration node.

After you install and set up the Inline Posture application, you must configure certificates before you can register the Inline Posture nodes. See *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2* for more information.

Cisco ISE Distributed Deployment

A deployment that has more than one Cisco ISE node is called a distributed deployment. To support failover and to improve performance, you can set up your deployment with multiple Cisco ISE nodes in a distributed fashion. In Cisco ISE distributed deployment, administration and monitoring activities are centralized, and processing is distributed across the Policy Service nodes. Depending on your performance needs, you can scale your deployment. Each Cisco ISE node in a deployment can assume any of the following personas: Administration, Policy Service, and Monitoring. The Inline Posture node cannot assume any other persona, due to its specialized nature. The Inline Posture node must be a dedicated node.

This section contains the following topics:

- [Cisco ISE Deployment Setup, page 3-8](#)
- [Data Replication from Primary to Secondary ISE Nodes, page 3-8](#)
- [Cisco ISE Node Deregistration, page 3-8](#)
- [Automatic Restart of the Cisco ISE Application Server, page 3-9](#)
- [Guidelines for Setting Up a Distributed Deployment, page 3-9](#)
- [Menu Options Available on Primary and Secondary Nodes, page 3-10](#)

Cisco ISE Deployment Setup

After you install Cisco ISE on all your nodes, as described in [Cisco Identity Services Engine Hardware Installation Guide, Release 1.2](#), the nodes come up in a standalone state. You must then define one node as your primary Administration node. While defining your primary Administration node, you must enable the Administration and Monitoring personas on that node. You can optionally enable the Policy Service persona on the primary Administration node. After you complete the task of defining personas on the primary Administration node, you can then register other secondary nodes to the primary Administration node and define personas for the secondary nodes.

All Cisco ISE system and functionality-related configurations should be done only on the primary Administration node. The configuration changes that you perform on the primary Administration node are replicated to all the secondary nodes in your deployment.

There must be at least one Monitoring node in a distributed deployment. At the time of configuring your primary Administration node, you must enable the Monitoring persona. After you register a secondary Monitoring node in your deployment, you can edit the primary Administration node and disable the Monitoring persona, if required.

Data Replication from Primary to Secondary ISE Nodes

When you register an Cisco 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 Cisco ISE configuration data from the primary to the secondary nodes. Replication ensures consistency among the configuration data present in all Cisco ISE nodes that are part of your deployment.

A full replication typically occurs when you first register an ISE node as a secondary node. 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 node are reflected in the secondary nodes. The process of replication ensures that all Cisco ISE nodes in a deployment are in sync. You can view the status of replication in the Node Status column from the deployment pages of the Cisco ISE Admin portal. When you register a Cisco ISE node as a secondary node or perform a manual synchronization with the primary Administration node, the node status shows an orange icon indicating that the requested action is in progress. Once it is complete, the node status turns green indicating that the secondary node is synchronized with the primary Administration node. After the node status turns green, it takes about five minutes for the Cisco ISE application server to restart and run to complete the secondary ISE node configuration.

Cisco ISE Node Deregistration

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the primary Administration 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 standalone node.

**Note**

You cannot deregister a primary Administration node.

Related Topics

[Chapter 4, “Setting Up Inline Posture”](#)

Automatic Restart of the Cisco ISE Application Server

The application server in an Cisco ISE node restarts which causes a delay when you make any of the following changes:

- Register a node (Standalone to Secondary)
- Deregister a node (Secondary to Standalone)
- Change a primary node to Standalone (if no other nodes are registered with it; Primary to Standalone)
- Promote an Administration node (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 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

Guidelines for Setting Up a Distributed Deployment

Read the following statements carefully before you set up Cisco ISE in a distributed environment.

- Choose a node type—ISE node or Inline Posture node. For Administration, Policy Service, and Monitoring capabilities, you must choose an ISE node. For Inline Posture service, you must choose the Inline Posture node.
- Choose the same Network Time Protocol (NTP) server for all the nodes—To avoid timezone issues among the nodes, you must provide the same NTP server name during the setup of each node. This setting ensures that the reports and logs from the various nodes in your deployment are always synchronized with timestamps.
- Configure the Cisco ISE Admin password when you install Cisco ISE. The previous Cisco ISE Admin default login credentials (admin/cisco) are no longer valid. Use the username and password that was created during the initial setup or the current password if it was changed later.
- Configure the Domain Name System (DNS) server—Enter the IP addresses and fully qualified domain names (FQDNs) of all the Cisco ISE nodes that are part of your distributed deployment in the DNS server. Otherwise, node registration will fail.
- Configure the Reverse DNS lookup for all Cisco ISE nodes in your distributed deployment in the DNS server. Otherwise, you may run into deployment related issues when registering Cisco ISE nodes, and restarting Cisco ISE nodes.
- (Optional) Deregister a secondary Cisco ISE node from the primary Administration node to uninstall Cisco ISE from it.
- Back up the primary Monitoring node, and restore the data to the new secondary Monitoring node. This ensures that the history of the primary Monitoring node is in sync with the new secondary node as new changes are replicated.
- Ensure that the primary Administration node and the standalone node that you are about to register as a secondary node are running the same version of Cisco ISE.
- Ensure that the database passwords of the primary and secondary nodes are the same. If these passwords are set differently 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`

Refer to *Cisco Identity Services Engine CLI Reference Guide, Release 1.2* for more details on how to use Cisco ISE CLI commands.

Related Topics

- [Performing an On-Demand Backup, page 12-4](#)
- [Restoration of Monitoring Database, page 12-10](#)

Menu Options Available on Primary and Secondary Nodes

Cisco ISE nodes provide you an Admin portal that you can use to perform your tasks. The menu options available in Cisco ISE nodes that are part of a distributed deployment depend on the personas that are enabled on them. You must perform all administration and monitoring activities through the primary Administration node. For some tasks, you must use the secondary nodes. Therefore, the user interface of the secondary nodes provides limited menu options based on the personas that are enabled on them.

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 nodes and Active Monitoring node will be available on that node.

The following table lists the menu options that are available on Cisco ISE nodes that assume different personas.

Table 3-1 *Cisco ISE Nodes and Available Menu Options*

Cisco ISE Node	Available Menu Options
All nodes	• 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 node	All menus and submenus.
Active Monitoring node	• Home and operations menus. • Provides redundant access to monitoring data that can be accessed from both the Primary and the Active Monitoring nodes.

Table 3-1 Cisco ISE Nodes and Available Menu Options (continued)

Cisco ISE Node	Available Menu Options
Policy Service nodes	Option to join, leave, and test Active Directory connection. Each Policy Service node must be separately joined to the Active Directory domain. You must first define the domain information and join the primary Administration node to the Active Directory domain. Then, join the other Policy Service nodes to the Active Directory domain individually.
Secondary Administration node	Option to promote the secondary Administration node to become the primary Administration node. Note After you have registered your secondary nodes to your primary Administration node, while logging in to the Admin portal of any of the secondary nodes, you must use the login credentials of the primary Administration node.

Configuring a Cisco ISE Node

After you install a Cisco ISE node, all the default services provided by the Administration, Policy Service, and Monitoring personas run on it. This node will be in a standalone state. You must log in to the Admin portal of the Cisco ISE node to configure it. You cannot edit the personas or services of a standalone Cisco ISE node. You can, however, edit the personas and services of the primary and secondary Cisco ISE nodes. You must first configure a primary ISE node and then register secondary ISE nodes to the primary ISE node.

If you are logging in to the node for the first time, you must change the default administrator password and install a valid license.

If you are logging in to the secondary Administration node to promote it as your primary Administration node, see [“Promoting Secondary Administration Node To Primary”](#) section on page 3-17.

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 reimaged the appliance, make changes, and configure the details during the initial deployment.

Before You Begin

You should have a basic understanding of how distributed deployments are set up in Cisco ISE. Read the [Guidelines for Setting Up a Distributed Deployment](#), page 3-9.

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Check the check box next to the Cisco ISE node that you want to configure, and click **Edit**.
The Node Edit page appears with a list of fields as described in [Deployment Settings](#).
-

What To Do Next

1. [Configuring a Primary Administration Node, page 3-12](#)
2. [Registering a Secondary Cisco ISE Node, page 3-12](#)

Related Topics

- [Cisco ISE Distributed Deployment, page 3-7](#)
- [Guidelines for Setting Up a Distributed Deployment, page 3-9](#)
- [Configuring Monitoring Nodes for Automatic Failover, page 3-18](#)
- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7](#)

Configuring a Primary Administration Node

To set up a distributed deployment, you must first configure a Cisco ISE node as your primary Administration node.

-
- Step 1** Choose **Administration > System > Deployment**.
- The Register button will be disabled initially. To enable this button, you must configure a primary Administration node.
- Step 2** Check the check box next to the current node, and click **Edit**.
- Step 3** Click **Make Primary** to configure your primary Administration node.
- Step 4** Enter data on the General Settings tab as described in [Deployment Settings](#).
- Step 5** Click **Save** to save the node configuration.
-

What To Do Next

1. To enable the Profiler service and configure the probes, see [Configuring Probes per Cisco ISE Node, page 21-13](#).
2. To add secondary nodes to your deployment, you must successfully register a secondary node as described in the [Registering a Secondary Cisco ISE Node, page 3-12](#).

Related Topics

[Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7](#)

Registering a Secondary Cisco ISE Node

We recommend that you decide on the type of node (Cisco ISE or Inline Posture) 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.

If you plan to deploy two Administration nodes for high availability, register the secondary Administration node before you register the other secondary nodes. If you register the nodes in this sequence, you do not have to restart the secondary ISE nodes after you promote the secondary Administration node as your primary.

If you plan to deploy multiple Policy Service nodes running Session services with mutual failover among these nodes, place the Policy Service nodes in a node group. You must create the node group before you register the nodes. See [Creating a Policy Service Node Group, page 3-16](#) for more information.

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.

You can view all the configuration changes that you make from the Deployment page of the primary Administration node. However, expect a delay of 5 minutes for your changes to take effect and appear on the Deployment page.

Before You Begin

Ensure that the primary node's Certificate Trust List (CTL) has the appropriate certificate authority (CA) certificates to validate the HTTPS certificate of the secondary node that you are going to register.

The certificates that you import into the CTL of the primary Administration node are replicated to the secondary nodes.

Also, after you register the secondary node to the primary node, if you change the HTTPS certificate on the secondary node, you must import the appropriate CA certificates into the CTL of the primary node.

-
- Step 1** Log in to the primary Administration node.
 - Step 2** Choose **Administration > System > Deployment**.
 - Step 3** Choose **Register > Register an Cisco ISE Node** to register a secondary Cisco ISE node.
 - Step 4** Enter the DNS-resolvable hostname of the secondary Cisco ISE node.



Note If you are using the hostname while registering the Cisco ISE node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com*, must be DNS-resolvable from the primary Administration node. Otherwise, node registration fails. You must have previously defined the IP address and the FQDN of the secondary node in the DNS server.

- Step 5** Enter a UI-based administrator credential for the standalone node in the Username and Password fields.
 - Step 6** Click **Next**.

Cisco ISE contacts the secondary node, obtains some basic information such as the hostname, default gateway, and so on, and displays it.

If you have chosen to register a secondary Cisco ISE node, you can edit the configuration of the secondary node.

If you have chosen to register a secondary Inline Posture node, no additional configuration needs to be performed at this point.
 - Step 7** Click **Save**.
-

Result

After a secondary node is registered successfully, you will receive an alarm on your primary Administration node that confirms a successful node registration. If the secondary node fails to register with the primary Administration 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 in to the user interface of the secondary node and perform any of the operations listed in [Menu Options Available on Primary and Secondary Nodes](#).

**Note**

In addition to the existing Primary node in the deployment, when you successfully register a new node, no alarm corresponding to the newly registered node is displayed. The Configuration Changed alarms reflect information corresponding to the newly registered nodes. You can use this information to ascertain the successful registration of the new node.

What To Do Next

- 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 [“Specifying System Time and NTP Server Settings” section on page 5-3](#) for information on how to synchronize the system time.
- To configure for high availability, you must complete the tasks described in the following sections:
 - [Promoting Secondary Administration Node To Primary, page 3-17](#)
 - [Configuring Monitoring Nodes for Automatic Failover, page 3-18](#)
- To add an Inline Posture node to your deployment, follow the instructions as described in the [“Setting Up Inline Posture” section on page 4-1](#).

Related Topics

- [Deployment Settings, page A-1](#)
- [Installation of CA Certificates for Cisco ISE Inter-node Communication, page 8-29](#)

Registering an Inline Posture Node

We recommend that you decide on the type of node (Cisco ISE or Inline Posture) 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.

Before You Begin

- Ensure that the primary node’s Certificate Trust List (CTL) has the appropriate certificate authority (CA) certificates to validate the HTTPS certificate of the secondary node that you are going to register.
- After you register the secondary node to the primary node, if you change the HTTPS certificate on the secondary node, you must import the appropriate CA certificates into the CTL of the primary node.

-
- Step 1** Log in to the primary Administration node.
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** Click **Deployment** from the navigation pane on the left.
- Step 4** Choose **Register > Register an Inline Posture Node** to register a secondary Inline Posture node.
-

Related Topics

- [Deployment Settings, page A-1](#)
- [Installation of CA Certificates for Cisco ISE Inter-node Communication, page 8-29](#)
- [Chapter 4, “Setting Up Inline Posture.”](#)

Viewing Nodes in a Deployment

In the Deployment Nodes page, you can view all the Cisco ISE nodes, primary and secondary, that are part of your deployment.

-
- Step 1** Log in to the primary Cisco ISE Admin portal.
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** Click **Deployment** from the navigation pane on the left.
- Step 4** Refer to [Deployment Settings](#) for a description of the fields in the Deployment Nodes page.

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 node. Click the Register button to register a Cisco ISE or Inline Posture node.
 - Initiate a full database replication from the primary to the selected secondary nodes.
 - Deregister one or more secondary nodes.
-

Synchronizing Primary and Secondary Cisco ISE Nodes

You can make configuration changes to Cisco ISE only through the primary Administration node. The configuration changes get replicated to all the secondary Cisco ISE Nodes. If, for some reason, this replication does not occur properly, you can manually synchronize the secondary Administration nodes with the primary Administration node.

Before You Begin

You must click the Syncup button to force a full replication if the Sync Status is set to Out of Sync or if the Replication Status is Failed or Disabled.

-
- Step 1** Log in to the primary Cisco ISE Admin portal.
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** Check the check box next to the node that you want to synchronize with the primary Administration node, and click **Syncup** to force a full database replication.
-

Creating a Policy Service Node Group

You can deploy more than one Policy Service node for load balancing to distribute requests evenly. To detect node failure and to reset sessions in a pending state on the failed node, two or more Policy Service nodes can be placed in the same node group. You must create a node group before you can add a node to it.

You can create, edit, and delete Policy Service node groups from the Deployment pages of the Cisco ISE Admin portal.

Before You Begin:

- Ensure that all the nodes that are going to be part of a node group are Layer 2 adjacent, which means they are on the same subnet, or connected over a routed LAN network that supports IP multicast.
- 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. Multicast over Layer 3 connections is also supported, but requires proper IP multicast configuration on all switches that connect members of the same node group. For simplicity and increased availability, we recommend that all nodes in a node group be Layer 2 adjacent.
- Ensure that node group members can communicate over UDP/45588, UDP/45590, and TCP/7802.
- Ensure that node groups do not have the same multicast address.
- Ensure that the multicast address that you assign to a node group is not 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 through 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>.

-
- Step 1** Choose **Administration > System > Deployment**.
 - Step 2** Click the **action** icon, and then click **Create Node Group**.
 - Step 3** Enter a unique name for your node group.
 - Step 4** (Optional) Enter a description for your node group.
 - Step 5** Enter a unique multicast address, which is used to communicate between nodes in a group to monitor the health of the nodes and for session cleanup. The multicast address must be between 224.0.0.1 and 239.255.255.255.
 - Step 6** Click **Submit** to save the node group.
-

Result

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.

What To Do Next

- To add a node to a node group, you must edit the node by choosing the node group from the Member of Node Group drop-down list.
- To remove a node from a node group, you must edit the node by choosing <none> from the Member of Node Group drop-down list.

Related Topics

- [Deployment Settings, page A-1](#)
- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-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.

Before You Begin

When you enable or disable any of the services that run on a Policy Service node or make any changes to a Policy Service node, you will be restarting the application server processes on which these services run. Expect a delay while these services restart.

-
- Step 1** Log in to the primary Administration node.
 - Step 2** Choose **Administration > System > Deployment**.
 - Step 3** Check the check box next to the node whose personas or services you want to change, and then click **Edit**.
 - Step 4** Choose the personas and services that you want.
 - Step 5** Click **Save**.
 - Step 6** Verify receipt of an alarm on your primary Administration node to confirm the persona or service change. If the persona or service change is not saved successfully, an alarm is not generated.
-

Related Topics

- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7](#)
- [Lost Monitoring and Troubleshooting Data After Registering Policy Service Node to Administration Node, page G-13](#)

Promoting Secondary Administration Node To Primary

If the primary Administration node fails, you must manually promote the secondary Administration node to become the new primary node.

If the node that was originally the primary Administration node comes back up, it will become a secondary Administration node. In the Edit Node page of a secondary node, you cannot modify the personas or services because the options are disabled. You have to log in to the Admin portal to make changes.

Before You Begin

Ensure that you have a second Cisco ISE node configured with the Administration persona to promote as your primary Administration node.

-
- Step 1** Log in to the user interface of the secondary Administration node.
 - Step 2** Choose **Administration > System > Deployment**.

Step 3 In the Edit Node page, click **Promote to Primary**.



Note You can only promote a secondary Administration node to become a primary Administration node. Cisco ISE nodes that assume only the Policy Service or Monitoring persona, or both, cannot be promoted to a primary Administration node.

Step 4 Click **Save**.

Step 5 Restart the secondary Cisco ISE nodes that were registered with the original primary Administration node before you registered the secondary Administration node.

For example, if you registered a secondary Administration node (the new primary) after you registered secondary Cisco ISE Policy Service and Monitoring nodes, then you must restart the secondary Cisco ISE nodes that were registered before the secondary Administration node was registered.

What To Do Next

After you promote your secondary Administration node to become the primary Administration node, you must reconfigure your scheduled Cisco ISE backups in the newly promoted primary Administration node because scheduled backups are not replicated from the primary to secondary Administration node. See [Scheduling a Backup, page 12-5](#) for more information.

Configuring Monitoring Nodes for Automatic Failover

If you have two Monitoring nodes in a deployment, you can configure a primary-secondary pair for automatic failover to avoid downtime in the Cisco ISE Monitoring service. A primary-secondary pair ensures that a secondary Monitoring node automatically provides monitoring should the primary node fail.

Before You Begin

- Before you can configure Monitoring nodes for automatic failover, they must be registered as Cisco ISE nodes. This procedure is described in [Guidelines for Setting Up a Distributed Deployment, page 3-9](#) and [Configuring a Cisco ISE Node, page 3-11](#).
- You must 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 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 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 node using the **repository** command in the system CLI. For more information, see [Back Up and Restore of the Monitoring Database, page 25-29](#) and the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).



Caution

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.

Before You Begin

From the Cisco ISE dashboard, verify that the Monitoring nodes are ready. The System Summary dashlet shows the Monitoring nodes with a green check mark to the left when their services are ready.

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** In the Deployment Nodes page, check the check box next to the Monitoring node that you want to specify as active, and click **Edit**.
- Step 3** Click the **General Settings** tab and choose **Primary** from the **Role** drop-down list.
- When you choose a Monitoring node as primary, the other Monitoring node automatically becomes secondary. In the case of a standalone deployment, primary and secondary role configuration is disabled.
- Step 4** Click **Save**. The active and standby nodes restart.
-

Removing a Node from Deployment

To remove a node from a deployment, you must deregister it. The deregistered node becomes a standalone Cisco ISE node. It retains the last configuration that it received from the primary Administration node and assumes the default personas of a standalone node that are Administration, Policy Service, and Monitoring. If you deregister a Monitoring node, this node will no longer be a syslog target.

You can view these changes from the Deployment page of the primary Administration node. However, expect a delay of 5 minutes for the changes to take effect and appear on the Deployment page.

Before You Begin

Before you remove any secondary node from a deployment, perform a backup of Cisco ISE configuration, which you can then restore later on, if needed.

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Check the check box next to the secondary node that you want to remove, and then click **Deregister**.
- Step 3** Click **OK**.
- Step 4** Verify receipt of an alarm on your primary Administration node to confirm that the secondary node is deregistered successfully. If the secondary node fails to deregister from the primary Administration node, the alarm is not generated.
-

Related Topics

[Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7](#)

Changing the Hostname or IP Address of a Standalone Cisco ISE Node

You can change the hostname, IP address, or domain name of standalone Cisco ISE nodes.

Before You Begin

If the Cisco ISE node is part of a distributed deployment, you must remove it from the deployment and ensure that it is a standalone node.

-
- Step 1** Change the hostname or IP address of the Cisco ISE node using the **hostname**, **ip address**, or **ip domain-name** command from the Cisco ISE CLI.
- Step 2** Reset the Cisco ISE application configuration using the **application stop ise** command from the Cisco ISE CLI to restart all the services.
- Step 3** Register the Cisco ISE node to the primary Administration node if it part of a distributed deployment.



Note If you are using the hostname while registering the Cisco ISE node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, *abc.xyz.com* must be DNS-resolvable from the primary Administration node. Otherwise, node registration fails. You must enter the IP addresses and FQDNs of the Cisco ISE nodes that are part of your distributed deployment in the DNS server.

After you register the Cisco ISE node as a secondary node, the primary Administration node replicates the change in the IP address, hostname, or domain name to the other Cisco ISE nodes in your deployment.

Related Topics

- [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#)
- [Removing a Node from Deployment, page 3-19](#)
- [Registering a Secondary Cisco ISE Node, page 3-12](#)

Replacing the Cisco ISE Appliance Hardware

You should replace the Cisco ISE appliance hardware only if there is an issue with the hardware. For any software issues, you can reimage the appliance and reinstall the Cisco ISE software.

-
- Step 1** Re-image or re-install the Cisco ISE software on the new nodes. Follow the steps 2 - 4, as described in [Recovery of Lost Nodes in Standalone and Distributed Deployments, page 12-14](#).
- Step 2** Register the new node as a secondary server with the primary Administration node.
-

Related Topics

- [Removing a Node from Deployment, page 3-19](#)
- [Registering a Secondary Cisco ISE Node, page 3-12](#)
- [Configuring a Cisco ISE Node, page 3-11](#)



Setting Up Inline Posture

This chapter describes how to set up and configure Inline Posture node in standalone mode, or as a high availability pair, and contains the following topics:

- [Role of Inline Posture Node in a Cisco ISE Deployment, page 4-1](#)
- [Best Practices for Inline Posture Deployment, page 4-9](#)
- [Inline Posture Node Guidelines, page 4-11](#)
- [Inline Posture Node Authorization, page 4-12](#)
- [Deploying an Inline Posture Node, page 4-13](#)
- [Configuring a High-Availability Pair, page 4-19](#)
- [Configuring Inline Posture Node as RADIUS Client in Administration Node, page 4-20](#)
- [Removing an Inline Posture Node from Deployment, page 4-21](#)
- [Health of an Inline Posture Node, page 4-22](#)
- [Remote Access VPN Use Case, page 4-22](#)
- [Collecting Inline Posture Node Logs, page 4-24](#)
- [Kclick process in Inline Posture Node, page 4-24](#)

Role of Inline Posture Node in a Cisco ISE Deployment

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 requests, such as wireless LAN controllers (WLCs) and VPN devices.

After the initial authentication of a client using the EAP/802.1x and RADIUS protocols, the client must 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, an Inline Posture node is responsible for the policy enforcement and CoA that these devices are unable to accommodate.

Inline Posture Policy Enforcement

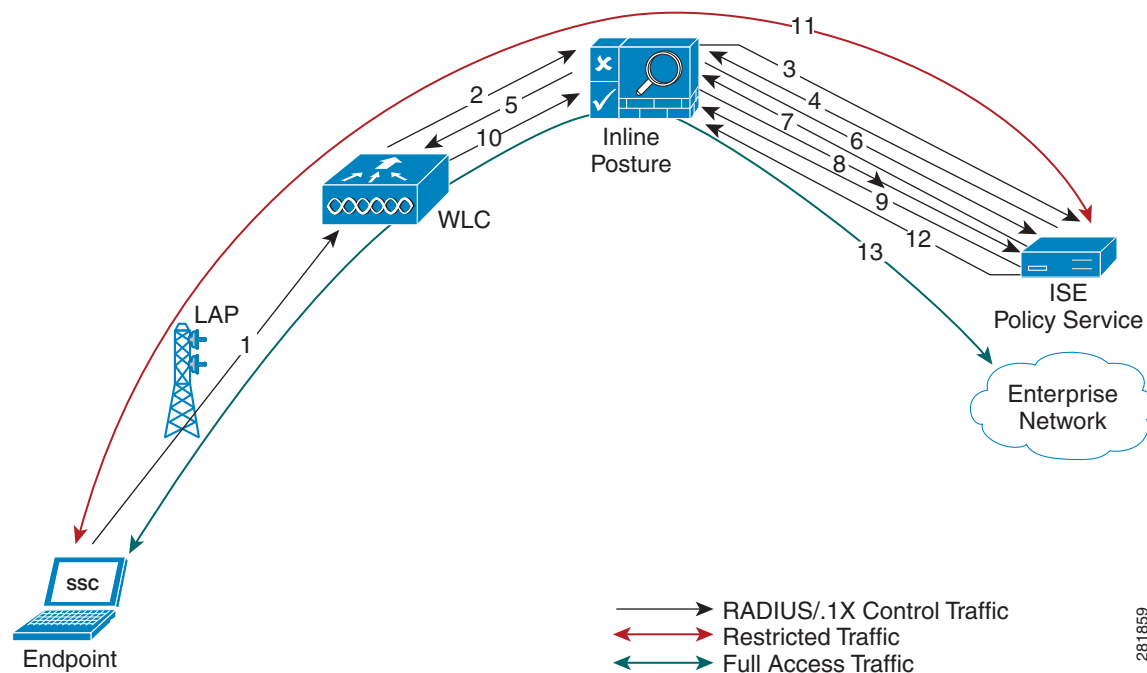
Inline Posture uses RADIUS proxy and URL redirect capabilities in the control plane to manage data plane traffic for endpoints. As a RADIUS proxy, Inline Posture is able to tap into RADIUS sessions between network access devices (NADs) and RADIUS servers. NADs can open full gate to client traffic. However, Inline Posture opens only enough to allow limited traffic from clients. The restricted bandwidth allows clients the ability to have an agent provisioned, posture assessed, and remediation completed. This restriction is accomplished by downloading and installing Downloadable Access Control Lists (DACLS) that are tailored for specific client flows. See [Downloadable ACLs](#), page 20-11.

When the client is compliant, a CoA is sent to the Inline Posture node by the Policy Service 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, and therefore duplicate downloads are not necessary as long as the DACL content does not change in the Cisco ISE servers.

Inline Posture Policy Enforcement Flow

Figure 4-1 illustrates the Inline Posture policy enforcement process and shows the flow for WLC enforcement for traffic to the Policy Service node. The access steps are similar for an inline deployment with VPN gateways.

Figure 4-1 *Inline Posture Policy Enforcement Flow*



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, which is usually the Policy Service node (in this illustration, the RADIUS Access-Request message is sent to the Inline Posture node).

3. The 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 the Inline Posture node to send an Authorization-Only request to the Policy Service node to retrieve the profile for the session.
7. The Policy Service node returns an Access-Accept message, along with the necessary Inline Posture node profile.
8. If the access control list (ACL) that is defined in the profile is not already available on the Inline Posture node, the Inline Posture node downloads it from the Policy Service 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 node 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, which is 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 access only 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 node initiates a RADIUS (CoA) with the new profile. Therefore, 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 the Inline Posture node.

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 example, there may be an employee, executive, and guest user 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 during 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 Inline Posture deployment:

- **Trusted**—The interface that talks to the Policy Service node and other trusted devices *inside* the Cisco ISE network. The trusted interface is always designated to Eth0 interface.
- **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 interface.

Dedicated Nodes Required for Inline Posture

Unlike other personas, 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 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. You can also have as many active-standby pairs or standalone Inline Posture nodes as needed, up to the limit of supported endpoints for your deployment.

For information on Cisco ISE distributed deployments, see [Chapter 3, “Setting Up Cisco ISE in a Distributed Environment.”](#)

Standalone Inline Posture Node in a Cisco ISE Deployment

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.

[Figure 4-2](#) illustrates a simple Inline Posture standalone configuration, with client access through WLC and VPN devices.

Inline Posture High Availability

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 and forwards all network packets until it fails and 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.

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. The secondary Inline Posture node is read-only, and cannot be used for configuration of any kind, even high availability.

When you configure an Inline Posture high-availability pair, 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.

Figure 4-4 illustrates a routed mode high-availability Inline Posture configuration.

An Inline Posture high-availability pair consists of two physical Inline Posture nodes configured as a cluster that have heartbeat links on the eth2 and eth3 interfaces, and are connected by dedicated cables.

The eth2 and eth3 interfaces of both nodes communicate with heartbeat protocol exchanges to determine the health of the nodes. 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 service IP address to both the trusted and untrusted interfaces for both nodes of the active-standby pair, thus making the service IP address the address of the cluster, representing it as a single entity to the rest of the network.

Automatic Failover in Inline Posture Nodes

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.

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.

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.

In addition to the heartbeat monitor, an optional (but highly recommended) link-detect mechanism is available. With the use of this mechanism, 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.

When failover occurs:

1. The standby Inline Posture node takes over the service IP address.
2. 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 [Synchronizing an Inline Posture Node, page 4-20](#).

3. Active sessions are automatically reauthenticated and authorized.

Inline Posture Operating Modes

The Inline Posture operating mode that you choose depends largely on the architecture of your existing network. Cisco ISE supports the following operating modes:

- [Inline Posture Routed Mode, page 4-6](#)
- [Inline Posture Bridged Mode, page 4-7](#)
- [Inline Posture Maintenance Mode, page 4-8](#)

Inline Posture Routed Mode

The Inline Posture routed 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.

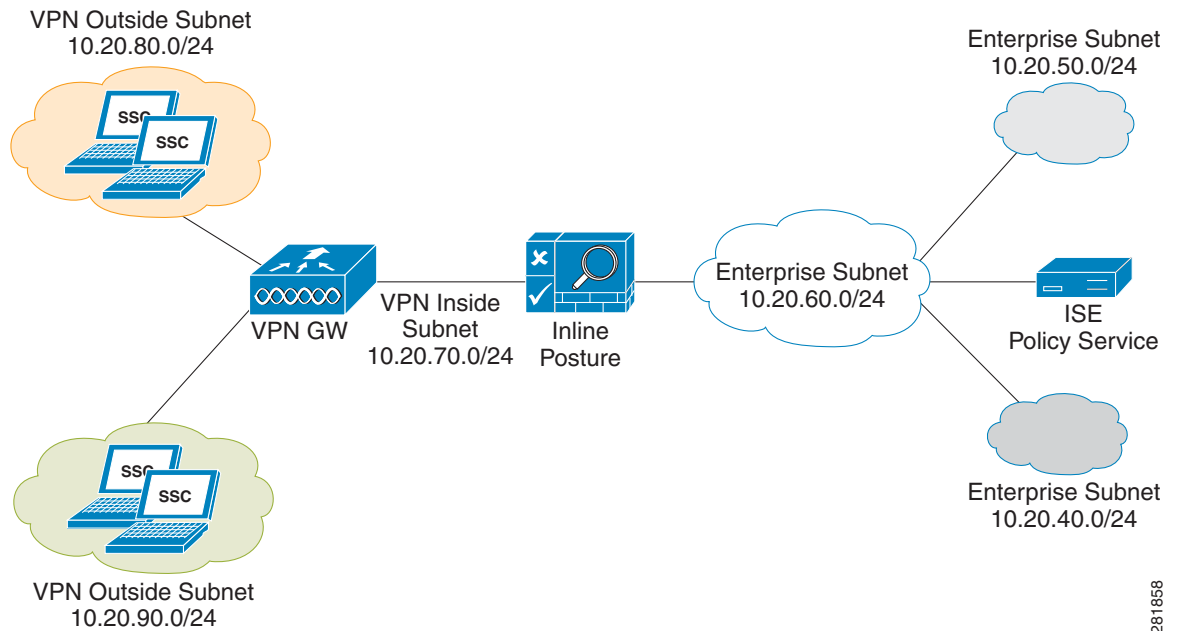
In routed mode, the Inline Posture node operates as a Layer 3 router, and becomes the default gateway for the untrusted network with its managed clients. All traffic between the untrusted and trusted networks passes through the Inline Posture node, which applies the IP filtering rules, access policies, and other traffic-handling mechanisms that you decide to configure.

When you configure Inline Posture in routed mode, you must 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 4-2](#) illustrates an Inline Posture routed mode configuration. In this example, Inline Posture is a hop for the client traffic from the VPN gateway (GW) en route to the Policy Service 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 4-2 *Inline Posture Routed Mode Configuration*

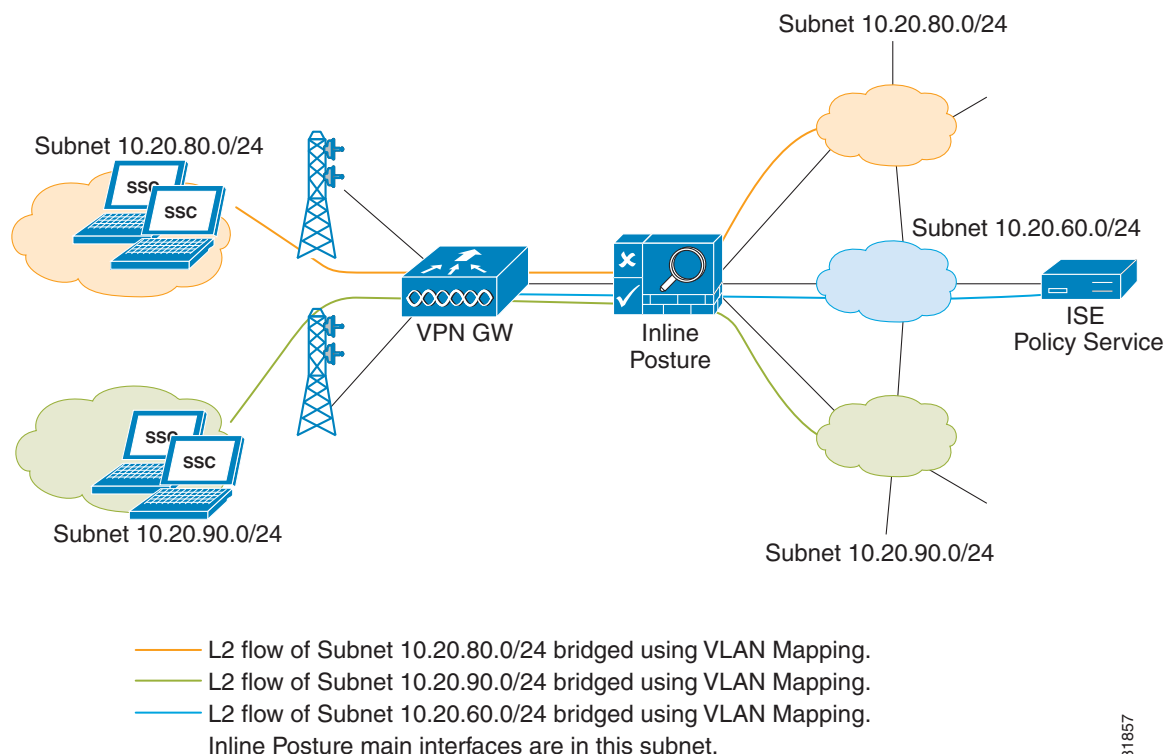
281858

Inline Posture Bridged Mode

The Inline Posture bridged mode acts as a Layer 2 “bump” in the wire, forwarding packets without regard to the destination address.

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 4-3 shows the Inline Posture node acting as a bridge for the Layer 2 client traffic from the WLC to the Cisco ISE network, managed by the Policy Service 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 4-3 *Inline Posture Bridged Mode Configuration*

281857

When the Inline Posture node is in bridged mode, the following conditions apply:

- Inline Posture eth0 and eth1 interfaces can have the same IP address.
- All end devices in the bridged subnet must be on the untrusted network.

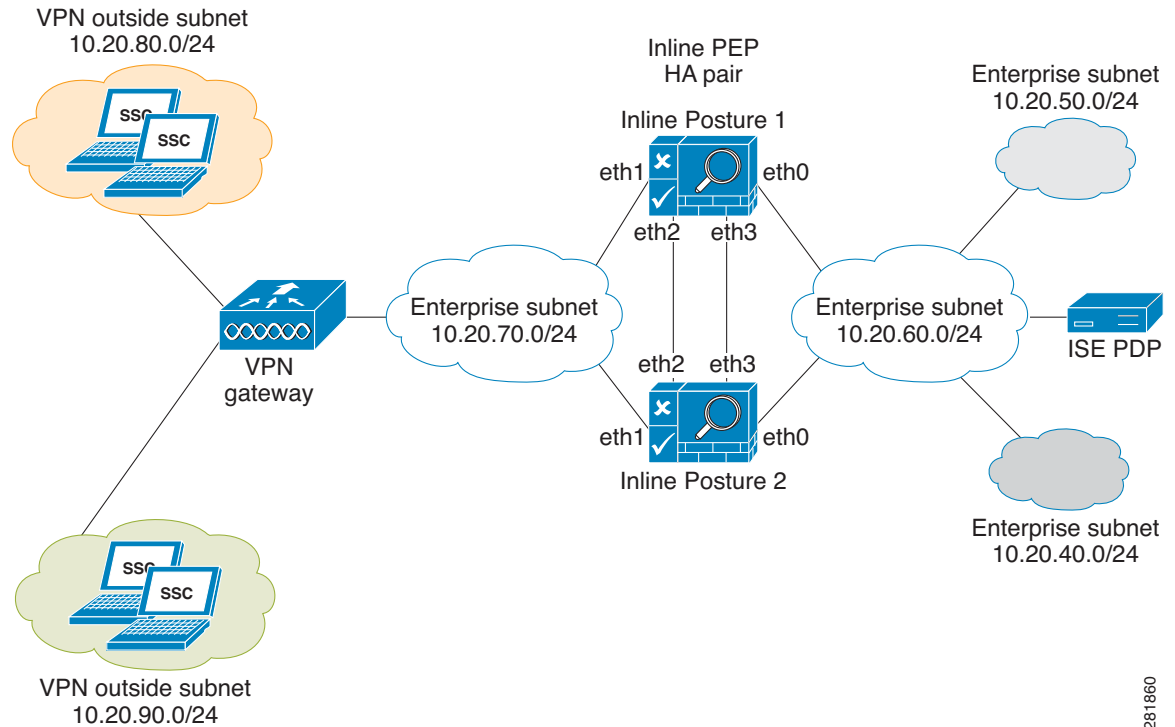
Inline Posture Maintenance Mode

The Inline Posture maintenance 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, and before you perform other configurations.

Inline Posture High Availability in Routed and Bridged Modes

Figure 4-4 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.

In this example, the untrusted IP address for Inline Posture 1 can be 10.20.70.101, and the untrusted IP address for Inline Posture 2 can be 10.20.70.102. However, the service IP address for both nodes on the untrusted side of the network would be 10.20.70.100. 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 4-4 *Inline Posture High-Availability Routed Mode Configuration*

281860

In a bridged mode, Inline Posture eth0 and eth1 interfaces 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.

Best Practices for Inline Posture Deployment

You can follow the best practices listed here to manage your Inline Posture deployment efficiently:

- [Use Filters to Define Access Privileges, page 4-9](#)
- [Configure Managed Subnets and Static Routes, page 4-10](#)
- [Configure High-Availability Pair, page 4-10](#)

Use Filters to Define Access Privileges

Consider the following when configuring filters for Inline Posture:

- In a typical implementation, 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, MAC and IP, or 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.

**Caution**

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 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.

Configure Managed Subnets and Static Routes

Consider the following when configuring managed subnets for Inline Posture:

- Configure a managed subnet for Inline Posture. A managed subnet 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.
- Configure managed subnets for endpoints in Layer 2 proximity of the Inline Posture node, such as, a WLC that delivers packets directly to the untrusted interface of the Inline Posture node.
- 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.
- Ensure that subnets on the trusted side of the Inline Posture node are different from the subnets on the untrusted side.
- Ensure that an Administration node, Policy Service node, and Monitoring node are not on the same subnet as the Inline Posture node, 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.
- Configure static routes for all downstream host networks that are typical of VPN address pools.

Configure High-Availability Pair

Consider the following when configuring Inline Posture for high availability:

- Assign a service IP address (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.

Inline Posture Node Guidelines

Before you configure an Inline Posture node in a distributed deployment, read and understand the following statements:

1. The Inline Posture node is supported only on Cisco ISE-3300 series and SNS-3415 appliances. It is not currently supported on Cisco SNS-3495 appliance or as a virtual appliance.
2. Inline Posture is unable to run concurrently with Administration, Policy Service, or Monitoring personas and, therefore, is a dedicated node.
3. An Inline Posture node must be registered to the primary Administration node on your network.
4. For each deployment instance of an Inline Posture node, you can deploy a standalone node, or an active-standby pair.
5. At any network entry point, like VPN headend using ASA or group of ASAs in an HA cluster, a maximum of 2 Inline Posture nodes can be deployed as active-standby pair for high-availability. You can have several HA pairs in a deployment.
6. Inline Posture nodes are similar to network access devices (NAD) in function from the perspective of Cisco ISE node. Inline Posture nodes can serve as multiple NADs like switches, Wireless Lan Controllers, and VPN devices. Based on the deployment needs, you can deploy multiple instances of Inline Posture nodes. To determine the maximum number of deployment instances, treat the Inline Posture nodes as access devices.
7. For an Inline Posture high-availability, two nodes are configured as an active-standby pair. One node is designated as the primary node and the other as the secondary node. The primary node becomes the active node when both nodes come up at the same time.
8. For an Inline Posture active-standby pair configuration, all configuration must be applied from the ISE administrative user interface. The standby node configuration displays only basic tables when viewed from the ISE administrative user interface.
9. You can synchronize an Inline Posture active node configuration to its peer standby node from the Failover tab of the active node. For more information, see [Synchronizing an Inline Posture Node](#), page 4-20.

**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.

10. Registering an Inline Posture node results in system restart. High-availability changes and changes to infrastructure configurations such as the eth1 IP address or Inline Posture mode 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.
11. After you register an Inline Posture node to the Administration node, you are not allowed to change the eth0 (Trusted) IP address through the Admin portal. The reason for this is that, if you change the eth0 IP address of a registered Inline Posture node, it cannot communicate with the Administration node. Any attempted communication between the Inline Posture node and Administration node then fails, leading to a potential exception.



Note

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.



Caution

The Inline Posture node's untrusted interface should be disconnected when the Inline Posture node is being configured. If the Inline Posture node's trusted and untrusted interfaces are connected to the same VLAN during initial configuration and the Inline Posture node initially starts after changing its persona, multicast packet traffic gets flooded out of the untrusted interface. This multicast storm can potentially bring down devices that are connected to the same subnet or VLAN. The Inline Posture node at this time is in Maintenance mode.

Inline Posture Node Authorization

The following images illustrate the client authorization flow and session recovery using Lazy Fetch mechanism for Inline Posture node.

Figure 4-5 *Inline Posture Node Client Authorization Flow*

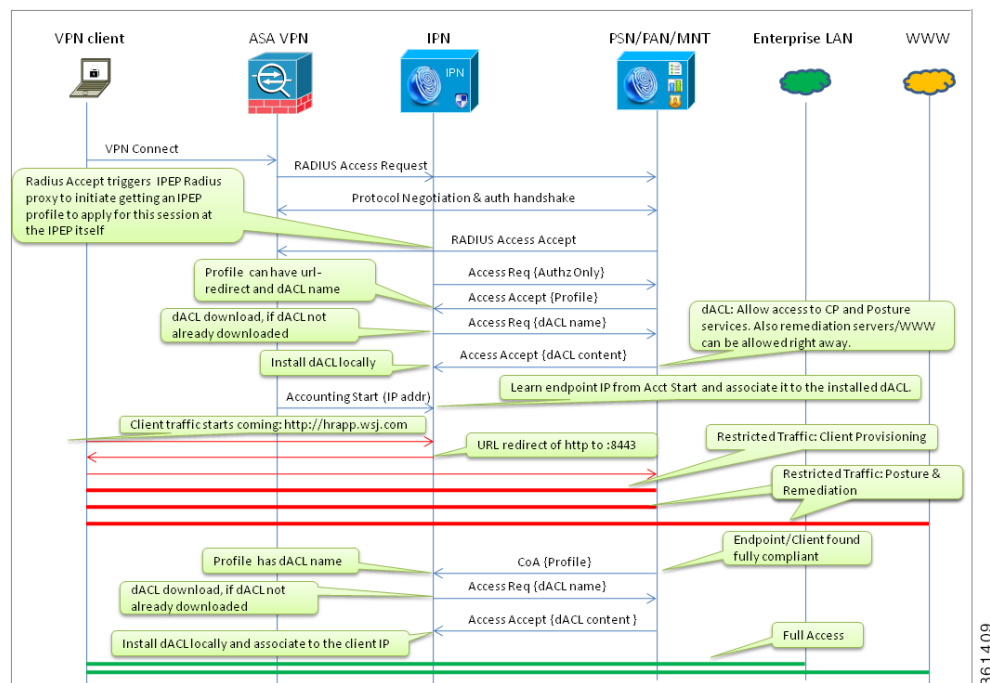
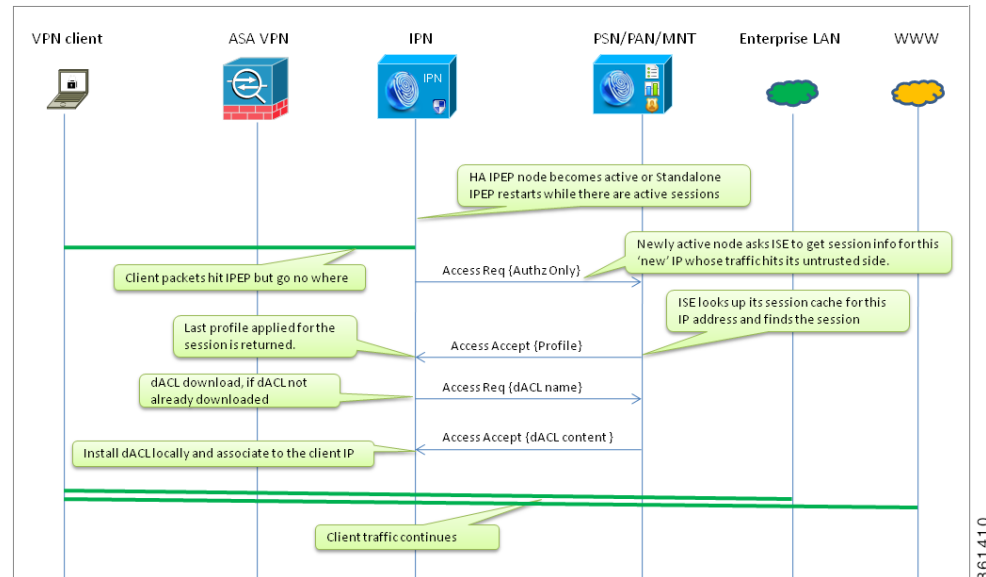


Figure 4-6 *Inline Posture Node Session Recovery Using Lazy Fetch Mechanism***Inline Posture Node Session Removal due to Client Disconnect**

When a wireless client is wandering off from the WLC control, the WLC is required to send a RADIUS Accounting Stop similar to the VPN gateway to ensure that the Inline Posture node cleans up the session corresponding to the client.

Deploying an Inline Posture Node

The initial process for deploying an Inline Posture node is the same, whether it is intended to be a standalone node or part of an active-standby pair.

**Note**

Inline Posture is supported on the Cisco ISE 3415, ISE 3315, ISE 3355, and ISE 3395 platforms.

To deploy an Inline Posture node, complete the following tasks:

1. [Configuring an Inline Posture Node, page 4-13](#)
2. [Creating Inline Posture Downloadable Access Control Lists, page 4-16](#)
3. [Creating Inline Posture Node Profiles, page 4-17](#)
4. [Creating an Inline Posture Authorization Policy, page 4-18](#)

Configuring an Inline Posture Node

Inline Posture is a dedicated node registered to the Administration node. You configure Inline Posture from the administration console, and that configuration is then replicated to the Inline Posture node. A copy of the configuration is stored locally in the administration database. After an Inline Posture node is registered, it is rebooted.

To introduce an Inline Posture node in your Cisco ISE network, you must first register the Inline Posture node with the primary Administration 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 node as a client making the Policy Service node its RADIUS server.

**Note**

After 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 a high-availability pair, the service IP address for the active node is used.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Inline Posture is not supported on the Cisco ISE 3495 platform. Ensure that you install Inline Posture on any one of the following supported platforms: ISE 3315, ISE 3355, ISE 3395, or ISE 3415.

Follow and apply the guidelines for configuring certificates for Inline Posture. Refer to [Cisco Identity Services Engine Hardware Installation Guide, Release 1.2](#) for details.

Register the Inline Posture node with the primary Administration node. All nodes must be registered with the primary Administration node to function as a member of the Cisco ISE distributed system.

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, IP addresses for other Cisco ISE nodes, shared secret information for the 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.

**Caution**

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.

Step 1 Choose **Administration > System > Deployment**.

Step 2 Check the **Inline Posture node** check box in the Deployment Nodes page and click **Edit**.

Step 3 Check the **Inline PEP** check box on the General Settings tab. The Administration, Monitoring, and Policy Service check boxes are automatically unchecked.

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 Step 3.

Step 4 Click the following tabs and enter the appropriate information for the fields in the tabs. See [Inline Posture Node Settings](#) for more information on the fields.

- **Basic Information**
- **Deployment Modes**—A newly registered Inline Posture node comes up in maintenance mode. For production purposes, you must choose the Routed or Bridged mode.
- **Filters**—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.
- **Radius Config**—RADIUS configuration is mandatory. At least one client and one server configuration is necessary for Inline Posture.
- **Managed Subnets**—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. You must enter the following values: IP Address, Subnet Mask, VLAN ID, and Description.
- **Static Routes**—Enter the subnet address, subnet mask, and choose **Trusted** or **Untrusted** from the Interface Type drop-down list. 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.

- **Logging**—Click the **Logging** tab and enter the IP address and port number for the logging server, which is typically the Monitoring 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 in the Cisco ISE dashboard in the System Summary dashlet, and that other log information regarding the nodes is available.

- **Failover**—This tab is for Inline Posture High Availability configuration.

Step 5 Click **Save**. The Inline Posture node restarts automatically.

Step 6 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 a high-availability pair, the service IP address for the active node is used.

What To Do Next

To complete the deployment of the Inline Posture node, you must create DACLs, authorization profiles, and authorization policy rules: unknown, compliant, and noncompliant.



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.

Related Topics

- [Inline Posture Node Settings, page A-6](#)
- [Registering an Inline Posture Node, page 3-14](#)
- [Configuring a High-Availability Pair, page 4-19](#)
- [Creating Inline Posture Downloadable Access Control Lists, page 4-16](#)
- [Creating Inline Posture Node Profiles, page 4-17](#)
- [Creating an Inline Posture Authorization Policy, page 4-18](#)

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.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Policy > Policy Elements > Results > Authorization > Downloadable ACLs .
Step 2	Click Add .
Step 3	Enter the name of the DACL and its description.
Step 4	Create the following DACLS: • ipn-compliant (Permit All): Use the following syntax: permit ip any any • ipn-noncompliant (Deny All): Use the following syntax: deny ip any any • ipn-unknown (Pre-Posture): Use at least one ACL to allow supplicants and the Policy Service node to have access to each other for posture evaluation. This DACL can be used to block or quarantine users until they pass authentication. Here is an example syntax: deny tcp any any eq 80 deny tcp any any eq 443 permit ip any 10.1.2.4 0.0.0.0 permit udp any any eq 53 deny ip any any
Step 5	Save the DACLS.
-

What To Do Next

[Creating Inline Posture Node Profiles, page 4-17](#)

Related Topics

[Cisco ISE Authorization Profiles, page 20-2](#)

Creating Inline Posture Node Profiles

You must create three Inline Posture authorization profiles, as well as an authorization profile for a NAD.

All Inline Posture inbound profiles are automatically set to `cisco-av-pair=ipep-authz=true` so that the Inline Posture node applies these rules instead of proxying them on to the NADs. The URL redirect is essential for client provisioning, as well as agent discovery redirection.

Before You Begin

To perform the following task, you must be a Super Admin, System Admin, or Policy Admin.

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Inline Posture Node Profiles**.
- Step 2** Click **Add**.
- Step 3** Enter a name and description for the authorization profile. Supported characters for the name field are: space, ! # \$ % & ' () * + , - . / ; = ? @ _ { .
-  **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 4** Create the following authorization profiles for Inline Posture that correspond to the DACLs you created. Specify the appropriate DACL for each of the following authorization profiles:
- IPN-Unknown-Compliant (Pre-Posture): This profile requires that you enter a URL redirect. To do this, check the URL Redirect check box.
The URL redirect appears in the Attributes Details field.
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.
 - IPN-Compliant (Permit All)
 - IPN-Noncompliant (Deny All).
- Step 5** Click **Submit**.
-

What To Do Next

[Creating an Inline Posture Authorization Policy, page 4-18](#)

Related Topics

- [Cisco ISE Authorization Policies, page 20-1](#)
- [Cisco ISE Authorization Profiles, page 20-2](#)

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 rules when creating 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.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Policy > Authorization**.
- Step 2** Leave the default rules as is.
- Step 3** Create the following Unknown Posture Status Rule:
- Identity Group: Any
 - Condition: Session:PostureStatus EQUALS = Unknown
 - Permissions: IPN-Unknown-Compliant + nad-authorization-profile
- Step 4** Create the following Compliant Posture Rule:
- Identity Group: Any
 - Condition: Session:PostureStatus EQUALS = Compliant
 - Permissions: IPN-Compliant + nad-authorization-profile
- Step 5** Create the following Noncompliant Posture Rule:
- Identity Group: Any
 - Condition: Session:PostureStatus EQUALS = Noncompliant
 - Permissions: IPN-Noncompliant + nad-authorization-profile
- Step 6** Save the policy. The Inline Posture node deployment is now complete.
-

What To Do Next

[Configuring Inline Posture Node as RADIUS Client in Administration Node, page 4-20.](#)

Related Topics

- [Cisco ISE Authorization Policies, page 20-1](#)
- [Cisco ISE Authorization Profiles, page 20-2](#)

Configuring a High-Availability Pair

When you configure two Inline Posture nodes for high availability, you specify one node as the primary unit in the pair and it 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. Because high-availability failover is stateless, all active sessions are automatically reauthorized after a failover occurs.

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.

**Note**

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.

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.
- You should have successfully configured two (2) Inline Posture nodes, and registered them on the Cisco ISE network.
- 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 4-4](#) 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 the course of this procedure.
- Have all necessary network configuration information for your installation on hand. Check with your system architect for a complete list of information you will need.

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Check the check box next to the Inline Posture node that you want to designate as the primary node, and click **Edit**.
- 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 list.
- Step 4** Click the **Failover** tab, and check the **HA Enabled** check box.
- Step 5** Enter the appropriate information in the fields.
- Step 6** 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.
- Step 7** Verify the node status by checking the check box next to it, and then clicking the **Failover** tab. Ensure that your primary and secondary Inline Posture nodes are configured correctly.
-

What To Do Next

Complete the following task: [Configuring Inline Posture Node as RADIUS Client in Administration Node, page 4-20](#).

Related Topics

- [Inline Posture Node Settings, page A-6](#)
- [Configuring an Inline Posture Node, page 4-13](#)
- [Synchronizing an Inline Posture Node, page 4-20](#)

Synchronizing an Inline Posture Node

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 synchronize the standby node with the latest Inline Posture database from the active node.

Before You Begin

- You must be a Super Admin or System Admin.
- You must configure two Inline Posture nodes.
- You must establish a relationship between the two nodes.

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Check the check box next to the Inline Posture node that you want to sync with the other node (usually the active node), and click the **Edit** icon.
- Step 3** Click the **Failover** tab. See [Deployment Settings](#) for a description of the fields in this tab.
- Step 4** Click **Sync Peer Node**. Data from the selected node is automatically transferred to its peer node.
-

Related Topics

- [Configuring an Inline Posture Node, page 4-13](#)
- [Configuring a High-Availability Pair, page 4-19](#)

Configuring Inline Posture Node as RADIUS Client in Administration Node

For an Inline Posture node to act as a RADIUS proxy, you must add it as a RADIUS client in the Administration node.

Before You Begin

- You must be a Super Admin or System Admin.
- You must deploy Inline Posture in your Cisco ISE deployment.

-
- Step 1** Choose **Administration > Network Resources > Network Devices**.
- Step 2** In the Network Devices navigation panel, click **Network Devices**.
- Step 3** Enter a Name and Description for the device.
- Step 4** Enter the IP address of the Inline Posture node.
- 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 RADIUS shared secret information.
- Step 8** Click **Save**.
-

Removing an Inline Posture Node from Deployment

To remove an Inline Posture node from a deployment, you must first change its deployment to maintenance mode and then deregister it. Maintenance mode is a neutral state that allows the node to smoothly transition to the network or from a deployment.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

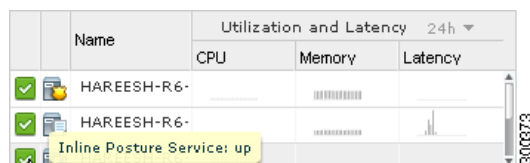
-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Check the check box next to the Inline Posture node that you want to remove from the deployment, and click **Edit**.
- Step 3** Click the **Deployment Modes** tab.
- Step 4** Click the **Maintenance Mode** radio button, and then 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.
- Step 6** Click **Deregister**.
- Step 7** Click **OK**.
-

Health of 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 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 your mouse cursor over the health icon, a quick view dialog appears showing detailed information on system health.

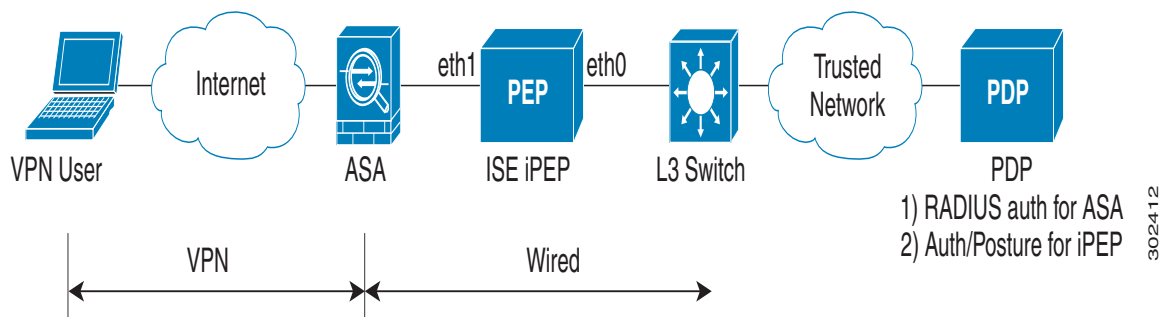
Figure 4-7 System Summary Quick View Status



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 4-8](#) 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 4-8 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 access control lists (DACLS) for policy enforcement by the Inline Posture node.
 - b. Standard authorization profile: Specifies any RADIUS attributes intended for the NAD, which is 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.

Related Topics

[Configuring an Inline Posture Node with a VPN Device, page 4-23](#)

Configuring an Inline Posture Node with a VPN Device

Before You Begin

Ensure that your network infrastructure is configured correctly to route or switch traffic to and from the Inline Posture node and its downstream networks.

-
Step 1	Configure a standalone Cisco ISE node. For more information, refer to Configuring a Cisco ISE Node, page 3-11 .
Step 2	Register the standalone Cisco ISE node as an Inline Posture node to an existing primary Administration node, and configure the Inline Posture node from the primary Administration node. For more information, refer to Deploying an Inline Posture Node, page 4-13 .
Step 3	Optionally, you can configure a second Inline Posture node and configure an Active/Standby pair. For more information, refer to Inline Posture High Availability, page 4-4 .
Step 4	Set up a Policy Service node to be the RADIUS server for the Inline Posture node. Configure the Policy Service node with the same RADIUS shared secret that is configured on the Inline Posture node.
Step 5	Configure authorization profiles (Inline Posture node profiles) for use by the Inline Posture node.
Step 6	(Optional) You can configure standard authorization profiles for the NAD's use. For more information, refer to Creating Inline Posture Node Profiles, page 4-17 and Creating Inline Posture Downloadable Access Control Lists, page 4-16 .
Step 7	Configure an 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 4-18 .

- 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:
- Choose **Policy > Authentication**.
 - Ensure that the Default Rule is configured to authenticate users against the identity source that contains the user records.
 - Click **Save**.

Collecting Inline Posture Node Logs

From the Inline Posture node CLI, all the logs can be archived and collected using the backup-logs command.

```
PEP/admin# config terminal
PEP/admin# repository remoteloc
PEP/admin# url ftp://myremoteserver/store
PEP/admin# user <myremoteuser> password plain <myremotepasswd>
PEP/admin# end
PEP/admin# backup-logs myipeplogs repository remoteloc
% Creating log backup with timestamped filename: myipeplogs-110317-1836.tar.gz
```



Note

Collecting Inline Posture node logs remotely from the Primary Administration UI is not supported.

Kclick process in Inline Posture Node

Click kernel module process, called as kclick owns CPU scheduling in Inline Posture node. Kclick provides the CPU cycles for other processes that request it. Due to this the 'top' output at an Inline Posture Node displays the kclick using all the CPU cycles in the system including idle cycles.



PART 4

Setting Up Cisco ISE Management Access



Administering Cisco ISE

Use the tasks and reference information in this chapter to specify global settings and configure essential functions in Cisco ISE.

- [Logging in to Cisco ISE, page 5-1](#)
- [Specifying Proxy Settings in Cisco ISE, page 5-2](#)
- [Ports Used by the Admin Portal, page 5-3](#)
- [Specifying System Time and NTP Server Settings, page 5-3](#)
- [Changing the System Time Zone, page 5-4](#)
- [Configuring the SMTP Server to Support Notifications, page 5-5](#)
- [Installing a Software Patch, page 5-5](#)
- [Rolling Back Software Patches, page 5-7](#)
- [Viewing Patch Install and Rollback Changes, page 5-8](#)
- [Enabling FIPS Mode in Cisco ISE, page 5-8](#)
- [Configuring Cisco ISE for Administrator CAC Authentication, page 5-10](#)
- [Securing SSH Key Exchange Using Diffie-Hellman Algorithm, page 5-13](#)
- [Configuring Cisco ISE to Send Secure Syslog for Common Criteria Compliance, page 5-13](#)

Logging in to Cisco ISE

Log in to Cisco ISE using your administrator username and password.

-
- Step 1** Enter the Cisco ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*).
- Step 2** Enter the username and case-sensitive password, that was specified and configured during the initial Cisco ISE setup.
- Step 3** Click **Login** or press **Enter**.

If your login is unsuccessful, click the **Problem logging in?** link in the Login page and follow the instructions in [Step 2](#).

Related Topics

- [Administrator Login Browser Support, page 5-2](#)
- [Administrator Lockout Following Failed Login Attempts, page 5-2](#)
- If you have to reset the Administrator password, see the “Performing Post-Installation Tasks” chapter of the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.2](#).

Administrator Login Browser Support

You can access the Cisco ISE Admin portal using the following browsers:

- Mozilla Firefox Versions 5.x, 8.x, 9.x, 14.x, 15.x, and 18.x (applicable for Windows, Mac OS X, and Linux-based operating systems)
- Windows Internet Explorer 8.x and 9.x (in Internet Explorer 8 Compatibility Mode)

**Note**

The Admin portal does not support using the Microsoft IE8 browser in its IE7 Compatibility Mode (the Microsoft IE8 is supported in its IE8-only mode).

Adobe Flash Player 11.2.0.0 or above must be installed on the system running your client browser.

The minimum required screen resolution to view the Admin portal and for a better user experience is 1280*800 pixels.

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for your specified administrator user ID enough times, the Admin portal “locks you out” of the system, adds a log entry in the 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 1.2](#). The number of failed attempts that is required to disable the administrator account is configurable according to the guidelines that are described in [User Account Custom Attributes and Password Policies, page 14-2](#). After an administrator user account gets locked out, an e-mail is sent to the associated administrator user.

Disabled System administrators' status can be enabled by any Super Admin, including Active Directory users.

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 Admin portal to specify proxy properties.

-
- Step 1** Choose **Administration > System > Settings > Proxy**.
- Step 2** Enter the proxy IP address or DNS-resolvable host name in **Proxy Address**, and specify the port through which proxy traffic travels to and from Cisco ISE in **Proxy Port**.

Step 3 Click **Save**.

What to Do Next

Once you have specified your proxy settings, you can optionally enable the following systemwide client provisioning functions:

- [Enabling and Disabling Client Provisioning, page 22-2](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)

Related Topics

- [Cannot Download Remote Client Provisioning Resources, page G-13](#)

Ports Used by the Admin Portal

The Admin portal is set to use HTTP port 80 and HTTPS port 443, and you cannot change these settings. Cisco ISE also prevents you from assigning any of the end-user portals to use the same ports, which reduces the risk to the Admin portal.

Related Topics

- [Port Settings for Web Portals, page A-50](#)
- [Specifying Ports and Ethernet Interfaces for End-User Portals, page 15-2](#)

Specifying System Time and NTP Server Settings

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. 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.

Cisco recommends that you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone—especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

Before You Begin

You must have either the Super Admin or System Admin administrator role assigned.

If you have both a primary and a secondary Cisco ISE node, you must log in to the user interface of the secondary node and configure the system time and NTP server settings on each Cisco ISE node in your deployment individually.

Step 1 Choose **Administration > System > Settings > System Time**.

Step 2 Enter unique IP addresses for your NTP servers.

Step 3 Check-the **Only allow authenticated NTP servers** check box if you want to restrict Cisco ISE to use only authenticated NTP servers to keep system and network time.

- Step 4** Click the **NTP Authentication Keys** tab and specify one or more authentication keys if any of the servers that you specify requires authentication via an authentication key, as follows:
- Click **Add**.
 - Enter the necessary **Key ID** and **Key Value**, specify whether the key in question is trusted by activating or deactivating the **Trusted Key** option, and click **OK**. The **Key ID** field supports numeric values between 1 to 65535 and the **Key Value** .field supports up to 15 alphanumeric characters.
 - Return to the **NTP Server Configuration** tab when you are finished entering the NTP Server Authentication Keys.
- Step 5** Click **Save**.
-

Related Topics

- [Role-Based Access Control in Cisco ISE, page 6-8](#)

Changing the System Time Zone

Once set, you cannot edit the time zone from the Admin portal. To change the time zone setting, you must enter the following command in the Cisco ISE CLI:

clock timezone *timezone*



Caution

Changing the time zone on a Cisco ISE appliance after installation causes the Cisco ISE application on that node to be unusable. However, the preferred time zone (default UTC) can be configured during the installation when the initial setup wizard prompts you for the time zone.

Changing time zone impacts different Cisco ISE node types in your deployment as follows:

Standalone or Primary ISE Node

Changing the time zone after installation is not supported on a Standalone or Primary ISE node. However, if you inadvertently change the time zone, do the following:

- Revert to the time zone back. (the time zone before it changed).
- Run the application reset-config ise command from the CLI of that node.
- Restore from the last known good backup before the time zone change on that node.

Secondary ISE Node

Changing the time zone on a secondary node renders it unusable on your deployment. If you want to change the time zone on the secondary node to keep it to be the same as the primary node, do the following:

- Deregister the secondary node.
- Correct the time zone to be the same as the primary node.
- Run the application reset-config ise command from the CLI of that node.
- Reregister the node as a secondary node to the primary node.

For more information on the **clock timezone** command, refer to [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

Configuring the SMTP Server to Support Notifications

You must set up a Simple Mail Transfer Protocol (SMTP) server to send e-mail notifications for alarms and to enable sponsors to send guests their account credentials using e-mail or Short Message Service (SMS) text messages.

-
- Step 1** Choose **Administration > System > Settings > SMTP Server**.
- Step 2** Enter the host name of the outbound SMTP server in the **SMTP server** field. This SMTP host server must be accessible from the Cisco ISE server. The maximum length for this field is 60 characters.
- Step 3** Choose one of these options:
- **Use email address from Sponsor** to send guest notification e-mail from the e-mail address of the sponsor and choose **Enable Notifications**.
 - **Use Default email address** to specify a specific e-mail address from which to send all guest notifications and enter it in the **Default email address** field.
- Step 4** Click **Save**.
-

The recipient of alarm notifications can be any internal admin users with “Include system alarms in emails” option enabled. The sender’s email address for sending alarm notifications is hardcoded as `ise@<hostname>`.

Related Topic

- [Customizing Guest Notifications, page 16-9](#)
- [Enabling and Configuring Alarms, page 25-11](#)
- [Creating a New Cisco ISE Administrator, page 6-2](#)

Installing a Software Patch

You can install patches on Cisco ISE servers in your deployment from the primary administration node. To install a patch from the Admin portal, you must download the patch from Cisco.com 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.

To install patches from the CLI, refer to [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

Before You Begin

You must have the Super Admin or System Admin administrator role assigned.

-
- Step 1** Choose **Administration > System > Maintenance > Patch Management > Install**.

Step 2 Click **Browse** and choose the patch that you downloaded from Cisco.com.

Step 3 Click **Install** to install the patch.

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 in again.



Note When patch installation is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.

Step 4 Log in and click the **Alarms** link at the bottom of the dashboard page.

Step 5 Choose **Administration > System > Maintenance > Patch Management** to return to the Patch Installation page.

Step 6 Click the radio button next to the patch that you have installed on any secondary nodes and click **Show Node Status** to verify whether installation is complete.

What To Do Next

If you need to install the patch on one or more secondary nodes, ensure that the nodes are up and repeat the process from [Step 1](#) to install the patch on the remaining nodes.

Related Topics

- [Cisco ISE Software Patches, page 5-6](#)
- [Software Patch Installation Guidelines, page 5-6](#)
- [Rolling Back Software Patches, page 5-7](#)
- [Viewing Patch Install and Rollback Changes, page 5-8](#)
- [Role-Based Access Control in Cisco ISE, page 6-8](#)

Cisco ISE Software Patches

Cisco ISE software patches are usually cumulative. However, any restrictions on the patch installation are described in the *README* file included with the patch. Cisco ISE allows you to perform patch installation and rollback from CLI or GUI.

Software Patch Installation Guidelines

When you install or roll back a patch from a standalone or primary administration node, Cisco ISE restarts the application. You might have to wait for a few minutes before you can log in again.

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 as well as any errors in the patch file.

You cannot install a patch with a version that is lower than the patch that is currently installed on Cisco 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 Cisco ISE servers, you cannot install or roll back patch 1 or 2.

When you install a patch from a primary administration node that is part of a distributed deployment, Cisco ISE installs the patch on the primary node and then all the secondary nodes in the deployment. If the patch installation is successful on the primary node, Cisco ISE then continues patch installation on the secondary nodes. If it fails on the primary node, the installation does not proceed to the secondary nodes. 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. Secondary Cisco ISE nodes are restarted consecutively after the patch is installed on those nodes. While installing a patch on secondary nodes, you can continue to perform tasks on the primary administration node.

Rolling Back Software Patches

When you roll back a patch from a primary administration node that is part of a distributed deployment, Cisco ISE installs the patch on the primary node and then all the secondary nodes in the deployment.

Before You Begin

You must have either the Super Admin or System Admin administrator role assigned.

-
- Step 1** Choose **Administration > System > Maintenance > Patch Management**.
- Step 2** Click the radio button for the patch version whose changes you want to roll back and click **Rollback**.



Note When a patch rollback is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.

After the patch is rolled back from the primary administration node, Cisco ISE logs you out and you have to wait a few minutes before you can log in again.

- Step 3** After you log in, click the **Alarms** link at the bottom of the page to view the status of the rollback operation.
- Step 4** Choose **Administration > System > Maintenance > Patch Management**
- Step 5** To view the progress of the patch rollback, choose the patch in the Patch Management page and click **Show Node Status**.
- Step 6** Click the radio button for the patch and click **Show Node Status** on any secondary nodes 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 1](#) to roll back the changes from the remaining nodes. Cisco ISE only rolls back the patch from the nodes that still have this version of the patch installed.

Related Topics

- [Software Patch Rollback Guidelines, page 5-8](#)
- To roll back patches from the CLI, refer to *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*
- [Installing a Software Patch, page 5-5](#)
- [Viewing Patch Install and Rollback Changes, page 5-8](#)
- [Role-Based Access Control in Cisco ISE, page 6-8](#)

Software Patch Rollback Guidelines

To roll back a patch from Cisco ISE nodes in a deployment, you must first roll back the change from the primary node. If this is successful, the patch is then rolled back from the secondary nodes. If the rollback process fails on the primary node, the patches are not rolled back from the secondary nodes. However, if the patch fails on any of the secondary nodes, it still continues to roll back the patch from the next secondary node 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.

Viewing Patch Install and Rollback Changes

The monitoring and troubleshooting component of Cisco ISE provides information on the patch installation and rollback operations that are performed on your Cisco ISE nodes according to a time period that you specify.

Before You Begin

You must have either the Super Admin or System Admin administrator role assigned.

-
- Step 1** Choose **Operations > Reports > Catalog > Server Instance**.
 - Step 2** Click the **Server Operations Audit** radio button, click **Run**, and choose the time period for which you want to generate the report.
 - Step 3** Click the **Launch Interactive Viewer** link in the upper right corner of the page to view, sort, and filter the data in this report.

Related Topics

- [Cisco ISE Software Patches](#)
- [Installing a Software Patch](#)
- [Rolling Back Software Patches](#)
- [Role-Based Access Control in Cisco ISE, page 6-8](#)
- [“Running and Viewing Reports” section on page 26-2](#)

Enabling FIPS Mode in Cisco ISE

You can provide Federal Information Processing Standard (FIPS) 140-2 compliant encryption and decryption in your Cisco ISE network.

-
- Step 1** Choose **Administration > System > Settings > FIPS Mode**.
 - Step 2** Choose the **Enabled** option from the FIPS Mode drop-down list.
 - Step 3** Click **Save** and restart your machine.
-

What to Do Next

Once you have enabled FIPS mode, enable and configure the following FIPS 140-2 compliant functions:

- [Importing Network Devices into Cisco ISE, page 9-4](#)
- [Generating a Self-Signed Certificate, page 8-18](#)
- [Generating a Certificate Signing Request, page 8-19](#)
- [RADIUS Authentication Settings, page A-37](#)

In addition, you may want 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 5-10](#). 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.

FIPS Mode Support

Cisco ISE supports 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.

When FIPS mode is enabled, the Cisco ISE administrator interface displays a FIPS mode icon to the left of the node name in the upper-right of the page.

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 the protocols have been addressed appropriately.

After you enable FIPS mode, you must 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 node and then restarting each secondary node, one at a time.



Tip

Cisco recommends that you do not enable FIPS mode before completing any database migration process.

FIPS Mode Operational Parameters

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 RADIUS shared secret and key management measures. While in FIPS mode, any functions using non-FIPS-compliant algorithms fail, and certain authentication functionality is disabled. For more details, including protocol support, see [FIPS 140-2 Implementation, page 1-4](#) and [Support for Common Access Card Functions, page 1-5](#).

Enabling FIPS mode also automatically disables Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) protocols, which the guest login function of Cisco ISE requires. For information on addressing this issue with Layer-3 guest login implementation, see [Chapter 16, “Supporting Authorized Network Access for Guests.”](#)

Cisco NAC Agent Requirements when FIPS Mode is Enabled

The Cisco NAC Agent always looks 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 and TLS1.0 enabled to allow for Cisco ISE posture assessment functions to operate on client machines accessing the network. 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.

Configuring Cisco ISE for Administrator CAC Authentication

Before You Begin

Before beginning configuration, do the following:

- (Optional) Turn on FIPS mode according to the instructions in [Enabling FIPS Mode in Cisco ISE, page 5-8](#). 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.
- Ensure that the domain name server (DNS) in Cisco ISE is set for Active Directory.
- Ensure that 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

You can use a Common Access Card (CAC) to authenticate credentials when logging into Cisco ISE.

-
- Step 1** Enable FIPS mode as described in [Enabling FIPS Mode in Cisco ISE, page 5-8](#). You will be prompted to restart your system after you enable the FIPS mode. You can defer the restart if you are going to import CA certificates as well.
- Step 2** Configure an Active Directory identity source in Cisco ISE and join all Cisco ISE nodes to Active Directory as described in [Configuring Active Directory as an External Identity Source, page 14-12](#).
- Step 3** Configure a certificate authentication profile according to the guidelines in [Adding a Certificate Authentication Profile, page 14-8](#).

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.")

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 that was specified earlier.

- Step 4** Enable Active Directory for Password-Based Admin Authentication as described in [Configuring a Password-Based Authentication Using an External Identity Store, page 6-17](#). Choose the Active Directory instance name that you connected and joined to Cisco ISE earlier.



Note You must use password-based authentication until you complete other configurations. Then, you can change the authentication type to client certificate based at the end of this procedure.

- Step 5** Create an External Administrator Group and map it to an Active Directory Group. Choose **Administration > System > Admin Access > Administrators > Admin Groups**. Create an external system administrator group as described in [Creating an External Administrator Group, page 6-18](#).
- Step 6** Configure an admin authorization policy to assign RBAC permissions to the external admin groups as described in [Creating an RBAC Policy for External Administrator Authentication, page 6-19](#).



Warning

We strongly recommend that you create an external Super Admin group, map it to an Active Directory group, and configure an admin authorization policy with Super Admin permissions (menu access and data access), and create at least one user in that Active Directory Group. This mapping ensures that at least one external administrator has Super Admin permissions once Client Certificate-Based Authentication is enabled. Failure to do this may lead to situations where the Cisco ISE administrator is locked out of critical functionality in the Admin Portal.

- Step 7** Choose **Administration > System > Certificates > Certificate Store** to import certificate authority certificates into the Cisco ISE certificate trust store.

Cisco ISE does not accept a client certificate unless the CA certificates in the client certificate's trust chain are placed in the Cisco ISE Certificate Store. You must import the appropriate CA certificates in to the Cisco ISE Certificate Store.

- Click **Browse** to choose the certificate.
- Check the Trust for client authentication check box.
- Click **Submit**.

Cisco ISE prompts you to restart all the nodes in the deployment after you import a certificate. You can defer the restart until you import all the certificates. However, after importing all the certificates, you must restart Cisco ISE before you proceed.

- Step 8** Configure the certificate authority certificates for revocation status verification.
- Choose **Administration > System > Certificates > OSCP Services**.
 - Enter the name of an OSCP server, an optional description, and the URL of the server.
 - Choose **Administration > System > Certificates > Certificate Store**.
 - For each CA certificate that can sign a client certificate, specify how to do the revocation status check for that CA. Choose a CA certificate from the list and click Edit. On the edit page, choose OCSP and/or CRL validation. If you choose OCSP, choose an OCSP service to use for that CA. If you choose CRL, specify the CRL Distribution URL and other configuration parameters. See [OCSP Services, page 8-31](#) and [Editing a Certificate Store Certificate, page 8-28](#) for more information.

Step 9 Enable client certificate-based authentication. Choose **Administration > System > Admin Access > Authentication**.

- a. Choose Client Certificate Based authentication type on the Authentication Method tab.
- b. Choose the certificate authentication profile that you configured earlier.
- c. Select the Active Directory instance name.
- d. Click **Save**.

Here, you switch from password-based authentication to client certificate-based authentication. The certificate authentication profile that you configured earlier determines how the administrator's certificate is authenticated. The administrator is authorized using the external identity source, which in this example is Active Directory.

The Principal Name attribute from the certificate authentication profile is used to look up the administrator in Active Directory.

You have now configured Cisco ISE for administrator CAC authentication.

Related Topics

- [Supported Common Access Card Standards, page 5-12](#)
- [Common Access Card Operation in Cisco ISE, page 5-12](#)

Supported Common Access Card Standards

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. Access via the CAC requires a card reader into which you insert the card and enter 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.

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/>.

Common Access Card Operation in Cisco ISE

The Admin portal can be configured so that you authentication with Cisco ISE is permitted only by using a client certificate. Credentials-based authentication—such as providing a user ID and password—is not permitted. In client certificate authentication, you insert a Common Access Card (CAC) card, enter a PIN and then enter the Cisco ISE Admin portal URL into the browser address field. The browser forwards the certificate to Cisco ISE, and Cisco ISE authenticates and authorizes your login session, based on the contents of the certificate. If this process is successful, you are presented with the Cisco ISE Monitoring and Troubleshooting home page and given the appropriate RBAC permissions.

Securing SSH Key Exchange Using Diffie-Hellman Algorithm

You can configure Cisco ISE to only allow Diffie-Hellman-Group14-SHA1 SSH key exchanges. To do this, you must enter the following commands from the Cisco ISE Command-Line Interface (CLI) Configuration Mode:

```
service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

Here's an example:

```
ise/admin# conf t
ise/admin (config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

Configuring Cisco ISE to Send Secure Syslog for Common Criteria Compliance

The Common Criteria (CC) Compliance Certification requires Cisco ISE to send only TLS-protected secure syslog between the Cisco ISE nodes and to the Monitoring nodes.

Before You Begin

- Ensure that all the Cisco ISE nodes in your deployment are configured with appropriate server certificates. If you want your setup to be FIPS 140-2 compliant, the certificate keys must have a key size of 2048 bits or greater. See [Chapter 8, “Managing Certificates”](#) for more information.
- Enable the FIPS mode in the Admin portal. See [Enabling FIPS Mode in Cisco ISE, page 5-8](#) for details.
- Ensure that the default network access authentication policy does not allow any version of the SSL protocol. Use the TLS protocol in the FIPS mode along with FIPS-approved algorithms. See [Chapter 19, “Managing Authentication Policies”](#) for more information.
- Ensure that all the nodes in your deployment are registered with the primary Administration node. Also, ensure that at least one node in your deployment has the Monitoring persona enabled to function as the secure syslog receiver (TLS server). See [Chapter 3, “Setting Up Cisco ISE in a Distributed Environment”](#) for more information.

To configure Cisco ISE to send TLS-protected secure syslog between the Cisco ISE nodes and to the Monitoring node, you must perform the following tasks:

1. Configure secure syslog remote logging target. See [Configuring Secure Syslog Remote Logging Target, page 5-13](#) for more information.
2. Enable Logging Categories to send auditable events to the secure syslog remote logging target. See [Enabling Logging Categories to Send Auditable Events to the Secure Syslog Target, page 5-14](#) for more information.
3. Disable TCP Syslog and UDP syslog collectors. Only TLS-protected syslog collectors should be enabled. See [Disabling the TCP Syslog and UDP Syslog Collectors, page 5-15](#) for more information.

Configuring Secure Syslog Remote Logging Target

Cisco ISE system logs are collected and stored by log collectors for various purposes. You must choose the Cisco ISE Monitoring node as your log collector for configuring a secure syslog target.

-
- Step 1** Log in to the Admin portal.
- Step 2** Choose **Administration > System > Logging > Remote Logging Targets**.
- Step 3** Click **Add**.
- Step 4** Enter a name for the secure syslog server.
- Step 5** Choose Secure Syslog from the Target Type drop-down list.
- Step 6** Choose Enabled from the Status drop-down list.
- Step 7** Enter the IP address of the Cisco ISE Monitoring node in your deployment.
- Step 8** Enter 6514 as the port number. The secure syslog receiver listens on TCP port 6514.
- Step 9** Choose the syslog facility code. The default is LOCAL6.
- Step 10** Enter the maximum length. The default is 8192.
- Step 11** Check the **Include Alarms for this Target** check box for alarms to be sent to the syslog server if your remote secure syslog logging target is not a Cisco ISE node.
- If you are configuring your Cisco ISE node (Monitoring) as your secure syslog logging target, uncheck the **Include Alarms for this Target** check box.
- Step 12** Check the **Buffer Messages When Server is Down** check box. If this option is checked, Cisco ISE stores the logs if the secure syslog receiver is unreachable, periodically checks the secure syslog receiver, and forwards them when the secure syslog receiver comes up.
- Enter the buffer size.
 - Enter the Reconnect Timeout in seconds for Cisco ISE to periodically check the secure syslog receiver.
- Step 13** Select a CA certificate that you want Cisco ISE to present to the secure syslog server.
- Step 14** Uncheck the **Ignore Server Certificate validation** check box. You must not check this option.
- Step 15** Click **Submit**.
-

Enabling Logging Categories to Send Auditable Events to the Secure Syslog Target

You must enable logging categories for Cisco ISE to send auditable events to the secure syslog target.

-
- Step 1** Log in to the Admin portal.
- Step 2** Choose **Administration > System > Logging > Logging Categories**.
- Step 3** Click the radio button next to the AAA Audit logging category, then click **Edit**.
- Step 4** Choose WARN from the Log Severity Level drop-down list.
- Step 5** Move the secure syslog remote logging target that you created earlier to the Selected box.
- Step 6** Click **Save**.
- Step 7** Repeat this procedure to enable the following logging categories:
- Administrative and Operational Audit

- Posture and Client Provisioning Audit
-

Disabling the TCP Syslog and UDP Syslog Collectors

For Common Criteria compliance, you must disable the TCP and UDP syslog collectors, and only the secure syslog collector must be enabled.

-
- Step 1** Log in to the Admin portal.
 - Step 2** Choose **Administration > System > Logging > Remote Logging Targets**.
 - Step 3** Click the radio button next to the TCP or UDP syslog collector.
 - Step 4** Click **Edit**.
 - Step 5** Choose Disabled from the Status drop-down list.
 - Step 6** Click **Save**.
 - Step 7** Repeat this process until you disable all the TCP or UDP syslog collectors.
-



Managing Administrators and Admin Access Policies

A Cisco Identity Services Engine (ISE) administrator, also known as an admin user, manages and performs specific types of administrative tasks using the Cisco ISE Admin portal.

This chapter describes how Cisco ISE manages administrators and their access to role-based access-control (RBAC) policies, permissions, and settings.

Cisco ISE allows you to define role-based access control (RBAC) policies that allow or deny certain system-operation permissions to an administrator. These RBAC policies are defined based on the identity of individual administrators or the admin group to which they belong.

To further enhance security and control who has access to the Admin portal, you can:

- Configure administrative access settings based on the IP address of remote clients.
- Define strong password policies for administrative accounts.
- Configure session timeouts for administrative GUI sessions.

This chapter contains the following sections:

- [Cisco ISE Administrators, page 6-1](#)
- [Cisco ISE Administrator Groups, page 6-3](#)
- [Administrative Access to Cisco ISE, page 6-7](#)

Cisco ISE Administrators

Cisco ISE administrators use the Admin portal to:

- Manage deployments, help desk operations, network devices and node monitoring and troubleshooting.
- Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations.
- Change administrator and user passwords.

Administrators can access Cisco ISE through the command-line interface (CLI) or web-based interface. The username and password that you configure during Cisco ISE setup is intended only for administrative access to the CLI. This role is considered to be the CLI-admin user, also known as CLI administrator. By default, the username for the CLI-admin user is admin and the password is defined

during setup. There is no default password. This CLI-admin user is known as the default admin user. This default admin user account cannot be deleted, but can be edited by other administrators (which includes options to enable, disable, or change password for this account).

You can create an administrator or you can promote an existing user to an administrator role. Administrators can also be demoted to simple network user status by disabling the corresponding administrative privileges.

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

Administrators are assigned to one or more admin groups.

Related Topics

- [Cisco ISE Administrator Groups, page 6-3](#)
- [Creating a New Cisco ISE Administrator, page 6-2](#)

Privileges of a CLI Administrator Vs. a Web-Based Administrator

A CLI administrator 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 granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE deployments.

Creating a New Cisco ISE Administrator

Cisco ISE administrators need accounts with specific roles assigned to it to perform specific administrative tasks. You can create administrator accounts and assign one or more roles to it based on the administrative tasks that an administrator has to perform.

You can use the Admin Users page to view, create, modify, delete, change the status, duplicate, or search for attributes of Cisco ISE administrators.

-
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Users > Add**.
- Step 2** Choose 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 Administrator fields. Supported characters for the name field are # \$ ' () * + - . / @ _ .
Check the **External** check box only if you are using the RSA or RADIUS external identity source for authentication, and are creating the same administrator account in the internal identity source for authorization.
- Step 4** Click **Submit** to create the new administrator in the Cisco ISE internal database.
-

Related Topics

- [Cisco ISE Administrators, page 6-1](#)
- [Cisco ISE Administrator Groups, page 6-3](#)

Cisco ISE Administrator Groups

Administrator groups, also called as role-based access control (RBAC) groups in Cisco ISE, contain a number of administrators who belong to the same administrative group. All administrators who belong to the same group share a common identity and have the same privileges. An administrator's identity as a member of a specific administrative group can be used as a condition in authorization policies. An administrator can belong to more than one administrator group.

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

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.

The following table lists the admin groups that are predefined in Cisco ISE and the tasks that members from these groups can perform.

Table 6-1 *Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions*

Admin Group Role	Access Level	Permissions	Restrictions
Helpdesk Admin	Query monitoring and troubleshooting operations	• Run all reports • Run all troubleshooting flows • View the Cisco ISE dashboard and livelogs • View alarms	Cannot create, update, or delete reports, troubleshooting flows, live authentications, or alarms
Identity Admin	• Manage user accounts and endpoints • Manage identity sources	• Add, edit, and delete user accounts and endpoints • Add, edit, and delete identity sources • Add, edit, and delete identity source sequences • Configure general settings for user accounts (attributes and password policy) • View the Cisco ISE dashboard, livelogs, alarms, and reports. • Run all troubleshooting flows.	Cannot perform any policy management or system-level configuration tasks in Cisco ISE

Table 6-1 *Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions (continued)*

Admin Group Role	Access Level	Permissions	Restrictions
MnT Admin	Perform all monitoring and troubleshooting operations.	• 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)	Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE
Network Device Admin	Manage Cisco ISE network devices and network device repository.	• Read and write permissions on network devices • Read and write permissions on NDGs and all network resources object types • View the Cisco ISE dashboard, livelogs, alarms, and reports • Run all troubleshooting flows	Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE
Policy Admin	Create and manage policies for all Cisco ISE services across the network that are related to authentication, authorization, posture, profiler, and client provisioning.	• 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 and settings • View the Cisco ISE dashboard, livelogs, alarms, and reports • Run all troubleshooting flows	Cannot perform any identity management or system-level configuration tasks in Cisco ISE

Table 6-1 *Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions (continued)*

Admin Group Role	Access Level	Permissions	Restrictions
RBAC Admin	All tasks under the Operations menu except for the Endpoint Protection Service, and partial access to some menu items under Administration	- View the authentication details - Enable or disable endpoint protection service - Create, edit, and delete alarms; generate and view reports; and use Cisco 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 page. - View the Cisco ISE dashboard, livelogs, alarms, and reports - Run all troubleshooting flows	Cannot perform any identity management or system-level configuration tasks in Cisco ISE
Super Admin	All Cisco ISE administrative functions. The default administrator account belongs to this group.	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.	—

Table 6-1 Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions (continued)

Admin Group Role	Access Level	Permissions	Restrictions
System Admin	All Cisco ISE configuration and maintenance tasks.	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. • Read permissions on administrator account settings and administrator group settings • Read permissions on admin access and data access permissions along with the RBAC policy page • 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 Cisco ISE to troubleshoot problems in your network	Cannot perform any policy management or system-level configuration tasks in Cisco ISE
External RESTful Services (ERS) Admin ¹	Full access to all ERS API requests such as GET, POST, DELETE, PUT	• Create, Read, Update, and Delete ERS API requests	The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT
External RESTful Services (ERS) Guest	Read-only access to ERS API, only GET	• Can only Read ERS API requests	The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT

1. To know more about ERS APIs, refer to [Cisco Identity Services Engine API Reference Guide, Release 1.2](#)

Creating Admin Groups

The Admin Groups page allows you to view, create, modify, delete, duplicate, or filter Cisco ISE network admin groups.

Before You Begin

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 [Active Directory as an External Identity Source, page 14-9](#), [LDAP, page 14-19](#), [RADIUS Token Identity Sources, page 14-27](#), and [RSA Identity Sources, page 14-32](#).

-
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups**.
- Step 2** Click **Add**, and enter a Name and Description. Supported characters for the name field are: space, # \$ & ' () * + - . / @ _ .
- 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 stored 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.
- Step 4** Click **Add** to add users to the Admin Group Users table. From the Users list, 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.
-

Related Topics

- [Cisco ISE Administrator Groups, page 6-3](#)
- [Active Directory as an External Identity Source, page 14-9](#)
- [LDAP, page 14-19](#)
- [RADIUS Token Identity Sources, page 14-27](#)
- [RSA Identity Sources, page 14-32](#)

Administrative Access to Cisco ISE

Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrative tasks are critical and you must ensure that administrative access is restricted to users who are authorized to administer Cisco ISE in your network.

Cisco ISE allows you to control administrative access to its web interface through the following options:

- [Role-Based Access Control in Cisco ISE, page 6-8](#)
- [Administrator Access Settings, page 6-12](#)

Role-Based Access Control in Cisco ISE

Role-based access control policies (known as admin access) are access control policies that you define to provide limited access to the Cisco ISE administrative interface. These admin access policies allow you to customize the amount and type of access on a per-administrator or per-admin group basis using specified role-based access permission settings that apply to an individual admin user or an admin group.

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 to which the entity belongs, and the corresponding permissions and settings that are applied based upon the role of the entity.

Related Topics

[Cisco ISE Administrator Groups, page 6-3](#)

Role-Based Permissions

Cisco ISE allows you to configure permissions at the menu and data levels, called the menu access and data access permissions.

The menu access permissions allow you to show or hide the menu items of the Cisco ISE administrative interface. This feature lets you create permissions so that you can restrict or enable access at the menu level.

The data access permissions allow you to grant full or no access to the following data in the Cisco ISE interface: Admin Groups, User Identity Groups, Endpoint Identity Groups, Locations, and Device Types.

RBAC Policies

RBAC policies determine if an administrator 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 administrator based on the admin group by using RBAC policies. When administrators log in to the Admin portal, they can access menus and data that are based on the policies and permissions defined for the admin groups with which they are associated.

RBAC policies map admin groups to menu access and data access permissions. 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.

Related Topics

- [Role-Based Access Control in Cisco ISE, page 6-8](#)
- [Default Menu Access Permissions, page 6-8](#)
- [Default Data Access Permissions, page 6-10](#)

Default Menu Access Permissions

Cisco ISE provides an out of the box set of permissions that are associated with a set of predefined admin groups. Having predefined 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.

Cisco ISE provides a set of system defined menu access permissions that are already used in the default RBAC policies. [Table 6-2](#) lists the default menu access permissions.

Apart from the predefined menu access permissions, Cisco ISE also allows you to create custom menu access permissions that you can use in RBAC policies.

Table 6-2 **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 Device Menu Access	Network Device Admin	• Operations > All menu items • Administration > – Network Resources > All menu items
System Admin Menu Access	System Admin	• Operations > Authentication, Alarms, Reports, and Troubleshoot • Administration > – System > All menu items
RBAC Admin Menu Access	RBAC Admin	• Operations > All menu items except Endpoint Protection Service • 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.

Related Topics

- [Role-Based Access Control in Cisco ISE, page 6-8](#)

- [Configuring Menu Access Permissions, page 6-10](#)
- [Default Data Access Permissions, page 6-10](#)

Configuring Menu Access Permissions

Cisco ISE allows you to create custom menu access permissions that you can map to an RBAC policy. Depending on the role of the administrators, you can allow them to access only specific menu options.

-
- Step 1** Choose **Administration > System > Admin Access > Authorization > Permissions > Menu Access**.
- Step 2** Click **Add**, and enter values for the Name and Description fields.
- 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 Permissions for Menu Access area, click **Show**.
- Step 3** Click **Submit**.
-

Related Topics

- [Role-Based Access Control in Cisco ISE, page 6-8](#)
- [Role-Based Permissions, page 6-8](#)
- [Default Menu Access Permissions, page 6-8](#)
- [Default Data Access Permissions, page 6-10](#)

Default Data Access Permissions

Cisco ISE comes with a set of predefined data access permissions. 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. [Table 6-3](#) lists the default data access permissions.

RBAC policies are defined based on the administrator (RBAC) group, menu access, and data access permissions. You first create menu access and data access permissions and then create an RBAC policy that associates an admin group with the corresponding menu access and data access permissions. The RBAC policy takes the form:

If admin_group=*Super Admin* then assign *SuperAdmin Menu Access* permission + *SuperAdmin Data Access* permission.

Apart from the predefined data access permissions, Cisco ISE also allows you to create custom data access permissions that you can associate with an RBAC policy.

Table 6-3 **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

Related Topics

- [Role-Based Access Control in Cisco ISE, page 6-8](#)
- [Configuring Data Access Permissions, page 6-11](#)
- [Role-Based Permissions, page 6-8](#)
- [Default Menu Access Permissions, page 6-8](#)

Configuring Data Access Permissions

Cisco ISE allows you to create custom data access permissions that you can map to an RBAC policy. Based on the role of the administrator, you can choose to provide them access only to select data.

-
- Step 1** Choose **Administration > System > Admin Access > Authorization > Permissions**.
- Step 2** Choose **Permissions > Data Access**.
- Step 3** Click **Add**, and enter values for the Name and Description fields.
- Click to expand the admin group and select the desired admin group.
 - Click **Full Access**.
- Step 4** Click **Save**.
-

Related Topics

- [Role-Based Access Control in Cisco ISE, page 6-8](#)
- [Role-Based Permissions, page 6-8](#)
- [Default Menu Access Permissions, page 6-8](#)
- [Default Data Access Permissions, page 6-10](#)

Configuring Admin Access Policies

An Admin Access (RBAC) policy is represented in an *if-then* format, where *if* is the RBAC Admin Group value and *then* is the RBAC Permissions value.

The RBAC policies page contains a list of default policies. These default policies cannot be modified or deleted. This page also allows you to create custom RBAC policies for an admin group specifically for your work place, and apply to personalized admin groups.

Before You Begin

- Ensure that you have created all admin groups for which you want to define the RBAC policies.
- Ensure that these admin groups are mapped to the individual admin users.
- Ensure that you have configured the RBAC permissions, such as menu access and data access permissions.
- To perform the following task, you must be a Super Admin.

Step 1 Choose **Administration > System > Admin Access > Authorization > Policy**.

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

Step 2 Click **Actions** next to any of the default RBAC policy rule.

Here, you can insert new RBAC policies, duplicate an existing RBAC policy, and delete an existing RBAC policy.

Step 3 Click **Insert new policy**.

Step 4 Enter values for the Rule Name, RBAC Group(s), and Permissions fields.

You cannot select multiple menu access and data access permissions when creating an RBAC policy.

Step 5 Click **Save**.

Related Topics

- [Creating Admin Groups, page 6-6](#)
- [Cisco ISE Administrators, page 6-1](#)
- [Default Menu Access Permissions, page 6-8](#)

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.

Cisco ISE does not support administrator passwords with UTF-8 characters. You can configure the following administrative access settings:

- [Configuring the Maximum Number of Concurrent Administrative Sessions and Login Banners, page 6-13](#)
- [Allowing Administrative Access to Cisco ISE from Select IP Addresses, page 6-13](#)

- [Configuring a Password Policy for Administrator Accounts, page 6-14](#)
- [Configuring Session Timeout for Administrators, page 6-15](#)

Configuring the Maximum Number of Concurrent Administrative Sessions and Login Banners

You can configure the maximum number of concurrent administrative GUI or CLI (SSH) sessions and login banners that help and guide administrators who access your administrative web or CLI interface. You can configure login banners that appear before and after an administrator logs in. By default, these login banners are disabled.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > System > Admin Access > Settings > Access > Session .
Step 2	Enter the maximum number of concurrent administrative sessions that you want to allow through the GUI and CLI interfaces. The valid range for concurrent administrative GUI sessions is from 1 to 20. The valid range for concurrent administrative CLI sessions is 1 to 10.
Step 3	If you want Cisco ISE to display a message before an administrator logs in, check the Pre-login banner check box and enter your message in the text box.
Step 4	If you want Cisco ISE to display a message after an administrator logs in, check the Post-login banner check box and enter your message in the text box.
Step 5	Click Save .
-

Related Topics

- [Administrator Access Settings, page 6-12](#)
- [Allowing Administrative Access to Cisco ISE from Select IP Addresses, page 6-13](#)

Allowing Administrative Access to Cisco ISE from Select IP Addresses

Cisco ISE allows you to configure a list of IP addresses from which administrators can access the Cisco ISE management interfaces.

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 Inline Posture nodes.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > System > Admin Access > Settings > Access > IP Access .
Step 2	From the Configure IP List for Access Restriction area, click Add .
Step 3	Enter IP addresses in the classless interdomain routing (CIDR) format in the IP address field.
Step 4	Enter the subnet mask in the Netmask in CIDR format field.
Step 5	Click OK . Repeat the process to add more IP address ranges to this list.

Step 6 Click **Save** to save the changes.

Related Topics

- [Cisco ISE Administrators, page 6-1](#)
- [Cisco ISE Administrator Groups, page 6-3](#)

Configuring a Password Policy for Administrator Accounts

Cisco ISE also allows you to create a password policy for administrator accounts to enhance security. You can define whether you want a password based or client certificate based administrator authentication. The password policy that you define here is applied to all administrator accounts in Cisco ISE.



Note Cisco ISE does not support administrator passwords with UTF-8 characters.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > System > Admin Access > Authentication**.

Step 2 Select either of these authentication methods:

- **Password Based**—If you want to use the standard user ID and password credentials for an administrator login, choose the **Password Based** option and specify either the “Internal” or “External” authentication type.



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.

- **Client Certificate Based**—If you want to specify a certificate-based policy, choose the **Client Certificate Based** option, and select an existing Certificate Authentication Profile.

Step 3 Click the **Password Policy** tab and enter the values as described in [Administrator Password Policy Settings](#).



Note If you are using an external identity store 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.

Step 4 Click **Save** to save the administrator password policy.

Related Topics

- [Cisco ISE Administrators, page 6-1](#)
- [Creating Admin Groups, page 6-6](#)

- [Administrative Access to Cisco ISE Using an External Identity Store, page 6-16](#)

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 Admin portal.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > System > Admin Access > Settings > Session > Session Timeout .
Step 2	Enter the 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 .
-

Related Topics

- [Terminating an Active Administrative Session, page 6-15](#)
- [Cisco ISE Administrators, page 6-1](#)
- [Creating Admin Groups, page 6-6](#)
- [Session Timeout and Session Info Settings, page A-18](#)

Terminating an Active Administrative Session

Cisco ISE displays all active administrative sessions from which you can select any session and terminate at any point of time, if a need to do so arises. The maximum number of concurrent administrative GUI sessions is 20. If the maximum number of GUI sessions is reached, an administrator who belongs to the super admin group can log in and terminate some of the sessions.

Before You Begin

To perform the following task, you must be a Super Admin.

-
Step 1	Choose Administration > System > Admin Access > Settings > Session > Session Info .
Step 2	Check the check box next to the session ID that you want to terminate and click Invalidate .
-

Related Topics

[Session Timeout and Session Info Settings, page A-18](#)

Changing Administrator Name

Cisco ISE allows you to change your username from the GUI.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Log in to the Admin portal.
Step 2	Click your username that appears as a link at the upper right corner of the Cisco ISE UI.
Step 3	Enter the new username in the Admin User page that appears.
Step 4	Edit any other details about your account that you want to change.
Step 5	Click Save .
-

Administrative Access to Cisco ISE Using an External Identity Store

In Cisco ISE, you can authenticate administrators via an external identity store such as Active Directory, LDAP, or RSA SecureID. There are two models you can use to provide authentication via an external identity store:

- **External Authentication and Authorization**—There are no credentials that are specified in the local Cisco ISE database for the administrator, and authorization is based on external identity store group membership only. This model is used for Active Directory and LDAP authentication.
- **External Authentication and Internal Authorization**—The administrator's authentication credentials come from the external identity source, and authorization and administrator role assignment take place using the local Cisco ISE database. This model 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 the authentication process, 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 Admin portal. The Cisco ISE Command Line Interface (CLI) does not feature these functions.

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.

Related Topics

- [External Authentication and Authorization, page 6-17](#)
- [Active Directory as an External Identity Source, page 14-9](#)
- [LDAP, page 14-19](#)
- [RADIUS Token Identity Sources, page 14-27](#)

- [RSA Identity Sources, page 14-32](#)

External Authentication and Authorization

By default, Cisco ISE provides internal administrator authentication. To set up external authentication, you must create a password policy for the external administrator accounts that you define in 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.

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.

To configure external authentication, you must:

- Configure password-based authentication using an external identity store.
- Create an external administrator group.
- Configure menu access and data access permissions for the external administrator group.
- Create an RBAC policy for external administrator authentication.

Related Topics

- [Configuring a Password Policy for Administrator Accounts, page 6-14](#)
- [Configuring Cisco ISE for Administrator CAC Authentication, page 5-10](#)
- [Configuring a Password-Based Authentication Using an External Identity Store, page 6-17](#)
- [Creating an External Administrator Group, page 6-18](#)
- [Configuring Menu Access and Data Access Permissions for the External Administrator Group, page 6-18](#)
- [Creating an RBAC Policy for External Administrator Authentication, page 6-19](#)

Configuring a Password-Based Authentication Using an External Identity Store

You must first configure password-based authentication for administrators who authenticate using an external identity store such as Active Directory or LDAP.

-
Step 1	Choose 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. For example, the Active Directory instance that you have created.
Step 3	Configure any other specific password policy settings that you want for administrators who authenticate using an external identity store.
Step 4	Click Save .
-

Related Topics

[Administrator Password Policy Settings, page A-17](#)

Creating an External Administrator Group

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.

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.

-
- Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups > Add**.
- Step 2** Enter a name and optional description.
- Step 3** Choose the External radio button.
- If you have connected and joined to an Active Directory domain, your Active Directory instance name appears in the Name field.
- Step 4** From the External Groups drop-down list box, choose the Active Directory group that you want to map for this external administrator group.
- Click the “+” sign to map additional Active Directory groups to this external administrator group.
- Step 5** Click **Save**.
-

Related Topics

[Creating Admin Groups, page 6-6](#)

Configuring Menu Access and Data Access Permissions for the External Administrator Group

You must configure menu access and data access permissions that can be assigned to the external administrator group.

-
- Step 1** Choose **Administration > System > Admin Access > Permissions**.
- Step 2** Click one of the following:
- **Menu Access**—All administrators who belong to the external administrator group can be granted permission at the menu or submenu level. The menu access permission determines the menus or submenus that they can access.
 - **Data Access**—All administrators who belong to the external administrator group can be granted permission at the data level. The data access permission determines the data that they can access.
- Step 3** Specify menu access or data access permissions for the external administrator group.
- Step 4** Click **Save**.
-

Related Topics

- [Configuring Menu Access Permissions, page 6-10](#)
- [Default Data Access Permissions, page 6-10](#)

Creating an RBAC Policy for External Administrator Authentication

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 Cisco ISE menu and data access permissions to manage the 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.

Step 1 Choose **Administration > System > Admin Access > Authorization > Policy**.

Step 2 Specify the rule name, external administrator group, and permissions.

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.

Step 3 Click **Save**.

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 Admin portal.

Related Topics

- [Cisco ISE Administrator Groups, page 6-3](#)
- [Administrative Access to Cisco ISE Using an External Identity Store, page 6-16](#)

Configuring Admin Access Using an External Identity Store for Authentication with Internal Authorization

This method requires you to configure the same username in both the external identity store and the local Cisco ISE database. When you configure 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 and 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.

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

Step 2 Ensure that the administrator username in the external RSA identity store is also present in Cisco ISE. Ensure that you click the **External** option under Password.

**Note**

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**.

Related Topics

[Creating a New Cisco ISE Administrator, page 6-2](#)

External Authentication Process Flow

When the administrator logs in, the login session passes through the following steps in the process:

1. The administrator sends an 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**.

Upon logging in, the administrator sees only the menu and data access items that are specified in the RBAC policy.

Related Topics

[Administrative Access to Cisco ISE Using an External Identity Store, page 6-16](#)



Cisco ISE Licenses

This chapter describes the licensing mechanism and schemes that are available for Cisco ISE and how to add and upgrade licensees.

- [Cisco ISE Licensing, page 7-1](#)
- [Obtaining a Cisco ISE License from Cisco.com, page 7-4](#)
- [Adding or Upgrading a License, page 7-5](#)
- [Removing a License, page 7-6](#)

Cisco ISE Licensing

You must have a valid license for Cisco ISE. Licensing provides the ability to manage the application features and access, such as the number of concurrent endpoints that can use Cisco ISE network resources.

Licenses are centrally managed by the Administration node. Inline Posture and Policy Service nodes do not require separate licenses. If you have two Administration nodes deployed in a high-availability pair, you must ensure that each of them have the same license capabilities and add the licenses while each node is in a standalone or primary state.

After you install the Cisco ISE software and initially configure the appliance as the primary Administration node, you must obtain a license for Cisco ISE as described in [Obtaining a Cisco ISE License from Cisco.com, page 7-4](#) and then apply that license according to the instructions in [Adding or Upgrading a License, page 7-5](#). You apply all licenses to the Cisco ISE primary Administration node by using the primary and secondary Administration node hardware ID. The primary Administration node then centrally manages all the licenses that are installed for your deployment.

Cisco ISE, Release 1.2, supports licenses with two hardware IDs. You can obtain a license based on the hardware IDs of both the primary and secondary Administration nodes. For more information on Cisco ISE, Release 1.2 licenses, see the [Cisco Identity Services Engine Licensing Note](#).

To avoid expiration issues that are associated with Base or Advanced features in Cisco ISE, Cisco recommends replacing the default Evaluation License with both a Base and Advanced License at the same time.

- When you install a Base License over a default Evaluation License, the Base License overrides only the base license-related portion of the Evaluation License and keeps the Advanced License capabilities available for the remainder of the default Evaluation License duration.
- You cannot upgrade the Evaluation License to an Advanced License without first installing the Base License.

- When you install a Wireless License over a default Evaluation License, the Wireless License overrides the Evaluation License parameters with the specific duration and user count associated with the Wireless License.

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.

To avoid service disruption, Cisco ISE continues to provide services to endpoints that exceed license entitlement. Cisco ISE instead relies on RADIUS accounting functions to track concurrent endpoints on the network and generate alarms when endpoint counts exceed the licensed amounts:

- 80% Info
- 90% Warning
- 100% Critical

90-Day Evaluation License

All Cisco ISE appliances come with a 90-day Evaluation License that contains Base and Advanced License packages and support for 100 endpoints. The 90-day duration is based on the Cisco ISE system clock.

As the Evaluation License approaches the end of its 90-day period, the Cisco ISE system generates an alarm that prompts you to download and install a valid license. When the Evaluation License expires at the end of its 90-day period, the Admin portal prompts you to install a valid production license. 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.

Although the Evaluation License allows you to provide support for both wired and wireless users, purchasing and applying a Wireless License option cuts off support for any wired users that you may have been supporting during the evaluation period.

Related Topics

- [Base License, page 7-3](#)
- [Advanced License, page 7-3](#)
- [Wireless and Wireless Upgrade Licenses, page 7-4](#)

Base License

Base Licenses are installed by using the Admin portal. Like the Evaluation License, Cisco ISE tracks Base License concurrent user counts. Base Licenses are perpetual licenses that include the following standard Cisco ISE functions:

- Basic network access
- Guest management
- Link encryption

Related Topics

- [90-Day Evaluation License, page 7-2](#)
- [Advanced License, page 7-3](#)
- [Wireless and Wireless Upgrade Licenses, page 7-4](#)

Advanced License

Advanced Licenses are subscription based and can be installed only on top of the Base License. You cannot upgrade an Evaluation License to an Advanced License without first installing a Base License. The Advanced License activates the following important Cisco ISE functions:

- Profiler
- Posture
- Device registration and supplicant provisioning
- Security group access
- Endpoint protection services

Licenses are applied to active (authenticated) endpoints. Each authenticated endpoint requires a Base license. The number of Advanced licenses cannot exceed the number of base licenses, or the number of authenticated endpoints.

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

Related Topics

- [90-Day Evaluation License, page 7-2](#)
- [Base License, page 7-3](#)
- [Wireless and Wireless Upgrade Licenses, page 7-4](#)

Wireless and Wireless Upgrade Licenses

Like Advanced License packages, Wireless Licenses are subscription based, but Wireless Licenses cannot coexist on an Cisco Administration node with Base or Base and Advanced Licenses.

Wireless Licenses are designed to provide a flexible option exclusively for wireless service providers and offer essential Base License functions such as basic network access, guest services, and link encryption, as well as all Advanced License services, including profiler, posture, and security group access services.

Cisco ISE ensures that wireless customers are able to take advantage of the Wireless License options by allowing RADIUS Wireless authentication requests that originate from a wireless LAN controller (WLC), while dropping other authentication request types.

Wireless Upgrade Licenses are designed to support users that currently subscribe to a Wireless License model and decide to offer Cisco ISE support for non-wireless endpoints in the network as well. Rather than uninstall licenses and revert to a Base and Advanced License scheme, you can upgrade to a Wireless Upgrade License, which provides the full range of Cisco ISE functions and policy management capabilities for all wireless and non-wireless client-access methods, including wired and VPN Concentrator access.

You can only install a Wireless Upgrade License option on top of an existing Wireless License with the same allowable endpoint count. You cannot install a Wireless Upgrade on top of a Base plus Advanced License package.

Related Topics

- [90-Day Evaluation License, page 7-2](#)
- [Base License, page 7-3](#)
- [Advanced License, page 7-3](#)

Obtaining a Cisco ISE License from Cisco.com

To continue to use Cisco ISE services after the 90-day Evaluation License expires, and to support more than 100 concurrent endpoints on the network, you must install a Base, Base and Advanced, or Wireless license package for Cisco ISE. License files are based on a combination of the Cisco ISE hardware ID and Product Authorization Key (PAK). When you purchase Cisco ISE, or before the 90-day license expires, you can research the licensing options on Cisco.com and order the package that is suitable for your deployment of Cisco ISE.

If you have two Administration nodes deployed in a high-availability pair, you must ensure each of them have the same license capabilities and add the licenses while the node is in a standalone or primary state.

Within an hour of ordering your license files from Cisco.com, you should receive an e-mail with the Cisco Supplemental End-User License Agreement and a Claim Certificate containing a PAK for each license that you order. After receiving the Claim Certificate, you can log in and access the Cisco Product License Registration website at <http://www.cisco.com/go/license> and provide the appropriate hardware ID information and PAK to generate your license.

You must supply the following specific information to generate your license file:

- Product identifier (PID) of both the primary and secondary Administration nodes
- Version identifier (VID)
- Serial number (SN)

- PAK

See the [Cisco Identity Services Engine Licensing Note](#) for more details.

The day after you submit your license information in the Cisco Product License Registration website, you will receive an e-mail with your license file as an attachment. Save the license file to a known location on a local machine and use the instructions in [Adding or Upgrading a License, page 7-5](#) to add and update any product licenses for Cisco ISE.

For detailed information and license part numbers that are available for Cisco ISE, including licensing options for new installations as well as migration from an existing Cisco security product like Cisco Secure Access Control Server, see the Cisco Identity Services Engine Ordering Guidelines at http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5712/ps11637/ps11195/guide_c07-656177.html.

Related Topics

- [Determining Your Hardware ID Using the CLI, page 7-5](#)
- [Determining Your Hardware ID Using the Admin Portal, page 7-5](#)

Determining Your Hardware ID Using the CLI

Cisco ISE licenses are generated based on the Administration node hardware ID, *not* the MAC address.

To determine the Hardware ID, access the Cisco ISE direct-console CLI and enter the **show inventory** command. The output includes a line showing the PID, VID, and SN, similar to the following:

```
PID: NAC3315, VID: V01, SN: ABCDEFG
```

Determining Your Hardware ID Using the Admin Portal

Cisco ISE licenses are generated based on the Administration node hardware ID, *not* the MAC address.

If your current license has not expired, you can view the Administration node hardware ID by completing the following steps:

-
Step 1	From the Cisco ISE Administration interface, choose Administration > System > Licensing .
Step 2	In the License Operations navigation pane, click Current Licenses .
Step 3	Select the button corresponding to the Cisco ISE node that you want to check for the Administration node hardware ID, and click Administration Node to view the PID, VID, and SN.
-

Adding or Upgrading a License

You can add a license only on a standalone or a primary Administration 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:

- Install a Base license and then choose whether or not to also install an Advanced license
- Install a Wireless license

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.

Before You Begin

Make sure that you have obtained and installed an appropriate license on your Cisco ISE node. See [Obtaining a Cisco ISE License from Cisco.com, page 7-4](#) for more information.

-
- Step 1** From the Cisco ISE Administration interface, choose **Administration > System > Licensing > Current Licenses**.
 - Step 2** Click the radio button next to the license name that you want to upgrade, and click **Edit**.
 - Step 3** Click **Add Services**.
 - Step 4** Click **Browse** and select the Licence file.
 - Step 5** Click **Import** to import the new license file that supports the added service.
 - Step 6** 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.
-

Related Topics

- [License Page Parameters, page A-9](#)
- [Removing a License, page 7-6](#)

Removing a License

You can remove individual Base, Advanced, and Wireless licenses, but keep in mind the following conditions:

- If the Advanced package count is greater than the Base package count, then the Base package cannot be deleted.
- If you install a combined license, all related installations in the Base and Advanced packages are also removed.
- If you remove a production-level license within the standard 90-day evaluation period, the Evaluation License is automatically restored after you remove the production license.
- You cannot remove Evaluation Licenses.

Before You Begin

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.

-
- Step 1** Choose **Administration > System > Licensing > Current Licenses**.
 - Step 2** Click the radio button next to the relevant node name, and click **Edit**.
 - Step 3** Click the radio button next to the license name that you want to delete and click **Remove**.

Step 4 Click **OK**.



Managing Certificates

Certificates are used in a network to provide secure access. Certificates are used to identify Cisco ISE to an endpoint and also to secure the communication between that endpoint and the Cisco ISE node. Certificates are used for all HTTPS communication and the Extensible Authentication Protocol (EAP) communication.

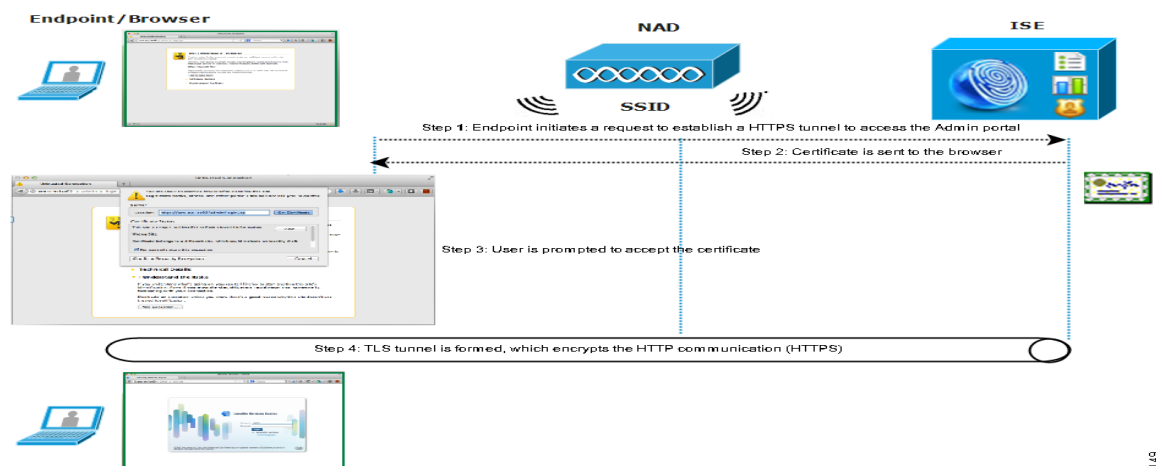
HTTPS Communication Using the Cisco ISE Certificate

All Cisco ISE web portals from release 1.1.0 onwards are secured using the HTTPS (TLS-encrypted HTTP communication) protocol:

- Administration Portal
- Centralized Web Authentication Portal
- Sponsor Portal
- Client Provisioning Portal
- My Devices Portal

Figure 8-1 shows an TLS-encrypted process when communicating with the Admin portal.

Figure 8-1 *HTTPS (TLS-Encrypted HTTP Communication)*



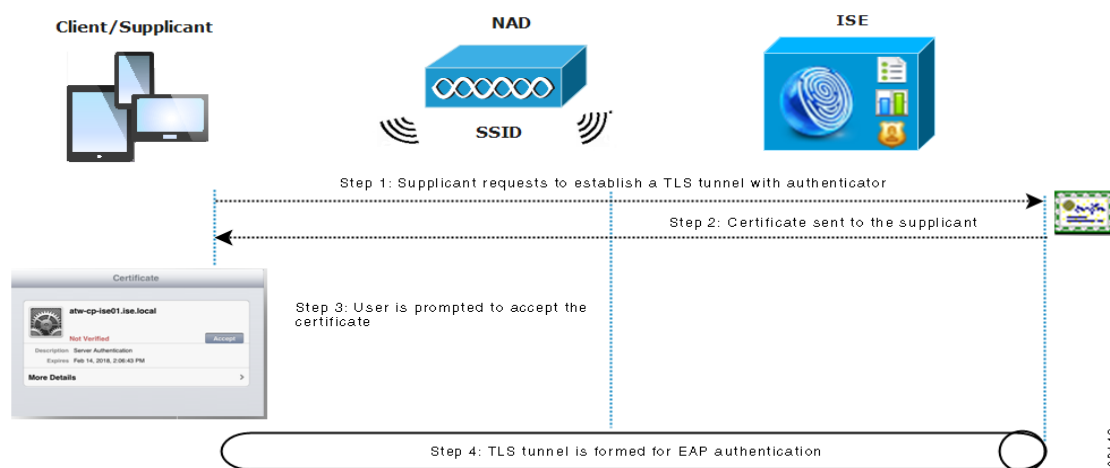
EAP Communication Using the Cisco ISE Certificate

Certificates are used with almost all EAP methods. The following EAP methods are commonly used:

- EAP-TLS
- PEAP
- EAP-FAST

For tunneled EAP methods, such as PEAP and FAST, Transport Layer Security (TLS) is used to secure the credential exchange. Similar to a request to a HTTPS web site, the client establishes a connection with the server. The server presents its certificate to the client. If the client trusts the certificate, the TLS tunnel is formed. The client's credentials are not sent to the server until after the tunnel is established, thereby ensuring a secure exchange. In a secure access deployment, the client is a supplicant, and the server is an ISE Policy Service node. [Figure 8-2](#) shows an example using PEAP.

Figure 8-2 EAP Communication



360148

Certificates Enable Cisco ISE to Provide Secure Access

The Cisco Identity Services Engine (ISE) relies on public key infrastructure (PKI) to provide secure communication with both endpoints and administrators, as well as between Cisco ISE nodes in a multinode deployment. PKI relies on X.509 digital certificates to transfer public keys for encryption and decryption of messages, and to verify the authenticity of other certificates representing users and devices. Cisco ISE provides the Admin Portal to manage the following two categories of X.509 certificates:

- **Local certificates**—These are server certificates that identify a Cisco ISE node to client applications. Every Cisco ISE node has its own local certificates, each of which are stored on the node along with the corresponding private key.
- **Certificate Store certificates**—These are certificate authority (CA) certificates used to establish trust for the public keys received from users and devices. The Certificate Store also contains certificates that are distributed by the Simple Certificate Enrollment Protocol (SCEP), which enables registration of mobile devices into the enterprise network. Certificates in the Certificate Store are managed on the primary Administration node, and are automatically replicated to all other nodes in an Cisco ISE deployment.

In a distributed deployment, you must import the certificate only in to the certificate trust list (CTL) of the primary Administration node. The certificate gets replicated to the secondary nodes.

In general, to ensure certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verification functions, use lower case hostnames for all Cisco ISE nodes deployed in a network.

Enabling PKI in Cisco ISE

You should enable PKI in Cisco ISE in the following way:

-
- Step 1** Establish local certificates on each deployment node for TLS-enabled authentication protocols (for example, EAP-TLS protocol), and for HTTPS, which is used by browser and REST clients to access the Cisco ISE web portals.

By default, a Cisco ISE node is preinstalled with a self-signed certificate that is used for both purposes. In a typical enterprise environment, this certificate is replaced with one or two server certificates that are signed by a trusted CA.

- Step 2** Populate the Certificate Store with the CA certificates that are necessary to establish trust with the user as well as device certificates that will be presented to Cisco ISE.

If a certificate chain consisting of a root CA certificate plus one or more intermediate CA certificates is required to validate the authenticity of a user or device certificate, you must import the entire chain into the Certificate Store.

Related Topics

- See [Local Certificates, page 8-4](#) for details on how to generate a Certificate Signing Request and import a CA-signed certificate.
- See [Certificate Store, page 8-24](#) for details on how to import these certificate chains.

The Cisco ISE nodes use HTTPS for inter-node communication, so an administrator must populate the Certificate Store with the trust certificate(s) needed to validate the HTTPS local certificate belonging to each node in the Cisco ISE deployment. If a default self-signed certificate is used for HTTPS, then you must export this certificate from each Cisco ISE node and import it into the certificate store. If you replace the self-signed certificates with CA-signed certificates, it is only necessary to populate the Certificate Store with the appropriate root CA and intermediate CA certificates. Be aware that you cannot register a node in a Cisco ISE deployment until you complete this step.

If a Cisco ISE deployment is to be operated in FIPS mode, you must ensure that all local and certificate store certificates are FIPS-compliant. This means that each certificate must have a minimum key size of 2048 bytes, and use SHA-1 or SHA-256 encryption.



Note

After you obtain a backup from a standalone Cisco ISE or primary Administration node, if you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore data. Otherwise, if you try to restore data using the older backup, communication between the nodes might fail.

This chapter contains the following sections:

- [Local Certificates, page 8-4](#)
- [Certificate Signing Requests, page 8-23](#)
- [Certificate Store, page 8-24](#)
- [Simple Certificate Enrollment Protocol Profiles, page 8-30](#)
- [OCSP Services, page 8-31](#)

Local Certificates

Cisco ISE local certificates are server certificates that identify a Cisco ISE node to client applications. Local certificates are:

- Used by browser and REST clients who connect to Cisco ISE web portals. You must use HTTPS protocol for these connections.
- Used to form the outer TLS tunnel with PEAP and EAP-FAST. These certificates can be used for mutual authentication with EAP-TLS, PEAP, and EAP-FAST.

You must install valid local certificates for HTTPS and EAP-TLS on each node in your Cisco ISE deployment. By default, a self-signed certificate is created on a Cisco ISE node during installation time, and this certificate is designated for HTTPS and EAP-TLS use (it has a key length of 1024 and is valid for one year). It is recommended that you replace the self-signed certificate with a CA-signed certificate for greater security.

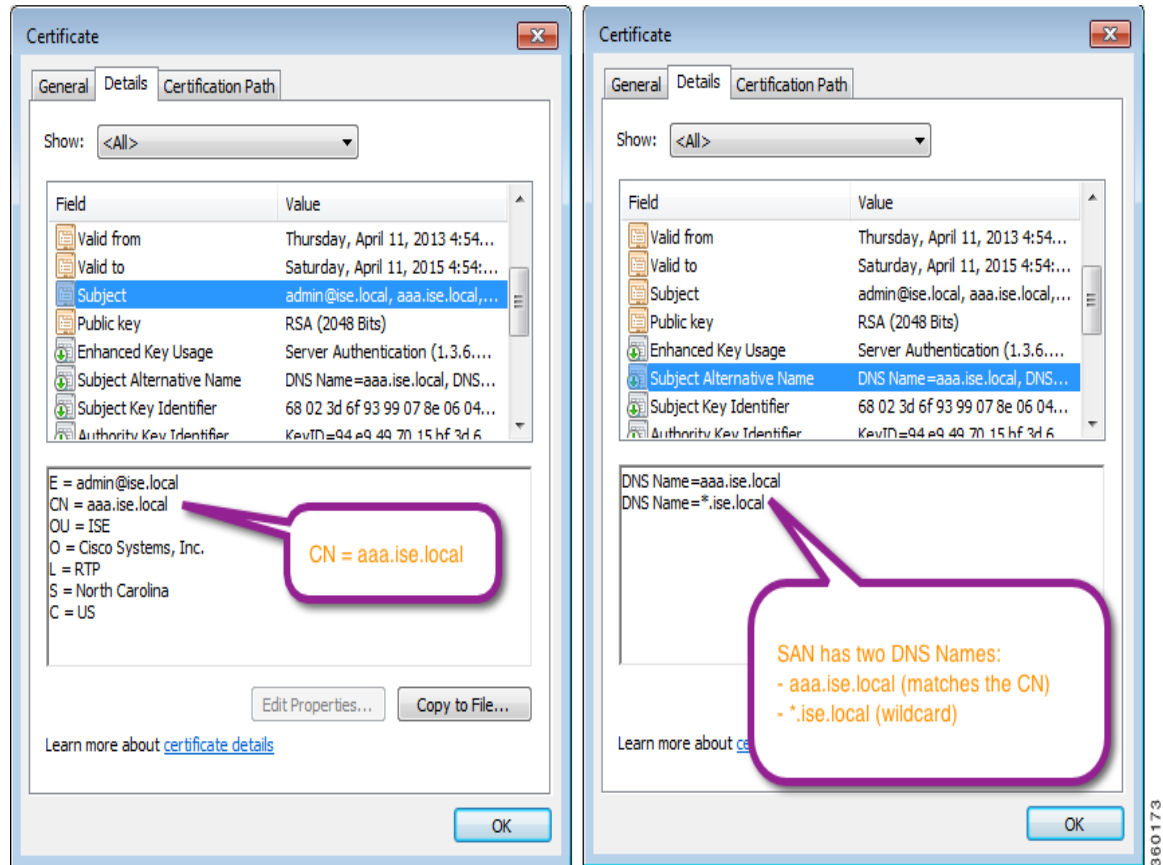
Wildcard Certificates

A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name) and allows the certificate to be shared across multiple hosts in an organization. For example, the CN value for the Certificate Subject would be some generic hostname such as `aaa.ise.local` and the SAN field would include the same generic hostname and the wildcard notation such as `DNS.1=aaa.ise.local` and `DNS.2=*.ise.local`

If you configure a wildcard certificate to use `*.ise.local`, you can use the same certificate to secure any other host whose DNS name ends with `“.ise.local,”` such as:

- `aaa.ise.local`
- `psn.ise.local`
- `mydevices.ise.local`
- `sponsor.ise.local`

[Figure 8-3](#) shows an example of a wildcard certificate that is used to secure a web site.

Figure 8-3 Wildcard Certificate Example

Wildcard certificates secure communications in the same way as a regular certificate, and requests are processed using the same validation methods.

Related Topics

- [Wildcard Certificates for HTTPS and EAP Communication, page 8-5](#)
- [Wildcard Certificate Support in Cisco ISE 1.2, page 8-6](#)
- [Fully Qualified Domain Name in URL Redirection, page 8-6](#)
- [Wildcard Certificate Compatibility, page 8-8](#)
- [Creating a Wildcard Certificate, page 8-8](#)
- [Installing Wildcard Certificates in Cisco ISE, page 8-10](#)

Wildcard Certificates for HTTPS and EAP Communication

You can use wildcard server certificates in Cisco ISE for HTTPS (web-based services) and EAP protocols that use SSL/TLS tunneling. With the use of wildcard certificates, you no longer have to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Using an asterisk (*) in the SAN field allows you to share a single certificate across multiple nodes in a deployment and helps prevent certificate name mismatch warnings. However, use of wildcard certificates is considered less secure than assigning a unique server certificate for each Cisco ISE node.

**Note**

If you use wildcard certificates, we strongly recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it can lead to serious security issues.

Wildcard certificate uses an asterisk (*) and a period before the domain name. For example, the CN value for a certificate's Subject Name would be a generic host name such as aaa.ise.local and the SAN field would have the wildcard character such as *.ise.local. Cisco ISE supports wildcard certifications in which the wildcard character (*) is the left most character in the presented identifier. For example, *.example.com or *.ind.example.com. Cisco ISE does not support certificates in which the presented identifier contains additional characters along with the wildcard character. For example, abc*.example.com or a*b.example.com or *abc.example.com.

Wildcard Certificate Support in Cisco ISE 1.2

Cisco ISE release 1.2 supports wildcard certificates. Prior to release 1.2, Cisco ISE verifies any certificate enabled for HTTPS to ensure the CN field matches the Fully Qualified Domain Name (FQDN) of the host exactly. If the fields did not match, the certificate could not be used for HTTPS communication.

Prior to release 1.2, Cisco ISE uses that CN value to replace the variable in the url-redirect A-V pair string. For all Centralized Web Authentication (CWA), onboarding, posture redirection, and so on, the CN value is used.

Cisco ISE 1.2 uses the hostname as the CN instead of relying on the CN field.

Fully Qualified Domain Name in URL Redirection

When Cisco ISE builds an authorization profile redirect (for central web authentication, device registration web authentication, native supplicant provisioning, mobile device management, and client provisioning and posture services), the resulting cisco-av-pair includes a string similar to the following:

url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

When processing this request, Cisco ISE substitutes actual values for some keywords in this string. For example, SessionIdValue is replaced with the actual session ID of the request. For eth0 interface, Cisco ISE replaces the IP in the URL with the FQDN of the Cisco ISE node. For non-eth0 interfaces, Cisco ISE uses the IP address in the URL. You can assign a host alias(name) for interfaces eth1 through eth3, which Cisco ISE can then substitute in place of IP address during URL redirection. To do this, you can use the **ip host** command in the configuration mode from the Cisco ISE CLI:

```
ISE /admin(config)# ip host IP_address host-alias FQDN-string
```

where *IP_address* is the IP address of the network interface (eth1 or eth2 or eth3)

host-alias is the name that you assign to the network interface

FQDN-string is the fully qualified domain name of the network interface

Using this command, you can assign a *host-alias* or an *FQDN-string* or both to a network interface.

Here is an example:

```
ISE/admin(config)# ip host a.b.c.d sales sales.amer.xyz.com
```

After you assign a host alias to the non-eth0 interface, you must restart the application services on Cisco ISE using the **application start ise** command.

Use the `no` form of this command to remove the association of the host alias with the network interface:
ISE/admin(config)# **no ip-host** *IP_address host-alias FQDN-string*

Use the **show running-config** command to view the host alias definitions.

If you provide the FQDN-string, Cisco ISE replaces the IP address in the URL with the FQDN. If you provide only the host alias, Cisco ISE combines the host alias with the configured IP domain name to form a complete FQDN, and replaces the IP address in the URL with the FQDN. If you do not map a network interface to a host alias, then Cisco ISE uses the IP address of the network interface in the URL.

When you make use of non-eth0 interfaces for client provisioning or native supplicant or guest flows, you have to make sure that the IP address or host alias for non-eth0 interfaces should be configured appropriately in the Policy Service node certificate's SAN fields.

Advantages of Using Wildcard Certificates

- Cost savings. Certificates signed by a third party Certificate Authority is expensive, especially as the number of servers increase. Wildcard certificates may be used on multiple nodes in the Cisco ISE deployment.
- Operational efficiency. Wildcard certificates allow all Policy Service Node (PSN) EAP and web services to share the same certificate. In addition to significant cost savings, certificate administration is also simplified by creating the certificate once and applying it on all the PSNs.
- Reduced authentication errors. Wildcard certificates address issues seen with Apple iOS devices where the client stores trusted certificates within the profile, and does not follow the iOS keychain where the signing root is trusted. When an iOS client first communicates with a PSN, it does not explicitly trust the PSN certificate, even though a trusted Certificate Authority has signed the certificate. Using a wildcard certificate, the certificate will be the same across all PSNs, so the user only has to accept the certificate once and successive authentications to different PSNs proceed without error or prompting.
- Simplified supplicant configuration. For example, Microsoft Windows supplicant with PEAP-MSCHAPv2 and server certificate trust enabled requires that you specify each of the server certificate to trust, or the user may be prompted to trust each PSN certificate when the client connects using a different PSN. With wildcard certificates, a single server certificate can be trusted rather than individual certificates from each PSN.
- Wildcard certificates result in an improved user experience with less prompting and more seamless connectivity.

Disadvantages of Using Wildcard Certificates

The following are some of the security considerations related to wildcard certificates:

- Loss of auditability and nonrepudiation
- Increased exposure of the private key
- Not common or understood by administrators

Wildcard certificates are considered less secure than a unique server certificate per ISE node. But, cost and other operational factors outweigh the security risk.

Security devices such as ASA also support wildcard certificates.

You must be careful when deploying wildcard certificates. For example, if you create a certificate with *.company.local and an attacker is able to recover the private key, that attacker can spoof any server in the company.local domain. Therefore, it is considered a best practice to partition the domain space to avoid this type of compromise.

To address this possible issue and to limit the scope of use, wildcard certificates may also be used to secure a specific subdomain of your organization. Add an asterisk (*) in the subdomain area of the common name where you want to specify the wildcard.

For example, if you configure a wildcard certificate for *.ise.company.local, that certificate may be used to secure any host whose DNS name ends in “.ise.company.local”, such as:

- psn.ise.company.local
- mydevices.ise.company.local
- sponsor.ise.company.local

Wildcard Certificate Compatibility

Wildcard certificates are usually created with the wildcard listed as the Common Name (CN) of the Certificate Subject, such as the example in [Figure 8-3](#). Cisco ISE release 1.2 supports this type of construction. However, not all endpoint supplicants support the wildcard character in the Certificate Subject.

All Microsoft native supplicants tested (including Windows Mobile) do not support wildcard character in the Certificate Subject.

You can use another supplicant, such as Cisco AnyConnect Network Access Manager (NAM) that might allow the use of wildcard character in the Subject field.

You can also use special wildcard certificates such as DigiCert's Wildcard Plus that is designed to work with incompatible devices by including specific subdomains in the Subject Alternative Name of the certificate.

Although the Microsoft supplicant limitation appears to be a deterrent to using wildcard certificates, there are alternative ways to create the wildcard certificate that allow it to work with all devices tested for secure access, including the Microsoft native supplicants.

To do this, instead of using the wildcard character in the Subject, you must use the wildcard character in the Subject Alternative Name (SAN) field instead. The SAN field maintains an extension designed for checking the domain name (DNS name). See RFCs 6125 and 2128 for more information.

For more information on Microsoft support of wildcard certificates, see:

<http://technet.microsoft.com/en-US/cc730460>

Creating a Wildcard Certificate

This section describes how to create a wildcard certificate. This procedure would work for most SSL certificate providers.

However, if your SSL certificate provider does not support wildcard values in the SAN field of the certificate, then you must populate the certificate SAN with the FQDN of each ISE node and interface (per the alias specified using the ip host command). This certificate is known as a multi-domain certificate. FQDNs for specific service aliases such as those used for the My Devices and Sponsor portals should also be included in the certificate SAN. Some services such as Local Web Authentication to the

ISE Admin portal, Sponsor portal, and the My Devices portal can use a load balancer. In these cases, the FQDN assigned to the virtual IP address of the load-balanced service should be included in the SAN field of the certificate.

**Note**

It is possible to have separate certificates for HTTPS and EAP authentication. The certificate designated for HTTPS is used to secure inter-node communications and all web portal services including Central Web Authentication, DRW, Posture Discovery and Assessment, Mobile Device Management, Native Supplicant Provisioning, Sponsor, and My Devices portals. The certificate designated for EAP is used to secure all client authentication using EAP protocols including PEAP, EAP-TLS, and EAP-FAST.

For example, if you have an ISE deployment with two PSN nodes (psn1 and psn2 with eth0, eth1, and eth2 interfaces enabled) and you want to create a multi-domain certificate without wildcards, then your values would be:

CN=aaa.company.local (FQDN of an ISE node in the deployment)

SAN=DNS.1=aaa.company.local, DNS.2=psn1.company.local, DNS.3=psn2.company.local, DNS.4=psn1-e1.company.local, DNS.5=psn2-e1.company.local, DNS.6=psn1-e2.company.local, DNS.7=psn2-e2.company.local.

**Tip**

If you are planning to deploy additional Policy Service nodes in the future, then you can add additional DNS name entries in the SAN field so that you can reuse the same certificate at the time of deploying the new nodes.

For cases where an IP address needs to be specified in the SAN field of the certificate (for example, DMZ with a static IP address for URL re-direction), ensure that you specify the IP address of the policy service node as the DNS Name and IP Address in the SAN field of the certificate. For example, CN=psn.ise.local and SAN=DNS.1=psn.ise.local, DNS.2=*.ise.local, DNS.3=10.1.1.20, IP.1=10.1.1.20.

Before You Begin

For Microsoft native supplicants, use the wildcard character in the SAN field of the certificate.

Step 1 Enter a generic hostname for the CN field of the Subject. For example, CN=aaa.ise.local.

Step 2 Enter the same generic hostname and a wildcard notation in the SAN field of the certificate. For example, DNS Name=aaa.ise.local, DNS Name=*.ise.local. See [Figure 8-3](#).

This method is successful with the majority of the tested public Certificate Authorities such as Comodo.com and SSL.com. With these public CAs, you must request a “Unified Communications Certificate (UCC).”

What To Do Next

Import the wildcard certificates in to the Policy Service nodes.

Related Topics

[Installing Wildcard Certificates in Cisco ISE, page 8-10](#)

Installing Wildcard Certificates in Cisco ISE

Before You Begin

If you have enabled non-eth0 interfaces, ensure that you map a host alias to that interface using the **ip host** command from the CLI. See [Fully Qualified Domain Name in URL Redirection](#) for more information.

To install wildcard certificates, you must perform the following tasks:

-
- Step 1** Create the Certificate Signing Request for Wildcard Certificates. See [Creating a Certificate Signing Request for Wildcard Certificates, page 8-10](#).
 - Step 2** Export the Certificate Signing Request. See [Exporting the Certificate Signing Request, page 8-11](#).
 - Step 3** Submit the Certificate Signing Request to a Certificate Authority. See [Submitting the CSR to a Certificate Authority, page 8-11](#).
 - Step 4** Import the Root Certificates to the Certificate Store. See [Importing the Root Certificates to the Certificate Store, page 8-12](#).
 - Step 5** Bind the Certificate Signing Request with the new public certificate. See [Binding the CSR With the New Public Certificate, page 8-13](#).
 - Step 6** Export the CA-Signed Certificate and Private Key. See [Exporting the CA-Signed Certificate and Private Key, page 8-13](#).
 - Step 7** Import the CA-Signed Certificate and Private Key in to all the Policy Service nodes. See [Importing the CA-Signed Certificate to the Policy Service Nodes, page 8-13](#).
-

Creating a Certificate Signing Request for Wildcard Certificates

-
- Step 1** Choose **Administration > Certificates > Local Certificates**.
 - Step 2** Click **Add > Generate Certificate Signing Request**.
 - Step 3** In the Certificate Subject, enter the generic FQDN of any one of your Policy Service nodes. For example, CN=psn.ise.local.
 - Step 4** Enter two values for the SAN. One of the values must be same as the CN that you entered for the Certificate Subject. The other value is the wildcard notation. For example, DNS name=psn.ise.local, DNS name=*.ise.local.
 - Step 5** Check the **Allow Wildcard Certificates** check box.

Figure 8-4 Certificate Signing Request Using a Wildcard Notation

Local Certificates > Generate Certificate Signing Request

Generate Certificate Signing Request

Certificate

* Certificate Subject:

▼ Subject Alternative Name (SAN)

DNS Name	Value	Remove	Add
DNS Name	psn.ise.local	—	+
DNS Name	*.ise.local	—	+

* Key Length:

* Digest to Sign With:

☒ Allow Wildcard Certificates

Step 6 Click **Submit**.

Exporting the Certificate Signing Request

- Step 1** Choose **Administration > Certificates > Certificate Signing Requests**.
- Step 2** Check the check box next to the CSR that you generated. For example, psn.ise.local.
- Step 3** Click **Export**.
- Step 4** Save the CSR to your local system.

Submitting the CSR to a Certificate Authority

- Step 1** Open the CSR in a text editor such as Notepad.
- Step 2** Copy all the text from “-----BEGIN CERTIFICATE REQUEST-----” through “-----END CERTIFICATE REQUEST-----.”
- Step 3** Paste the contents of the CSR in to the certificate request of a chosen CA. See [Figure 8-5](#).

Figure 8-5 CSR Content in a Certificate Request Form - Active Directory CA

Microsoft Active Directory Certificate Services -- ise-ATW-CP-AD-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request (from a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```

jOjvC3L8YJqX6tBcEMEDrcNE0dWkc3KRZWkZz4N0
wtFcD+Jqw7LhpVU7uIEI5EsYr+DbPtkg2GpxCary.
9MChvat71+7V22couHdiEODkMcSQELRn0YD1xi7.
AldRRWZspKfDUtNaa6G+wGontN1jUMsHxRHcCX+H
oOFht/K3FyHJxKCzDvAqqlIgepG3D64uDJLGuvhO
-----END CERTIFICATE REQUEST-----

```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

360147

Step 4 Download the signed certificate.

Some CAs might email the signed certificate to you. The signed certificate is in the form of a zip file that contains the newly issued certificate and the public signing certificates of the CA that you must add to the Cisco ISE trusted certificate store. See Figure 8-6.

Figure 8-6 Certificates Returned By the CA

Name	Date Modified	Size	Kind
FromComodo	Today 2:14 PM	--	Folder
12938541.crt	Apr 25, 2013 12:00 AM	2 KB	certificate
AddTrustExternalCARoot.crt	May 30, 2000 10:48 AM	2 KB	certificate
COMODOSSLCA.crt	Aug 23, 2011 12:00 AM	2 KB	certificate

Signed Public Certificate for ISE

Root Cert to be Trusted

Another Root Cert to be Trusted

360150

Importing the Root Certificates to the Certificate Store

Before You Begin

Before we bind the newly signed certificate to the CSR on Cisco ISE, ensure that the signing root certificates exist in the Cisco ISE Certificate Store.

-
- Step 1** Choose **Administration > Certificates > Certificate Store**.
 - Step 2** Click **Import**.
 - Step 3** Choose the root certificates returned by your CA.
-

Binding the CSR With the New Public Certificate

-
- Step 1** Choose **Administration > Certificates > Local Certificates**.
 - Step 2** Click **Add > Bind CA signed Certificate**.
 - Step 3** Choose the CA-signed certificate.
 - Step 4** Check the **Allow Wildcard Certificates** check box.
 - Step 5** Choose the protocol.
 - Step 6** Click **Submit**.
-

Exporting the CA-Signed Certificate and Private Key

-
- Step 1** Choose **Administration > Certificates > Local Certificates**.
 - Step 2** Check the check box next to the CA-signed certificate and click **Export**.
 - Step 3** Save the file to your local system.
-

Importing the CA-Signed Certificate to the Policy Service Nodes

-
- Step 1** Choose **Administration > Certificates > Certificate Store**.
 - Step 2** Choose the CA-signed certificate that you exported.
 - Step 3** Click **Submit**.
-

Installing a CA-Signed Certificate in Cisco ISE

The procedure for installing a CA-signed certificate is as follows:

-
- Step 1** In the Cisco ISE administration interface of the node requiring the CA-signed certificate, generate a Certificate Signing Request (CSR).
 - Step 2** Export the CSR into a file.
 - Step 3** Provide the CSR file to the Certificate Authority and request the CA to create and sign a certificate using the attributes specified in the CSR. The CA should return the certificate in a file.

- Step 4** In the Cisco ISE administration interface of the same node, bind the CA-signed certificate to its private key, which is kept with the CSR on the node. Designate the certificate for HTTPS and/or EAP-TLS use.
-

**Note**

If you are going to use the CA-signed certificate for HTTPS, the subject Common Name value specified for the CSR must match the fully qualified domain name (FQDN) of the Cisco ISE node, or must match the wildcard domain name specified in the SAN/CN field of the certificate.

Cisco ISE checks for a matching subject name as follows:

1. Cisco ISE looks at the subject alternative name (SAN) extension of the certificate. If the SAN contains one or more DNS names, then one of the DNS names must match the FQDN of the Cisco ISE node. If a wildcard certificate is used, then the wildcard domain name must match the domain in the Cisco ISE node's FQDN.
2. If there are no DNS names in the SAN, or if the SAN is missing entirely, then the Common Name (CN) in the Subject field of the certificate or the wildcard domain in the Subject field of the certificate must match the FQDN of the node.
3. If no match is found, the certificate is rejected.

**Note**

X.509 certificates imported to Cisco ISE must be in privacy-enhanced mail (PEM) or distinguished encoding rule (DER) format. Files containing a certificate chain, which is a local certificate along with the sequence of trust certificates that sign it, can be imported, subject to certain restrictions. See [Importing Certificate Chains, page 8-28](#) for more information.

X.509 certificates are only valid until a specific date. When a local certificate expires, the Cisco ISE functionality that depends on the certificate is impacted. Cisco ISE will notify you about the pending expiration of a local certificate when the expiration date is within 90 days. This notification appears in several ways:

- Colored expiration status icons appear in the Local Certificates page.
- Expiration messages appear in the Cisco ISE System Diagnostic report.
- Expiration alarms are generated at 90 days, 60 days, and every day in the final 30 days before expiration.

If the expiring certificate is a self-signed certificate, you can extend its expiration date by editing the certificate. For a CA-signed certificate, you must allow sufficient time to acquire replacement certificate from your CA.

You can perform the following tasks from the Cisco ISE administration interface to manage local certificates:

- View a list of the local certificates stored on an Cisco ISE node. The list shows the protocol assignment (HTTPS, EAP-TLS) of each certificate, along with its expiration status.
- Generate a CSR
- Export a CSR
- Bind a CA-signed certificate to its private key
- Export a local certificate and, optionally, its private key
- Import a local certificate and its private key

- Generate a self-signed local certificate
- Edit a local certificate, which includes extending the expiration date if the certificate is self-signed
- Delete a local certificate
- Delete a CSR

This section contains the following topics:

- [Viewing Local Certificates, page 8-15](#)
- [Adding a Local Certificate, page 8-16](#)
- [Editing a Local Certificate, page 8-21](#)
- [Exporting a Local Certificate, page 8-22](#)

Related Topics

- [Wildcard Certificates, page 8-4](#)
- [Fully Qualified Domain Name in URL Redirection, page 8-6](#)
- [Importing a Local Certificate, page 8-16](#)
- [Generating a Certificate Signing Request, page 8-19](#)
- [Binding a CA-Signed Certificate, page 8-20](#)

Viewing Local Certificates

The Local Certificate page lists all the local certificates added to Cisco ISE.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > System > Certificates > Local Certificates**.

The Local Certificate page appears and provides the following information for the local certificates:

- Friendly Name—Name of the certificate.
- Protocol—Protocols for which to use this certificate.
- Issued To—Common Name of the certificate subject.
- Issued By—Common Name of the certificate issuer
- Valid From—Date on which the certificate was created, also known as the Not Before certificate attribute.
- Expiration Date—Expiration date of the certificate, also known as the Not After certificate attribute.
- Expiration Status—Indicates when the certificate expires. There are five categories along with an associated icon that appear here:
 1. Expiring in more than 90 days (green icon)
 2. Expiring in 90 days or less (blue icon)
 3. Expiring in 60 days or less (yellow icon)
 4. Expiring in 30 days or less (orange icon)

5. Expired (red icon)

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Wildcard Certificates, page 8-4](#)

Adding a Local Certificate

You can add a local certificate to Cisco ISE in one of the following ways:

- [Importing a Local Certificate, page 8-16](#)
- [Generating a Self-Signed Certificate, page 8-18](#)
- [Generating a Certificate Signing Request, page 8-19](#) and [Binding a CA-Signed Certificate, page 8-20](#)

If you are planning to import a wildcard certificate, ensure that you have read the following sections:

- [Wildcard Certificates, page 8-4](#)
- [Creating a Wildcard Certificate, page 8-8](#)
- [Installing Wildcard Certificates in Cisco ISE, page 8-10](#)



Note

If you are using Firefox and Internet Explorer 8 browsers and 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 to see the new certificate.

Importing a Local Certificate

You can add a new local certificate by importing a local certificate.

Before You Begin

Ensure that you have the local certificate and the private key file on the system that is running the client browser.

To perform the following task, you must be a Super Admin or System Admin.

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.

Step 1 Choose **Administration > System > Certificates > Local Certificates**.

To import a local certificate to a secondary node, choose **Administration > System > Server Certificate**.

Step 2 Choose **Add > Import Local Server Certificate**.

Step 3 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 4 Enter a Friendly Name for the certificate. 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 Check the **Enable Validation of Certificate Extensions** check box if you want Cisco ISE to validate certificate extensions.

If you check the **Enable Validation of Certificate Extensions** check box and the certificate that you are importing contains a basic constraints extension with the 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 6 Check the **Allow Wildcard Certificates** check box if you want to import a wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name).

Step 7 In the Protocol group box:

- Check the **EAP** check box to use this certificate for EAP protocols to identify the Cisco ISE node.
- Check the **HTTPS** check box to use this certificate to authenticate the web server.

If you check the Management Interface check box, ensure that the Common Name value in the Certificate Subject matches the fully qualified domain name (FQDN) of the node or a wildcard notation if a wildcard certificate is used. Otherwise, the import process will fail.

Step 8 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 RSA key size must be 2048 bits or greater in size and use either SHA-1 or SHA-256 hash algorithm.

Step 9 Click **Submit** to import the local certificate.

If you import a local certificate to your primary Cisco ISE node and 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 Cisco ISE node.

To restart the secondary nodes from the CLI, enter the following commands in the given order:

- a. **application stop ise**
- b. **application start ise**

Refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.2* for more information on these commands.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Wildcard Certificates, page 8-4](#)
- [Creating a Wildcard Certificate, page 8-8](#)
- [Installing Wildcard Certificates in Cisco ISE, page 8-10](#)

Generating a Self-Signed Certificate

You can add a new local certificate by generating a self-signed certificate. Cisco recommends that you only employ self-signed certificates for your internal testing and evaluation needs. If you are planning to deploy Cisco ISE in a production environment, be sure to use CA-signed certificates whenever possible to ensure more uniform acceptance around a production network.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Administration > System > Certificates > Local Certificates**.
- To generate a self-signed certificate from a secondary node, choose **Administration > System > Server Certificate**.
- Step 2** Choose **Add > Generate Self Signed Certificate**.
- Step 3** Enter the following information in the Generate Self Signed Certificate page:
- **Certificate Subject**—A distinguished name (DN) identifying the entity that is associated with the certificate. The DN must include a Common Name (CN) value.
 - **Subject Alternative Name**—A DNS name or IP Address that is associated with the certificate.
 - **Required Key Length**—Valid values are 512, 1024, 2048, and 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 TTL**. You can specify an expiration 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 4** Check the **Allow Wildcard Certificates** check box if you want to generate a self-signed wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name. For example, DNS name assigned to the SAN can be *.amer.cisco.com.
- Step 5** In the Protocol group box:
- Check the **EAP** check box to use this certificate for EAP protocols that use SSL/TLS tunneling.
 - Check the **HTTPS** check box to use this certificate to authenticate the Cisco ISE portals.
- If you check the Management Interface check box, ensure that the Common Name value in the Certificate Subject matches the fully qualified domain name (FQDN) of the node. Otherwise, the self-signed certificate will not be generated.
- If the HTTPS check box is checked, then the Primary Administration node in a deployment will be restarted.
- 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 generate the certificate.



Note

If you are using a self-signed certificate and you must change the hostname of your Cisco ISE node, you must log in to the Admin portal of the Cisco ISE node, delete the self-signed certificate that has the old hostname, and generate a new self-signed certificate. Otherwise, Cisco ISE will continue to use the self-signed certificate with the old hostname.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Wildcard Certificates, page 8-4](#)
- [Installing Wildcard Certificates in Cisco ISE, page 8-10](#)

Generating a Certificate Signing Request

You can add a new local certificate by generating a certificate signing request and then binding a CA-signed certificate.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > System > Certificates > Local Certificates**.

To generate a CSR from a secondary node, choose **Administration > System > Server Certificate**.

Step 2 Choose **Add > Generate Certificate Signing Request**.

Step 3 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
- ST = Test state or province
- L = Test locality (City)
- O = Organization name
- OU = Organizational unit name
- CN = Common name
- E = E-mail address

For example, the Certificate Subject in a CSR can take the following values: “CN=Host-ISE.cisco.com, OU=Cisco, O=security, C=US, ST=NC, L=RTP, e=test@test.com” or “CN=aaa.amer.cisco.com, DNS name in SAN=*.amer.cisco.com, OU=Cisco, O=security, C=US, ST=NC, L=RTP, e=abc@xyz.com.”



Note

When populating the Certificate Subject field, do not encapsulate the string in quotation marks.

If you intend to use the certificate generated from this CSR for HTTPS communication, ensure that the common name 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 4 Subject Alternative Name—A DNS name or IP Address that is associated with the 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 RSA key size must be 2048 bits or greater in size and use either SHA-1 or SHA-256 hash algorithm.

Step 6 Check the **Allow Wildcard Certificates** check box if the Certificate Subject contains a CN or SAN with a wildcard FQDN.

Step 7 Click **Submit** to generate a CSR.

A CSR and its private key are generated and stored in Cisco 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.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Wildcard Certificates, page 8-4](#)
- [Creating a Certificate Signing Request for Wildcard Certificates, page 8-10](#)

Binding a CA-Signed Certificate

After a Certificate Signing Request is signed by a Certificate Authority and returned to you, you must bind the CA-signed certificate with its private key to complete the process of adding a local certificate in Cisco ISE.

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > System > Certificates > Local Certificates**.

To bind a CA-signed certificate to a secondary node, choose **Administration > System > Server Certificate**.

Step 2 Choose **Add > Bind CA Certificate**.

Step 3 Click **Browse** to choose the CA-signed certificate and choose the appropriate CA-signed certificate.

Step 4 Specify a **Friendly Name** for the certificate. 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 Check the **Enable Validation of Certificate Extensions** check box if you want Cisco ISE to validate certificate extensions.



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 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 6** Check the **Allow Wildcard Certificates** check box to bind a certificate that contains the wildcard character, asterisk (*) in any CN in the Subject or DNS in the Subject Alternative Name.
- Step 7** In the Protocol group box:
- Check the **EAP** check box to use this certificate for EAP protocols that use SSL/TLS tunneling.
 - Check the **HTTPS** check box to use this certificate to authenticate the Cisco ISE web portal.
- If you check the Management Interface check box, ensure that the Common Name value in the Certificate Subject matches the fully qualified domain name (FQDN) of the node or a wildcard notation if a wildcard certificate is used. Otherwise, the bind operation will fail.
- If the HTTPS check box is checked, then the Primary Administration node in a deployment will be restarted.
- Step 8** 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.
-

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Wildcard Certificates, page 8-4](#)
- [Installing Wildcard Certificates in Cisco ISE, page 8-10](#)

Editing a Local Certificate

You can use this page to edit local certificates.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Administration > System > Certificates > Local Certificates**.
- To edit a local certificate on a secondary node, choose **Administration > System > Server Certificate**.
- Step 2** Check the check box next to the certificate that you want to edit, and click **Edit**.
- Step 3** You can edit the following:
- Friendly name
 - Description
 - Protocols
 - Expiration TTL (if the certificate is self-signed)
- Step 4** Enter an optional friendly name and description to identify this certificate.
- Step 5** In the Protocol group box:
- Check the **EAP** check box to use this certificate for EAP protocols that use SSL/TLS tunneling.
 - Check the **HTTPS** check box to use this certificate to authenticate the Cisco ISE web portal.

If the HTTPS check box is checked, then the Primary Administration node in a deployment will be restarted.

**Note**

If you check the Management Interface check box, ensure that the Common Name value in the Certificate Subject matches the fully qualified domain name (FQDN) of the node or a wildcard notation if a wildcard certificate is used. If the Common Name value is blank, 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 6** Check the **Renew Self Signed Certificate** check box if you are editing a self-signed certificate and want to extend the Expiration Date.
- Step 7** Enter the Expiration TTL (Time to Live) in days, weeks, months, or years.
- Step 8** Click **Save** to save your changes.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Wildcard Certificates, page 8-4](#)
- [Creating a Wildcard Certificate, page 8-8](#)
- [Installing Wildcard Certificates in Cisco ISE, page 8-10](#)

Exporting a Local Certificate

You can export a selected local certificate or a certificate and its associated private key. If you export a certificate and its private key for backup purposes, you can reimport them later if needed.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

- Step 1** Choose **Administration > System > Certificates > Local Certificates**.
To export a local certificate from a secondary node, choose **Administration > System > Server Certificate**.
- Step 2** Check the check box next to the certificate that you want to export and then click **Export**.
- Step 3** Choose whether to export only the certificate, or the certificate and its associated private key.

**Tip**

We do not recommend exporting the private key associated with a certificate because its value may be exposed. If you must export a private key, specify an encryption password for the private key. You will need to specify this password while importing this certificate into another Cisco ISE server to decrypt the private key.

- 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 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.
-

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Importing a Local Certificate, page 8-16](#)

Certificate Signing Requests

The list of Certificate Signing Requests (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.

**Note**

If your Cisco ISE deployment has multiple nodes in a distributed setup, you must export the CSRs from each node in your deployment individually.

Related Topic

[Exporting Certificate Signing Requests, page 8-23](#)

Exporting Certificate Signing Requests

You can use this page to export certificate signing requests.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

- Step 1** Choose **Administration > System > Certificates > Certificate Signing Requests**.
- If you want to export CSRs from a secondary node, choose **Administration > System > Certificate Signing Requests**.
- Step 2** Check the check box next to the certificates that you want to export, and click **Export**.
- Step 3** Click **OK** to save the file to the file system that is running the client browser.
-

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Wildcard Certificates, page 8-4](#)

Certificate Store

The Cisco ISE Certificate Store contains X.509 certificates that are used for trust and for Simple Certificate Enrollment Protocol (SCEP). The certificates in the Certificate Store are managed on the primary administration node, and are replicated to every node in the Cisco ISE deployment.

Cisco ISE supports wildcard certificates.

Cisco ISE uses the Certificate Store certificates for the following purposes:

- To verify client certificates used for authentication by endpoints, and by Cisco ISE administrators accessing the Admin Portal using certificate-based administrator authentication.
- To enable secure communication between Cisco ISE nodes in a deployment. The Certificate Store must contain the chain of CA certificates needed to establish trust with the local HTTPS server certificate on each node in a deployment.
 - If a self-signed certificate is used for the server certificate, the self-signed certificate from each node must be placed in the Certificate Store of the primary Administration node.
 - If a CA-signed certificate is used for the server certificate, the CA root certificate, as well as any intermediate certificates in the trust chain, must be placed in the Certificate Store of the primary Administration node.
- To enable secure LDAP authentication. A certificate from the Certificate Store must be selected when defining an LDAP identity source that will be accessed over SSL.
- For distribution to mobile devices preparing to register in the network using the My Devices portal. Cisco ISE implements the SCEP on Policy Service Nodes (PSN) to support mobile device registration. A registering device uses the SCEP protocol to request a client certificate from a PSN. The PSN contains a registration authority (RA) that acts as an intermediary; it receives and validates the request from the registering device, and then forwards the request to a CA, which actually issues the client certificate. The CA sends the certificate back to the RA, which returns it to the device.

Each SCEP CA used by Cisco ISE is defined by a SCEP RA Profile. When a SCEP RA Profile is created, two certificates are automatically added to the Certificate Store:

- a. A CA certificate (a self-signed certificate)
- b. An RA certificate (a Certificate Request Agent certificate), which is signed by the CA.

The SCEP protocol requires that these two certificates be provided by the RA to a registering device. By placing these two certificates in the Certificate Store, they are replicated to all PSN nodes for use by the RA on those nodes.

**Note**

X.509 certificates imported to Cisco ISE must be in Privacy-Enhanced Mail (PEM) or Distinguished Encoding Rule (DER) format. Files containing a certificate chain, that is, a local certificate along with the sequence of trust certificates that sign it, can be imported, subject to certain restrictions.

**Note**

Performance Issues:

The default configuration of the maximum processes for SCEP module on the Windows CA server is set as 1. Increasing the value of maximum processes (say to 20) would improve the device registration performance. The performance could further be improved with a faster disk, for example an SSD.

Related Topics

- [Configuring a Password Policy for Administrator Accounts, page 6-14](#)
- [Adding LDAP Identity Sources, page 14-24](#)
- [Simple Certificate Enrollment Protocol Profiles, page 8-30](#)
- [Importing Certificate Chains, page 8-28](#)
- [Expiration of X.509 Certificates, page 8-25](#)
- [CA Certificate Naming Constraint, page 8-25](#)
- [Viewing Certificate Store Certificates, page 8-27](#)
- [Changing the Status of a Certificate in Certificate Store, page 8-27](#)
- [Adding a Certificate to Certificate Store, page 8-27](#)
- [Editing a Certificate Store Certificate, page 8-28](#)
- [Exporting a Certificate from the Certificate Store, page 8-28](#)

Expiration of X.509 Certificates

X.509 certificates are only valid until a specific date. Once a Certificate Store certificate expires, the Cisco ISE functionality that depends on the certificate is impacted. Cisco ISE notifies you about the pending expiration of a certificate when the expiration date is within 90 days. This notification appears in several ways:

- Colored expiration status icons appear in the Certificate Store page.
- Expiration messages appear in the Cisco ISE System Diagnostic report.
- Expiration alarms are generated at 90 days, 60 days, and every day in the final 30 days before expiration.

The Certificate Store is prepopulated with two Cisco CA certificates: a Manufacturing certificate and a Root certificate. The Root certificate signs the Manufacturing certificate. These certificates are disabled by default. If you have Cisco IP phones as endpoints in your deployment, you should enable these two certificates so the Cisco-signed client certificates for the phones can be authenticated.

This section contains the following topics:

- [Viewing Certificate Store Certificates, page 8-27](#)
- [Adding a Certificate to Certificate Store, page 8-27](#)
- [Editing a Certificate Store Certificate, page 8-28](#)
- [Exporting a Certificate from the Certificate Store, page 8-28](#)
- [Importing Certificate Chains, page 8-28](#)
- [Installation of CA Certificates for Cisco ISE Inter-node Communication, page 8-29](#)

CA Certificate Naming Constraint

A CA certificate in CTL may contain a name constraint extension. This extension defines a namespace for values of all subject name and subject alternative name fields of subsequent certificates in a certificate chain. Cisco ISE does not check constraints specified in a root certificate.

The following name constraints are supported:

- Directory name

The Directory name constraint should be a prefix of the directory name in subject/SAN. For example,

- Correct subject prefix:

CA certificate name constraint: Permitted: O=Cisco

Client certificate subject: O=Cisco,CN=Salomon

- Incorrect subject prefix:

CA certificate name constraint: Permitted: O=Cisco

Client certificate subject: CN=Salomon,O=Cisco

- DNS
- E-mail
- URI (The URI constraint must start with a URI prefix such as http://, https://, ftp://, or ldap://).

The following name constraints are not supported:

- IP address
- Othername

When a CA certificate contains a constraint that is not supported and certificate that is being verified does not contain appropriate field, it is rejected because Cisco ISE cannot verify unsupported constraints.

The following is an example of the name constraints definition within the CA certificate:

```
X509v3 Name Constraints: critical
    Permitted:
        othername:<unsupported>
        email:.stihl.at
        email:.stihl.be
        email:.stihl.bg
        email:.stihl.by
        DNS:.dir
        DirName: DC = dir, DC = emea
        DirName: C = AT, ST = EMEA, L = AT, O = STIHL Group, OU = Domestic
        DirName: C = BG, ST = EMEA, L = BG, O = STIHL Group, OU = Domestic
        DirName: C = BE, ST = EMEA, L = BN, O = STIHL Group, OU = Domestic
        DirName: C = CH, ST = EMEA, L = CH, O = STIHL Group, OU = Service Z100
        URI:.dir
        IP:172.23.0.171/255.255.255.255
    Excluded:
        DNS:.dir
        URI:.dir
```

An acceptable client certificate subject that matches the above definition is as follows:

```
Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1,
CN=flovison
```

Viewing Certificate Store Certificates

The Certificate Store page lists all the CA certificates that have been added to Cisco ISE. To view the CA certificates, you must be a Super Admin or System Admin.

To view all the certificates, choose **Administration > System > Certificates > Certificate Store**. The Certificate Store page appears, listing all the CA certificates.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Certificate Store Page, page A-11](#)

Changing the Status of a Certificate in Certificate Store

The status of a certificate must be enabled so that Cisco ISE can use the certificate for establishing trust. When a certificate is imported into the Certificate Store, it is automatically enabled.

-
Step 1	Choose Administration > System > Certificates > Certificate Store .
Step 2	Check the check box next to the certificate you want to enable or disable, and click Change Status .
-

Adding a Certificate to Certificate Store

The Certificate Store page allows you to add CA certificates to Cisco ISE.

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.
- Ensure that the certificate store certificate resides on the file system of the computer where your browser is running. The certificate must be in PEM or DER format.

-
Step 1	Choose Administration > System > Certificates > Certificate Store .
Step 2	Click Import .
Step 3	Configure the field values as necessary.

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.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Certificate Store Import Settings, page A-11](#)

Editing a Certificate Store Certificate

After you add a certificate to the Certificate Store, you can further edit it by using the edit settings.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > System > Certificates > Certificate Store .
Step 2	Check the check box next to the certificate that you want to edit, and click Edit .
Step 3	Modify the editable fields as required.
Step 4	Click Save to save the changes you have made to the certificate store.
-

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Certificate Store Edit Settings, page A-12](#)

Exporting a Certificate from the Certificate Store

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > System > Certificates > Certificate Store .
Step 2	Check the check box next to the certificate that you want to export, and click Export . You can export only one certificate at a time.
Step 3	Save the privacy-enhanced mail file to the file system that is running your client browser.
-

Related Topics

[Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Importing Certificate Chains

You can import multiple certificates from a single file that contains a certificate chain received from a Certificate store. All certificates in the file must be in Privacy-Enhanced Mail (PEM) format, and the certificates must be arranged in the following order:

- The last certificate in the file must be the client or server certificate being issued by the CA.
- All preceding certificates must be the root CA certificate plus any intermediate CA certificates in the signing chain for the issued certificate.

Importing a certificate chain is a two-step process:

-
- Step 1** Import the certificate chain file into the Certificate Store using the [Adding a Certificate to Certificate Store](#) operation. This operation will import all certificates from the file except the last one into the Certificate Store. You can perform this step only on the primary Administration node.
- Step 2** Import the certificate chain file using the [Binding a CA-Signed Certificate](#) operation. This operation will import the last certificate from the file as a local certificate.
-

Installation of CA Certificates for Cisco ISE Inter-node Communication

In a distributed deployment, before registering a secondary node, you must populate the primary node's CTL with the appropriate CA certificates that are 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 must import the CA-signed certificate of the secondary node into the CTL of the primary node.
- 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.



Note

If you change the HTTPS certificate on the registered secondary node, after registering your secondary node to the primary node, you must obtain appropriate CA certificates that can be used to validate the secondary node's HTTPS certificate.

Related Topics

- [Importing a CA-Signed Certificate from a Secondary Node into the Primary Node's CTL, page 8-29](#)
- [Importing a Self-Signed Certificate from a Secondary Node into the CTL of the Primary Node, page 8-30](#)

Importing a CA-Signed Certificate from a Secondary Node into the Primary Node's CTL

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Log in to the Admin portal 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.
- Step 2** In the Export dialog box, click the **Export Certificate Only** radio button.
- Step 3** Log in to the Admin portal of your primary node, and import the CA-signed certificate of the secondary node into the CTL of the primary node.
-

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Exporting a Certificate from the Certificate Store, page 8-28](#)
- [Adding a Certificate to Certificate Store, page 8-27](#)

Importing a Self-Signed Certificate from a Secondary Node into the CTL of the Primary Node

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Log in to the Admin portal 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.
Step 2	In the Export dialog box, click the Export Certificate Only radio button.
Step 3	Log in to the Admin portal of your primary node, and import the self-signed certificate of the secondary node into the CTL of the primary node.
-

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Exporting a Local Certificate, page 8-22](#)
- [Adding a Certificate to Certificate Store, page 8-27](#)

Simple Certificate Enrollment Protocol Profiles

To help enable certificate provisioning functions for the variety of mobile devices that users can register on the network, Cisco ISE enables you to configure one or more Simple Certificate Enrollment Protocol (SCEP) Certificate Authority (CA) profiles to point Cisco ISE to multiple CA locations. The benefit of allowing for multiple profiles is to help ensure high availability and perform load balancing across the CA locations that you specify. If a request to a particular SCEP CA goes unanswered three consecutive times, Cisco ISE declares that particular server unavailable and automatically moves to the CA with the next lowest known load and response times, then it begins periodic polling until the server comes back online.

For details on how to set up your Microsoft SCEP server to interoperate with Cisco ISE, see

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf.

Related Topics

- [Adding Simple Certificate Enrollment Protocol Profiles, page 8-30](#)
- [OCSP Services, page 8-31](#)

Adding Simple Certificate Enrollment Protocol Profiles

-
Step 1	Choose Administration > System > Certificates > SCEP CA Profile .
Step 2	Specify a Name for the profile to distinguish it from other SCEP CS profile names.
Step 3	Enter an optional Description of the profile.
Step 4	Specify the URL of the SCEP CA server in question, where Cisco ISE can direct SCEP CA requests when users access the network from their mobile devices.

You can optionally use the adjacent **Test Connectivity** button to verify that Cisco ISE is able to reach the server at the URL that you specify, before clicking the Submit button to end the session. (Either way, Cisco ISE will test the URL before allowing you to save the profile.)

Step 5 Click **Submit**.

For Reference:

Once users' devices receive their validated certificate, they reside on the device as described in [Table 8-1](#).

Table 8-1 *Device Certificate Location*

Device	Certificate Storage Location	Access Method
iPhone/iPad	Standard certificate store	Settings > General > Profile
Android	Encrypted certificate store	Invisible to end users. Note Certificates can be removed using Settings > Location & Security > Clear Storage.
Windows	Standard certificate store	Launch mmc.exe from the <code>/cmd</code> prompt or view in the certificate snap-in.
Mac	Standard certificate store	Application > Utilities > Keychain Access

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 Certificate Revocation List (CRL) 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 Store Certificate, page 8-28](#).

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 an unknown status is returned for a given certificate, Cisco ISE switches to checking the CRL.

This section contains the following topics:

- [OCSP Certificate Status Values, page 8-32](#)
- [OCSP High Availability, page 8-32](#)
- [Adding OCSP Services, page 8-33](#)
- [OCSP Statistics Counters, page 8-34](#)
- [OCSP Failures, page 8-32](#)
- [Monitoring OCSP, page 8-35](#)

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 8-34](#)

OCSP High Availability

Cisco ISE has the capability to configure up to two OCSP servers per CA, and they are 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 replay attacks.
- **Validate response**—Cisco ISE validates the response signature that is received from the OCSP server.

In case of timeout (which is 5 seconds), when Cisco ISE communicates with the primary OCSP server, it switches to the secondary OCSP server.

Cisco 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 (Cisco 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 Cisco ISE OCSP request.
 - b. Errors or responses not received from Cisco ISE OCSP requests.

An OCSP responder may not provide a response to the Cisco 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, in 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

Adding OCSP Services

You can use the add OCSP page to add new OCSP services to Cisco ISE.

-
- Step 1** Choose **Administration > System > Certificates > OCSP Services**.
- Step 2** Click **Add**
- Step 3** Provide a name and description for the OCSP service.
- Step 4** Check the **Enable Secondary Server** check box if you want to enable high availability.
- Step 5** 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, Cisco 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 Cisco 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 to 999 minutes.
- Step 6** Provide the URLs or IP addresses of the primary and secondary OCSP servers.
- Step 7** Check or uncheck the following options:
- **Nonce**—You can configure a nonce to be sent as part of the OCSP request. The Nonce 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 certificate different from the CA certificate
- In order for Cisco 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 Cisco ISE to validate it. If OCSP signs the response with a different certificate that is not configured in Cisco ISE, the response verification will fail.
- Step 8** 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 the 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 or persistent, so when Cisco ISE restarts, the cache is cleared.

The OCSP cache is used in order to maintain the OCSP responses and 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 9 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.

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 data from 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 8-2 lists the OCSP syslog messages and their descriptions.

Table 8-2 OCSP Syslog Messages

Message	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
ClearCacheInvokedCount	How many times clear cache was triggered since the interval

Table 8-2 OCSP Syslog Messages

Message	Description
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. For more information on Cisco ISE reports, see [Chapter 26, “Reporting.”](#)



Managing Network Devices

This chapter describes how to manage network devices in your network. This chapter contains the following sections:

- [Network Devices Definitions in Cisco ISE, page 9-1](#)
- [Default Network Device Definition in Cisco ISE, page 9-2](#)
- [Creating a Network Device Definition in Cisco ISE, page 9-3](#)
- [Importing Network Devices into Cisco ISE, page 9-4](#)
- [Exporting Network Devices from Cisco ISE, page 9-4](#)
- [Network Device Groups, page 9-5](#)
- [Importing Network Device Groups in to Cisco ISE, page 9-6](#)
- [Exporting Network Device Groups from Cisco ISE, page 9-6](#)
- [Import Templates in Cisco ISE, page 9-7](#)
- [Mobile Device Manager Interoperability with Cisco ISE, page 9-11](#)
- [Setting Up MDM Servers With Cisco ISE, page 9-15](#)

Network Devices Definitions in Cisco ISE

A network device such as a switch or a router is an authentication, authorization, and accounting (AAA) client through which AAA service requests are sent to Cisco ISE. You must define network devices for Cisco ISE to interact with the network devices. You can configure network devices for RADIUS authentication, Simple Network Management Protocol for the Profiling service to collect Cisco Discovery Protocol and Link Layer Discovery Protocol attributes for profiling endpoints, and Security Group Access (SGA) attributes for SGA devices. A network device that is not defined in Cisco ISE cannot receive AAA services from Cisco ISE.

In the network device definition:

- You can configure the RADIUS protocol for RADIUS authentications. When Cisco 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 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 network device. A failed authentication report is generated, which provides the failure reason.

- You can configure the Simple Network Management Protocol (SNMP) in the network device definition for the Profiling service to communicate with the network devices and profile endpoints that are connected to the network devices.
- You must define Security Group Access (SGA)-enabled devices in Cisco ISE to process requests from SGA-enabled devices that can be part of the Cisco SGA solution. Any switch that supports the Security Group Access solution is an SGA-enabled device.

SGA devices do not use the IP address. Instead, you must define other settings so that SGA devices can communicate with Cisco ISE.

SGA-enabled devices use the Security Group Access attributes to communicate with Cisco ISE. SGA-enabled devices, such as the Nexus 7000 series switches, Catalyst 6000 series switches, Catalyst 4000 series switches, and Catalyst 3000 series switches are authenticated using the SGA attributes that you define while adding SGA devices.

Related topics

- [RADIUS Authentication Settings, page A-37](#)
- [SNMP Settings, page A-38](#)
- [SGA Device Attribute Settings, page A-39](#)

Default Network Device Definition in Cisco ISE

Cisco ISE supports the default device definition for RADIUS authentications. You can define a default network device that Cisco ISE can use if it does not find a device definition for a particular IP address. This feature enables you to define a default RADIUS shared secret and the level of access for newly provisioned devices.

Cisco ISE looks for the corresponding device definition to retrieve the shared secret that is configured in the network device definition when it receives a RADIUS request from a network device.

Cisco ISE performs the following procedure when a RADIUS request is received:

1. Looks for a specific IP address that matches the one in the request.
2. Looks up the ranges to see if the IP address in the request falls within the range that is specified.
3. If both step 1 and 2 fail, it uses the default device definition (if defined) to process the request.

Cisco ISE obtains the shared secret that is configured in the device definition for that device and matches it against the shared secret in the RADIUS request to authenticate access. If no device definitions are found, Cisco ISE obtains the shared secret from the default network device definition and processes the RADIUS request.

Related Topics

- [RADIUS Authentication Settings, page A-37](#)

When an endpoint performs MAB using Password Authentication Protocol (PAP) and the default network device is configured in Cisco ISE, there is a security risk that any network access Device (NAD) can be used to connect the endpoint to the network. We recommend MAB using EAP-MD5 for such cases to increase protection. EAP-MD5 obligates the usage of Message-Authentication RADIUS attribute that will cause incoming RADIUS MAB request dropping in case of wrong shared secret configured in Cisco ISE.

Creating a Network Device Definition in Cisco ISE

You can create a network device definition in Cisco ISE and use the default network device definition when there is no network device definition in Cisco ISE.

A network device definition must include the following:

- Device name
- IP address and subnet mask
- Model name (Optional)
- Version name (Optional)
- Network device group by location and device type
- Authentication settings
- SNMP settings
- Security Group Access attributes settings

-
- Step 1** Choose **Administration > Network Resources > Network Devices**.
- Step 2** Click **Add**.
- Step 3** Enter the name and description of the network device that you want to add.
- Step 4** Enter a single IP address and a subnet mask.
- Step 5** Click the arrow next to the Model Name drop-down list to choose the network device model.
- Step 6** Click the arrow next to the Software Version drop-down list to choose the Cisco Internetwork Operating System (Cisco IOS) version.
- Step 7** Choose the Network Device Group from the Location drop-down list and the Device Type drop-down list.
- Step 8** Check the **Authentication Settings** check box to configure the RADIUS protocol for authentication.
- Step 9** Check the **SNMP Settings** check box to configure the Simple Network Management Protocol for the Profiling service to collect device information.
- Step 10** Check the **Advanced Trustsec Settings** check box to configure an SGA-enabled device.
- Step 11** Click **Submit**.
-

Related Topics

- [Network Device Definition Settings, page A-36](#)
- [Network Devices Definitions in Cisco ISE, page 9-1](#)
- [RADIUS Authentication Settings, page A-37](#)
- [Default Network Device Definition Settings, page A-41](#)

Importing Network Devices into Cisco ISE

You can import a list of device definitions into a Cisco ISE node using a comma-separated value (CSV) file. You must first update the imported template before you can import network devices into Cisco ISE. You cannot run an import of the same resource type at the same time. For example, you cannot concurrently import network devices from two different import files.

You can download the CSV template from the Admin portal, enter your device definition details in the template, and save it as a CSV file, which you can then import this back in to Cisco ISE.

While importing devices, you can create new records or update existing records. Cisco ISE displays the summary of the number of devices that are imported and also reports any errors that were found during the import process. When you import devices, you can also define whether you want Cisco ISE to overwrite the existing device definitions with the new definitions or stop the import process when Cisco ISE encounters the first error.

You cannot import network devices in Cisco ISE, Release 1.2 that are exported in previous Cisco ISE, Releases 1.1 and 1.1.x as the import template for these releases are different.

-
- Step 1** Choose **Administration > Network Resources > Network Devices**.
 - Step 2** Click **Import**.
 - Step 3** Click **Browse** to choose the CSV file from the system that is running the client browser.
 - Step 4** Check the **Overwrite Existing Data with New Data** check box.
 - Step 5** Check the **Stop Import on First Error** check box.
 - Step 6** Click **Import**.
-

Related Topics

- [Exporting Network Devices from Cisco ISE, page 9-4](#)
- [Network Device Import Settings, page A-41](#)
- [Network Devices Import Template Format, page 9-7](#)

Exporting Network Devices from Cisco ISE

You can export network devices configured in Cisco ISE in the form of a CSV file that you can use to import these network devices into another Cisco ISE node.

-
- Step 1** Choose **Administration > Network Resources > Network Devices**.
 - Step 2** Click **Export**.
 - Step 3** To export network devices, you can do one of the following:
 - Check the check boxes next to the devices that you want to export, and choose **Export > Export Selected**.
 - Choose **Export > Export All** to export all the network devices that are defined.
 - Step 4** Save the export.csv file to your local hard disk.
-

Related Topics

[Importing Network Devices into Cisco ISE, page 9-4](#)

Network Device Groups

Cisco ISE allows you to create hierarchical Network Device Groups (NDGs) that contain network devices. NDGs logically group network devices based on various criteria such as geographic location, device type, and the relative place in the network (like “Access Layer” or “Data Center,” for example).

For example, to organize your network devices by geographic location, you can group them by continent, region, and country:

- Africa -> Southern -> Namibia
- Africa -> Southern -> South Africa
- Africa -> Southern -> Botswana

You can also group network devices by device type:

- Africa -> Southern -> Botswana -> Firewalls
- Africa -> Southern -> Botswana -> Routers
- Africa -> Southern -> Botswana -> Switches

Network devices can be assigned to one or more hierarchical NDGs. Thus, when Cisco ISE passes through the ordered list of configured NDGs to determine the appropriate group to assign to a particular device, it may find that the same device profile applies to multiple Device Groups, and will apply the first Device Group matched.

Root Network Device Groups

Cisco ISE includes two predefined root NDGs: All Device Types and All Locations. You cannot edit, duplicate, or delete these predefined NDGs, but you can add new device groups under them.

You can also create a root Network Device Group (NDG), and then create child NDGs under the root group in the Network Device Groups page. When you create a new root NDG, you must provide the name and type of the NDG. This information is not required when you create a child under the root NDG.

Related Topics

[Network Device Group Settings, page A-42](#)

Network Device Attributes Used By Cisco ISE in Policy Evaluation

When you create a new network device group, a new network device attribute is added to the Device dictionary defined in the system, which you can use in policy definitions. Cisco ISE allows you to configure authentication and authorization policies based on Device dictionary attributes, such as device type, location, model name, and software version that is running on the network device.

Related Topics

[System Defined Dictionaries and Dictionary Attributes, page 10-1](#)

Importing Network Device Groups in to Cisco ISE

You can import network device groups in to a Cisco ISE node using a comma-separated value (CSV) file. You cannot run import of the same resource type at the same time. For example, you cannot concurrently import network device groups from two different import files.

You can download the CSV template from the Admin portal, enter your device group details in the template, and save the template as a CSV file, which you can then import back into Cisco ISE.

While importing device groups, you can create new records or update existing records. When you import device groups, you can also define whether you want Cisco ISE to overwrite the existing device groups with the new groups or stop the import process when Cisco ISE encounters the first error.

-
- Step 1** Choose **Administration > Network Resources > Network Device Groups > Groups**.
 - Step 2** Click **Import**.
 - Step 3** Click **Browse** to choose the CSV file from the system that is running the client browser.
 - Step 4** Check the **Overwrite Existing Data with New Data** check box.
 - Step 5** Check the **Stop Import on First Error** check box.
 - Step 6** Click **Import** or click the **Network Device Groups List** link to return to the Network Device Groups list page.
-

Related Topics

- [Exporting Network Device Groups from Cisco ISE, page 9-6](#)
- [Network Device Group Import Settings, page A-43](#)
- [Network Device Groups Import Template Format, page 9-10](#)

Exporting Network Device Groups from Cisco ISE

You can export network device groups configured in Cisco ISE in the form of a CSV file that you can use to import these network device groups into another Cisco ISE node.

-
- Step 1** Choose **Administration > Network Resources > Network Device Groups > Groups**.
 - Step 2** To export the network device groups, you can do one of the following:
 - Check the check boxes next to the device groups that you want to export, and choose **Export > Export Selected**.
 - Choose **Export > Export All** to export all the network device groups that are defined.
 - Step 3** Save the export.csv file to your local hard disk.
-

Related Topics

- [Importing Network Device Groups in to Cisco ISE, page 9-6](#)

Import Templates in Cisco ISE

Cisco ISE allows you to import a large number of network devices and network device groups using comma-separated value (CSV) files. The template contains a header row that defines the format of the fields. The header row should not be edited, and should be used as is.

By default, you can use the Generate a Template link to download a CSV file in the Microsoft Office Excel application and save the file format 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 and save the template.csv file locally on your system with an appropriate name for network devices and network device groups. If you choose to open the template.csv file from the dialog, the file opens in the Microsoft Office Excel application by default.

Related Topics

- [Importing Network Devices into Cisco ISE, page 9-4](#)
- [Exporting Network Devices from Cisco ISE, page 9-4](#)
- [Importing Network Device Groups in to Cisco ISE, page 9-6](#)
- [Exporting Network Device Groups from Cisco ISE, page 9-6](#)
- [Network Devices Import Template Format, page 9-7](#)
- [Network Device Groups Import Template Format, page 9-10](#)

Network Devices Import Template Format

Table 9-1 lists the fields in the template header and provides a description of the fields in the Network Device CSV file.

Table 9-1 CSV Template Fields and Description for Network Devices

Field	Description
Name:String(32):	(Required) This field is the network device name. It is an alphanumeric string, with a maximum of 32 characters in length.
Description:String(256)	This field is an optional description for the network device. A string, with a maximum of 256 characters in length.
IP Address:Subnets(a.b.c.d/ml...)	(Required) This field is the IP address and subnet mask of the network device. (It can take on more than one value separated by a pipe “ ” symbol).
Model Name:String(32):	(Required) This field is the network device model name. It is a string, with a maximum of 32 characters in length.
Software Version:String(32):	(Required) This field is the network device software version. It is a string, with a maximum of 32 characters in length.

Table 9-1 CSV Template Fields and Description for Network Devices (continued)

Field	Description
Network Device Groups:String(100):	(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 enter a value for the Authentication Protocol field) This field is a string, with a maximum of 128 characters in length.
EnableKeyWrap:Boolean(truelfalse)	This is an optional field. It is enabled only when it is supported on the network device. Valid value is true or false.
EncryptionKey:String(ascii:16 hexa:32)	(Required, if you enable KeyWrap) Indicates the encryption key that is used for session encryption. ASCII—16 characters (bytes) long Hexadecimal—32 characters (bytes) long.
AuthenticationKey:String(ascii:20 hexa:40)	(Required, if you enable KeyWrap). Indicates the keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages. ASCII—20 characters (bytes) long Hexadecimal—40 characters (bytes) long.
InputFormat:String(32)	Indicates encryption and authentication keys input format. Valid value is ASCII or Hexadecimal.
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 value is 1, 2c, or 3.
SNMP:RO Community:String(32)	(Required, if you enter a value for the SNMP Version field) SNMP Read Only community. It is a string, with a maximum of 32 characters in length.
SNMP:RW Community:String(32)	(Required, if you enter a value for the SNMP Version field) SNMP Read Write community. It is a string, with a maximum of 32 characters in length.
SNMP:Username:String(32)	This is an optional field. It is a string, with a maximum of 32 characters in length.
SNMP:Security Level:Enumeration(Auth No Auth Priv)	(Required if you choose SNMP version 3) Valid value is Auth, No Auth, or Priv.
SNMP:Authentication Protocol:Enumeration(MD5 SHA)	(Required if you have entered Auth or Priv for the SNMP security level) Valid value is 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 in length.

Table 9-1 CSV Template Fields and Description for Network Devices (continued)

Field	Description
SNMP:Privacy Protocol:Enumeration(DES AES128 AES192 AES256 3DES)	(Required if you have entered Priv for the SNMP security level) Valid value is 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 in length.
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(truelfalse)	This is an optional field to enable or disable the SNMP link trap. Valid value is true or false.
SNMP:Is MAC Trap Query:Boolean(truelfalse)	This is an optional field to enable or disable the SNMP MAC trap. Valid value is true or false.
SNMP:Originating Policy Services Node:String(32)	This is an optional field. Indicates which ISE server to be used to poll for SNMP data. By default, it is automatic, but you can overwrite the setting by assigning different values.
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 in length.
SGA:Device Password:String(256)	(Required if you have entered SGA device ID) This is the security group access device password and is a string, with a maximum of 256 characters in length.
SGA:Environment Data Download Interval:Integer:1-2147040000 seconds	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:1-2147040000 seconds	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:1-2147040000 seconds	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:1-2147040000 seconds	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(truelfalse)	This is an optional field. Indicates whether security group access is trusted. Valid value is true or false.
SGA:Notify this device about SGA configuration changes:String(ENABLE_ALL DISABLE_ALL)	This is an optional field. Notifies SGA configuration changes to the SGA device. Valid value is ENABLE_ALL or DISABLE_ALL
SGA:Include this device when deploying Security Group Tag Mapping Updates:Boolean(truelfalse)	This is an optional field. It is the security group access device included on SGT. Valid value is true or false.

Table 9-1 CSV Template Fields and Description for Network Devices (continued)

Field	Description
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 in length.
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 in length.
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 in length.
SGA:PAC issue date:Date	This is the field that displays the issuing date of the last SGA PAC that has been generated by Cisco ISE for the SGA device.
SGA:PAC expiration date:Date	This is the field that displays the expiration date of the last SGA PAC that has been generated by Cisco ISE for the SGA device.
SGA:PAC issued by:String	This is a field that displays the name of the issuer (an SGA administrator) of the last SGA PAC that has been generated by Cisco ISE for the SGA device. It is a string.

Network Device Groups Import Template Format

Table 9-2 lists the fields in the template header and provides a description of the fields in the Network Device Group CSV file.

Table 9-2 CSV Template Fields and Description for Network Device Groups

Field	Description
Name:String(100):	(Required) This field is the network device group name. It is a string with a maximum of 100 characters in length. The full name of an NDG can have a maximum of 100 characters in length. 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 cannot exceed 100 characters in length. If the full name of the NDG exceeds 100 characters in length, 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 in length.
Type:String(64):	(Required) This field is the network device group type. It is a string, with a maximum of 64 characters in length.
Is Root:Boolean(true/false):	(Required) This is a field that determines if the specific network device group is a root group. Valid value is true or false.

Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM servers consist of a policy server that controls the use of some applications on a mobile device (for example, an e-mail application) in the deployed environment. However, the network is the only entity that can provide granular access to endpoints based on ACLs, SGTs, etc. To do its job, Cisco ISE queries the MDM servers for the necessary device attributes to ensure it is then able to provide network access control for those devices.

Figure 9-1 MDM Interoperability with Cisco ISE

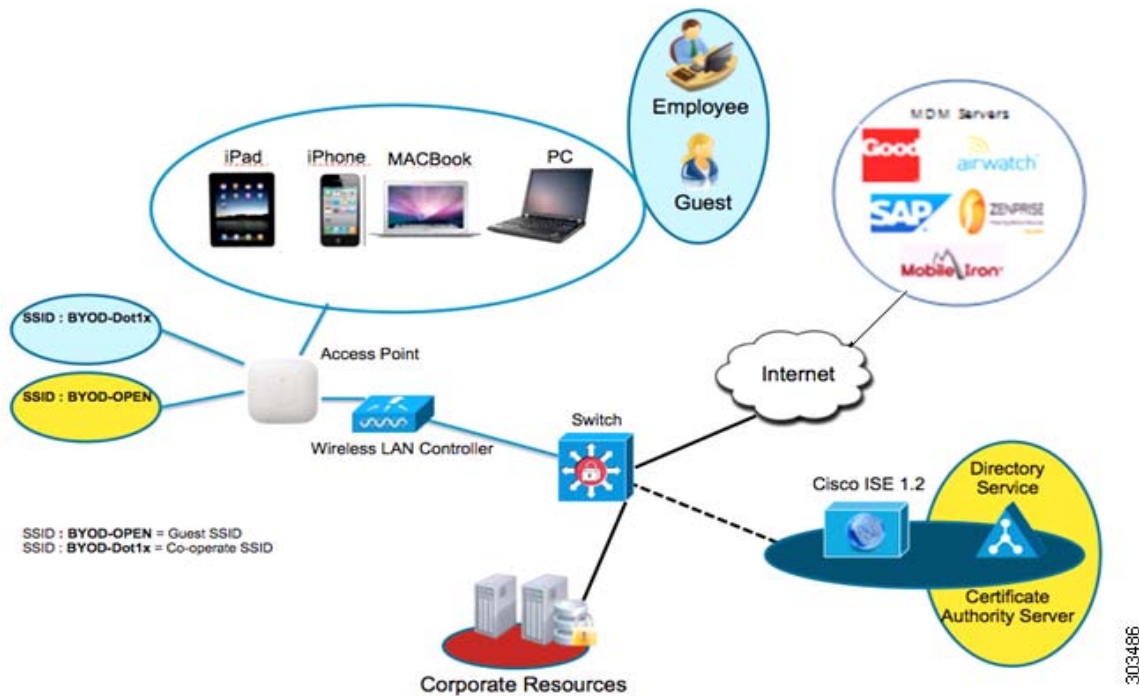


Table 9-3 lists the components that are used in the MDM setup.

Table 9-3 Components Used in the MDM Setup

Component	Specification
Cisco Identity Services Engine, Release 1.2	Any of the following: ISE 3315, 3355, 3395, 3415, 3495, or VMware
MDM Server	—
(Optional) Certificate Authority Server	As per Microsoft specification (Windows 2008 R2 Enterprise SP2)

Table 9-3 **Components Used in the MDM Setup**

Component	Specification
Wireless LAN Controller (WLC)	- Hardware: 5500 Series, 2500 Series, WLSM-2 - Software: Unified Wireless Network Software, Release 7.2
Mobile Devices	Devices supported by the MDM vendor. See Supported MDM Servers, page 9-13 for a list of supported MDM vendors. For example, Apple iOS 5.0 and higher, Google Android 2.3.

In [Figure 9-1](#), Cisco ISE is the enforcement point while the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

You can configure Cisco ISE to interoperate with an external Mobile Device Manager (MDM) server. By setting up this type of third-party connection, you can leverage the detailed information available in the MDM database. Cisco ISE uses REST API calls to pull the various pieces of information from the external MDM server. Cisco ISE applies appropriate access control policies to switches, access routers, wireless access points, and other network access points to achieve greater control of remote device access to your Cisco ISE network.

The following sections describe only the MDM configuration. For detailed ISE and WLC configuration, refer to the design documents that are available at:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Supported MDM Use Cases

The functions Cisco ISE performs in conjunction with the external MDM server are as follows:

- Facilitating device registration—Unregistered endpoints accessing the network are redirected to a registration page hosted on the MDM server for registration based on user role, device type, and so on.
- Handling device remediation—Endpoints are granted only restricted access after becoming noncompliant.
- Augmenting endpoint data—Update the endpoint database with information from the MDM server that you cannot gather using the Cisco ISE Profiler. Cisco ISE uses six device attributes you can view using the **Administration > Identity Management > Identities > Endpoints** page if an endpoint is a MDM monitored device. For example:
 - MDMImei: 99 000100 160803 3
 - MDMManufacturer: Apple
 - MDMModel: iPhone
 - MDMOSVersion: iOS 6.0.0
 - MDMPhoneNumber: 9783148806
 - MDMSerialNumber: DNPGQZGUDTF9

- Periodically checking compliance—Cisco ISE polls the MDM server once every four hours for device compliance data.
- Issuing device instructions through the MDM server—Issues remote actions for users' devices through the MDM server.

Cisco ISE allows you to configure MDM policy based on the following attributes:

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber

Supported MDM Servers

Supported MDM servers include products from the following vendors:

- Airwatch, Inc.
- Good Technology
- MobileIron, Inc.
- Zenprise, Inc.
- SAP Afaria
- Fiberlink MaaS

Ports Used by the MDM Server

Table 9-4 lists the ports that must be open between the Cisco ISE and the MDM server to enable them to communicate with each other. Refer to the *MDM Server Documentation* for a list of ports that must be open on the MDM agent and server.

Table 9-4 Ports Used by the MDM Server

MDM Server	Ports
Mobile Iron	443
Zenprise	443
Good	19005
Airwatch	443
Afaria	443
Fiberlink MaaS	443

MDM Dictionary Attributes

After you add the MDM server definition in Cisco ISE, the MDM dictionary attributes are available in Cisco ISE that you can use in authorization policies. You can view the dictionary attributes that are available for use in authorization policies (Policy > Policy Elements > Dictionaries > MDM > Dictionary Attributes).

When you are using these MDM dictionary attributes in policies, you cannot delete the MDM server configuration from Cisco ISE. To remove the MDM server configuration, you must first remove the MDM dictionary attributes from policies, and then remove the MDM server from Cisco ISE.

MDM Integration Process Flow

This section describes the MDM integration process:

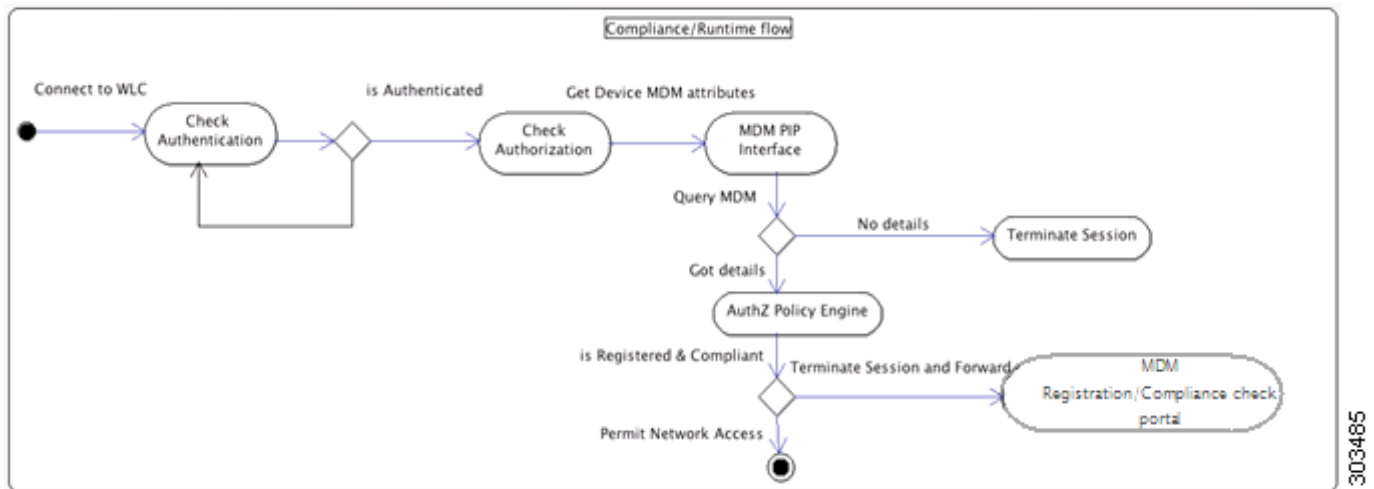
1. The user associates a device to SSID.
2. (Optional) If the device is not registered, the user goes through the device on-boarding flow.
3. Cisco ISE makes an API call to the MDM server.
4. This API call returns a list of devices for this user and the posture status for the devices.



Note The input parameter is the MAC address of the endpoint device.

5. If the user's device is not in this list, it means the device is not registered. Cisco ISE sends an authorization request to the NAD to redirect to Cisco ISE. The user is presented the MDM server page.
6. Cisco ISE uses MDM to provision the device and presents an appropriate page for the user to register the device.
7. The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE (through automatic redirection or manual browser refresh).
8. Cisco ISE queries the MDM server again for the posture status.
9. If the user's device is not compliant to the posture (compliance) policies configured on the MDM server, the user is notified that the device is out of compliance and must be compliant.
10. After the user's device becomes compliant, the MDM server updates the device state in its internal tables.
11. If the user refreshes the browser now, the control is transferred back to Cisco ISE.
12. Cisco ISE polls the MDM server once every four hours to get compliance information and issues Change of Authorization (CoA) appropriately.

The following figure illustrates the MDM process flow.



303485

Setting Up MDM Servers With Cisco ISE

To set up MDM servers with Cisco ISE, you must perform the following tasks:

1. [Importing MDM Server Certificate into Cisco ISE, page 9-15](#)
2. [Creating Mobile Device Manager Definitions, page 9-16](#)
3. Configure ACLs on the Wireless LAN Controllers. See [“Configure ACLs on the Wireless LAN Controller for MDM Interoperability” section on page F-10](#) for more information.
4. [Configuring an Authorization Profile for Redirecting Nonregistered Devices, page 9-16](#)
5. [Configuring Authorization Policy Rules for the MDM Use Cases, page 9-17](#)

Importing MDM Server Certificate into Cisco ISE

For Cisco ISE to connect with the MDM server, you must import the MDM server certificate into the Cisco ISE Certificate Store. If your MDM server has a CA-signed certificate, you must import the root CA into the Cisco ISE Certificate Store.

-
- Step 1** Export the MDM server certificate from your MDM server and save it on your local machine.
- Step 2** Choose **Administration > Certificates > Certificate Store > Import**.
- Step 3** Click **Browse** to select the MDM server certificate that you obtained from the MDM server.
- Step 4** Add a friendly name.
- Step 5** Click **Submit**.
- Step 6** Verify that the Certificate Store list page lists the MDM server certificate.
-

Creating Mobile Device Manager Definitions

You can create one or more Mobile Device Manager (MDM) definitions for external MDM servers to help ensure Cisco ISE is able to obtain the most up-to-date device connection status from logged-in user devices as possible on demand. (Although you can configure multiple MDM server definitions, you can activate only one MDM server with which Cisco ISE interoperates at a time.)

Before You Begin

Ensure that you have imported the MDM server certificate into Cisco ISE. For more information, see [Importing MDM Server Certificate into Cisco ISE, page 9-15](#).

-
- Step 1** Choose **Administration > Network Resources > MDM**.
 - Step 2** Click **Add**.
 - Step 3** Enter the name and description of the MDM server that you want to add.
 - Step 4** Check (or uncheck) the **Status** check box to indicate which MDM server should be Active. Cisco ISE can communicate with only one MDM server at a time.
 - Step 5** Enter the MDM server IP address or hostname (FQDN) in the **MDM server host** field.
 - Step 6** Specify the network/proxy port through which Cisco ISE must communicate with the MDM server.
 - Step 7** Specify a server instance if you are using a multitenant cloud-based MDM service.
 - Step 8** Specify the MDM server administrator username and password so that Cisco ISE can log in to and interoperate with the MDM server database.
 - Step 9** Enter the polling interval in minutes for Cisco ISE to poll the MDM server for compliance check information. This value should be the same as the polling interval on your MDM server. The default value is 240 minutes.

We recommend that you set the polling interval below 60 minutes only for testing a few active clients on your network. If you set this value below 60 minutes for a production environment with many active clients, the system's load increases significantly and might negatively impact its performance.
 - Step 10** Check the **Enable** check box to activate the MDM server connection with Cisco ISE.
 - Step 11** Click **Test Connection** to test Cisco ISE's connection to the MDM server.

If Cisco ISE displays a connection error, delete the definition that you created, ensure that your MDM server is reachable, and re-create the MDM server definition in Cisco ISE.
 - Step 12** Click **Submit** to save the MDM server definition. Only after you successfully connect Cisco ISE with the MDM server, the MDM dictionary gets populated in Cisco ISE.
-

Configuring an Authorization Profile for Redirecting Nonregistered Devices

You must configure an authorization profile in Cisco ISE to redirect nonregistered devices.

Before You Begin

Ensure that you have created the MDM server definition in Cisco ISE. Only after you successfully integrate ISE with the MDM server, the MDM dictionary gets populated and you can create authorization policy using the MDM dictionary attributes. See [Creating Mobile Device Manager Definitions, page 9-16](#).

Configure ACLs on the Wireless LAN Controller for redirecting unregistered devices. See [“Configure ACLs on the Wireless LAN Controller for MDM Interoperability”](#) section on page F-10.

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add**.
- Step 2** Create an authorization profile for redirecting nonregistered devices that are not compliant or registered.
- Step 3** Enter a name for the authorization profile.
- Step 4** Choose ACCESS_ACCEPT as the Access Type.
- Step 5** Check the **Web Redirection** check box and choose MDM Redirect from the drop-down list.
- Step 6** Enter the name of the ACL that you configured on the wireless LAN controller in the ACL field.
- Step 7** Click **Submit**.
-

Configuring Authorization Policy Rules for the MDM Use Cases

You must configure authorization policy rules in Cisco ISE to complete the MDM configuration in Cisco ISE.

Before You Begin

- Add the MDM server certificate into the Cisco ISE certificate store. See [Importing MDM Server Certificate into Cisco ISE, page 9-15](#).
- Ensure that you have created the MDM server definition in Cisco ISE. Only after you successfully integrate ISE with the MDM server, the MDM dictionary gets populated and you can create authorization policy using the MDM dictionary attributes. See [Creating Mobile Device Manager Definitions, page 9-16](#).
- Configure ACLs on the Wireless LAN Controller for redirecting unregistered or noncompliant devices. [“Configure ACLs on the Wireless LAN Controller for MDM Interoperability”](#) section on page F-10.

-
- Step 1** Choose **Policy > Authorization > Insert New Rule Below**.
- Step 2** Add the following rules:
- MDM_Un_Registered_Non_Compliant—For devices that are not yet registered with an MDM server or compliant with MDM policies. Once a request matches this rule, the ISE MDM page appears with information on registering the device with MDM.
 - PERMIT—If the device is registered with Cisco ISE, registered with MDM, and is compliant with Cisco ISE and MDM policies, it will be granted access to the network based on the access control policies configured in Cisco ISE.

Figure 9-2 shows an example of this configuration.

Figure 9-2 Authorization Policy Rules for the MDM Use Cases



Step 3 Click **Save**.

Wiping or Locking a Device

Cisco ISE allows you to wipe or turn on pin lock for a device that is lost. You can do this from the Endpoints page.

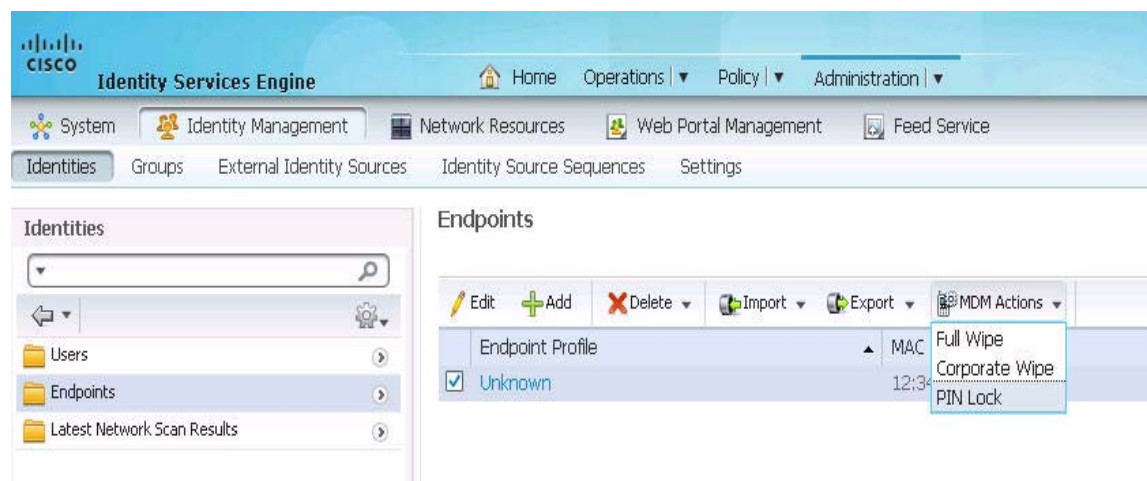
Step 1 Choose **Administration > Identity Management > Identities > Endpoints**.

Step 2 Check the check box next to the device that you want to wipe or lock.

Step 3 From the MDM Access drop-down list, choose any one of the following options as shown in :

- Full Wipe—Removes all information from the device
- Corporate Wipe—Removes applications that you have configured in the MDM server policies
- PIN Lock—Locks the device

Figure 9-3 Locking a Device



Step 4 Click **Yes** to wipe or lock the device.

Viewing Mobile Device Manager Reports

Cisco ISE records all additions, updates, and deletions of MDM server definitions. You can view these event in the “Change Configuration Audit” report, which provides all the configuration changes from any system administrator for a selected time period.

Choose **Operations > Reports > Change Configuration Audit > MDM**, and specify the period of time to display in the resulting report.

Related Topics

- [Mobile Device Manager Interoperability with Cisco ISE, page 9-11](#)
- [Supported MDM Use Cases, page 9-12](#)
- [Supported MDM Servers, page 9-13](#)
- [Creating Mobile Device Manager Definitions, page 9-16](#)
- [Viewing Mobile Device Manager Logs, page 9-19](#)

Viewing Mobile Device Manager Logs

You can use the Message Catalog page to view Mobile Device Manager log messages. Choose **Administration > System > Logging > Message Catalog**. The default reporting level for MDM log entries is “INFO.”

Related Topics

- [Mobile Device Manager Interoperability with Cisco ISE, page 9-11](#)
- [Supported MDM Use Cases, page 9-12](#)
- [Supported MDM Servers, page 9-13](#)
- [Creating Mobile Device Manager Definitions, page 9-16](#)
- [Viewing Mobile Device Manager Reports, page 9-18](#)



Managing Resources

This chapter provides information and procedures for managing Cisco ISE network resources and contains the following topics:

- [Dictionaries and Dictionary Attributes, page 10-1](#)
- [RADIUS-Vendor Dictionaries, page 10-3](#)

Dictionaries and Dictionary Attributes

Dictionaries are domain-specific catalogs of attributes and allowed values that can be used to define access policies for a domain. An individual dictionary is a homogeneous collection of attribute type. Attributes that are defined in a dictionary have the same attribute type and the type indicates the source or context of a given attribute.

Attribute types can be one of the following:

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

In addition to attributes and allowed values, a dictionary contains information about the attributes such as the name and description, data type, and the default values. An attribute can have one of the following data types: BOOLEAN, FLOAT, INTEGER, IPv4, OCTET_STRING, STRING, UNIT32, and UNIT64.

Cisco ISE creates system dictionaries during installation and allows you to create user dictionaries.

System Defined Dictionaries and Dictionary Attributes

Cisco ISE creates system dictionaries during installation that you can find in the System Dictionaries page. System-defined dictionary attributes are read-only attributes. Because of their nature, you can only view existing system-defined dictionaries. You cannot create, edit, or delete system-defined values or any attributes in a system dictionary.

A system-defined dictionary attribute is displayed with the descriptive name of the attribute, an internal name as understood by the domain, and allowed values.

Cisco ISE also creates dictionary defaults for the IETF RADIUS set of attributes that are also a part of the system-defined dictionaries, which are defined by the Internet Engineering Task Force (IETF). You can edit all free IETF RADIUS attribute fields except the ID.

Related Topics

- [Displaying System Dictionaries and Dictionary Attributes, page 10-2](#)
- [User-Defined Dictionaries and Dictionary Attributes, page 10-2](#)

Displaying System Dictionaries and Dictionary Attributes

You cannot create, edit, or delete any system-defined attribute in a system dictionary. You can only view system-defined attributes. You can perform a quick search that is based on a dictionary name and description or an advanced search that is based on a search rule that you define.

-
Step 1	Choose Policy > Policy Elements > Dictionaries > System .
Step 2	Choose a system dictionary in the System Dictionaries page, and click View .
Step 3	Click Dictionary Attributes .
Step 4	Choose a system dictionary attribute from the list, and click View .
Step 5	Click the Dictionaries link to return to the System Dictionaries page.
-

User-Defined Dictionaries and Dictionary Attributes

Cisco ISE displays the user-defined dictionaries that you create in the User Dictionaries page. You cannot modify the values for Dictionary Name or Dictionary Type for an existing user dictionary once created and saved in the system.

You can do the following in the User Dictionaries page:

- Edit and delete user dictionaries.
- Search user dictionaries based on name and description.
- Add, edit, and delete user-defined dictionary attributes in the user dictionaries.
- Add or remove allowed values for dictionary attributes.

Related Table

- [Creating User-Defined Dictionaries, page 10-2](#)
- [Creating User Defined Dictionary Attributes, page 10-3](#)

Creating User-Defined Dictionaries

You can create, edit, or delete user-defined dictionaries.

-
Step 1	Choose Policy > Policy Elements > Dictionaries > User .
Step 2	Click Add .
Step 3	Enter the name for the user dictionary, an optional description, and a version for the user dictionary.
Step 4	Choose the attribute type from the Dictionary Attribute Type drop-down list.

Step 5 Click **Submit**.

Related Topics

[Creating User Defined Dictionary Attributes, page 10-3](#)

Creating User Defined Dictionary Attributes

You can add, edit, and delete user-defined dictionary attributes in user dictionaries as well as add or remove allowed values for the dictionary attributes.

-
- Step 1** Choose **Policy > Policy Elements > Dictionaries > User**.
- Step 2** Choose a user dictionary from the User Dictionaries page, and click **Edit**.
- Step 3** Click **Dictionary Attributes**.
- Step 4** Click **Add**.
- Step 5** Enter the name for an attribute name, an optional description, and an internal name for the dictionary attribute.
- Step 6** Choose a data type from the Data Type drop-down list.
- Step 7** Click **Add** to configure the name, allowed value, and set the default status in the Allowed Values table.
- Step 8** Click **Submit**.
-

Related Topics

- [Results, page B-18](#)
- [RADIUS Vendor Dictionary Attribute Settings, page B-8](#)

RADIUS-Vendor Dictionaries

Cisco ISE allows you to define a set of RADIUS-vendor dictionaries, and define a set of attributes for each one. Each vendor definition in the list contains the vendor name, the vendor ID, and a brief description.

Cisco ISE provides you the following RADIUS-vendor dictionaries by default:

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

The RADIUS protocol supports these vendor dictionaries, and the vendor-specific attributes that can be used in authorization profiles and in policy conditions.

Related Topics

- [Creating RADIUS Vendor Dictionaries, page 10-4](#)
- [Creating RADIUS-Vendor Dictionary Attributes, page 10-4](#)

Creating RADIUS Vendor Dictionaries

You can also create, edit, delete, export, and import RADIUS-vendor dictionaries.

-
Step 1	Choose Policy > Policy Elements > Dictionaries > System > Radius > Radius Vendors .
Step 2	Click Add .
Step 3	Enter a name for the RADIUS-vendor dictionary, an optional description, and the vendor ID as approved by the Internet Assigned Numbers Authority (IANA) for the RADIUS vendor.
Step 4	Choose the number of bytes taken from the attribute value to specify the attribute type from the Vendor Attribute Type Field Length drop-down list. Valid values are 1, 2, and 4. The default value is 1.
Step 5	Choose the number of bytes taken from the attribute value to specify the attribute length from the Vendor Attribute Size Field Length drop-down list. Valid values are 0 and 1. The default value is 1.
Step 6	Click Submit .
-

Related Topics

[Creating RADIUS-Vendor Dictionary Attributes, page 10-4](#)

Creating RADIUS-Vendor Dictionary Attributes

You can create, edit, and delete RADIUS vendor attributes that Cisco ISE supports. Each RADIUS-vendor attribute has a name, data type, description, and direction, which specifies whether it is relevant to requests only, responses only, or both.

-
Step 1	Choose Policy > Policy Elements > Dictionaries > System > Radius > Radius Vendors .
Step 2	Choose a RADIUS-vendor dictionary from the RADIUS vendor dictionaries list, and click Edit .
Step 3	Click Dictionary Attributes , and then click Add .
Step 4	Enter the attribute name for the RADIUS vendor attribute and an optional description.
Step 5	Choose the data type from the Data Type drop-down list.
Step 6	Check the Enable MAC option check box.
Step 7	Choose the direction that applies to RADIUS requests only, RADIUS responses only, or both from the Direction drop-down list.
Step 8	Enter the vendor attribute ID in the ID field.
Step 9	Check the Allow Tagging check box.
Step 10	Check the Allow multiple instances of this attribute in a profile check box.
Step 11	Click Add to add the allowed value for the vendor attribute in the Allowed Values table.

Step 12 Click **Submit**.

Related Topics

[RADIUS Vendor Dictionary Attribute Settings, page B-8](#)



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 chapter contains the following topics:

- [Cisco ISE Logging Mechanism, page 11-1](#)
- [Cisco ISE System Logs, page 11-2](#)
- [Cisco ISE Message Codes, page 11-6](#)
- [Cisco ISE Message Catalogs, page 11-7](#)
- [Debug Log Configuration Options, page 11-7](#)
- [Collection Filters, page 11-8](#)

Cisco ISE Logging Mechanism

Cisco ISE provides a logging mechanism that is used for auditing, fault management, and troubleshooting. 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 a 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, which are called targets. Logs are classified into various predefined categories, which are discussed in [Cisco ISE Message Codes](#). You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

You can perform the following logging-related tasks in Cisco ISE:

- To configure local log settings, see [Configuring Local Log Purge Settings, page 11-2](#)
- To understand and create remote logging targets, see [Cisco ISE System Logs, page 11-2](#)
- To understand and edit logging categories, see [Cisco ISE Message Codes, page 11-6](#)
- To view message catalogs, see [Cisco ISE Message Catalogs, page 11-7](#)
- To understand and configure debug logs, see [Debug Log Configuration Options, page 11-7](#)

Configuring Local Log Purge Settings

Use this process to set local log-storage periods and to delete local logs after a certain period of time.

-
Step 1	Choose Administration > System > Logging > Local Log Settings .
Step 2	In the Local Log Storage Period field, enter the maximum number of days to keep the log entries in the configuration source.
Step 3	Click Delete Logs Now to delete the existing log files at any time before the expiration of the storage period.
Step 4	Click Save .
-

Cisco ISE System Logs

In Cisco ISE, system logs are collected at locations called logging targets. Targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can use the FTP facility to transfer 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.

By default, AAA Diagnostics subcategories and System Diagnostics subcategories logging targets are disabled during a fresh Cisco ISE installation or an upgrade to reduce the disk space. You can configure logging targets manually for these subcategories but local logging for these subcategories are always enabled.

You can use the default logging targets that are configured locally at the end of the Cisco ISE installation or you can create external targets to store the logs. You can create targets only for the subcategories. The parent categories are containers of the subcategories and hence you cannot create targets for them.

Related Topics:

[Configuring Remote Syslog Collection Locations, page 11-4](#)

Local Store Syslog Message Format

Log messages are sent to the local store with this syslog message format: *time stamp sequence_num msg_code msg_sev msg_class msg_text attr=value*.

Table 11-1 Local Store and Syslog Message Format

Field	Description
<i>timestamp</i>	Date of the message generation, according to the local clock of the originating the Cisco ISE node, in the format <i>YYYY-MM-DD hh:mm:ss:xxx +/-zh:zm</i>. Possible values are: • <i>YYYY</i> = Numeric representation of the year. • <i>MM</i> = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number. • <i>DD</i> = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number. • <i>hh</i> = The hour of the day—00 to 23. • <i>mm</i> = The minute of the hour—00 to 59. • <i>ss</i> = The second of the minute—00 to 59. • <i>xxx</i> = The millisecond of the second—000 to 999. • <i>+/-zz:zz</i> = The time zone offset from the Cisco ISE server's time zone, where <i>zh</i> is the number of offset hours and <i>zm</i> is the number of minutes of the offset hour, all of which is preceded by a minus or plus sign to indicate the direction of the offset. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server's time zone.
<i>sequence_num</i>	Global counter of each message. If one message is sent to the local store and the next to the syslog server target, the counter increments by 2. Possible values are 0000000001 to 999999999.
<i>msg_code</i>	Message code as defined in the logging categories.
<i>msg_sev</i>	Message severity level of a log message (see Logging Category Settings, page A-14).
<i>msg_class</i>	Message class, which identifies groups of messages with the same context.
<i>msg_text</i>	English language descriptive text message.
<i>attr=value</i>	Set of attribute-value pairs that provides details about the logged event. A comma (,) separates each pair. Attribute names are as defined in the Cisco ISE dictionaries. Values of the Response direction AttributesSet are bundled to one attribute called Response and are enclosed in curly brackets { }. In addition, the attribute-value pairs within the Response are separated by semicolons. For example: <pre>Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00; }</pre>

Configuring Remote Syslog Collection Locations

You can create external locations to store the syslogs.

The UDP SysLog (Log Collector) is the default remote logging target. When you disable this logging target, it no longer functions as a log collector and is removed from the Logging Categories page. When you enable this logging target, it becomes a log collector in the Logging Categories page.

-
Step 1	Choose Administration > System > Logging > Remote Logging Targets .
Step 2	Click Add .
Step 3	Configure the field as necessary.
Step 4	Click Save .
Step 5	Go to the Remote Logging Targets page and verify the creation of the new target.
-

After you have created the syslog storage location on logging target page, you should map the storage location to the required logging categories, to receive the logs.

Related Topics

- [Remote Logging Target Settings, page A-13](#)

Remote Syslog Message Format

Log messages are sent to the remote syslog server with this syslog message header format, which precedes the local store syslog message format. (see [Table 11-1](#)):

pri_num YYYY Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num

The syslog message data or payload is the same as the Local Store Syslog Message Format, which is described in [Table 11-1](#).

Table 11-2 Remote Syslog Message Header Format

Field	Description
<i>pri_num</i>	Priority value of the message; a combination of the facility value and the severity value of the message. Priority value = (facility value* 8) + severity value. The facility code valid options are: • LOCAL0 (Code = 16) • LOCAL1 (Code = 17) • LOCAL2 (Code = 18) • LOCAL3 (Code = 19) • LOCAL4 (Code = 20) • LOCAL5 (Code = 21) • LOCAL6 (Code = 22; default) • LOCAL7 (Code = 23) Severity value—See Setting Severity Levels for Message Codes for severity values.
<i>time</i>	Date of the message generation, according to the local clock of the originating Cisco ISE server, in the format <i>YYYY Mmm DD hh:mm:ss</i>. Possible values are: • <i>YYYY</i> = Numeric representation of the year. • <i>Mmm</i> = Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • <i>DD</i> = Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number. • <i>hh</i> = The hour of the day—00 to 23. • <i>mm</i> = The minute of the hour—00 to 59. • <i>ss</i> = The second of the minute—00 to 59. Some device send messages that specify a time zone in the format <i>-/+hhmm</i>, where - and + identifies the directional offset from the Cisco ISE server's time zone, hh is the number of offset hours, and mm is the number of minutes of the offset hour. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server's time zone.
<i>xx:xx:xx:xx/host_name</i>	IP address of the originating Cisco ISE node, or the hostname.
<i>cat_name</i>	Logging category name preceded by the <i>CSCOxxx</i> string.
<i>msg_id</i>	Unique message ID; 1 to 4294967295. The message ID increases by 1 with each new message. Message IDs restart at 1 each time the application is restarted.

Table 11-2 Remote Syslog Message Header Format (continued)

Field	Description
<i>total_seg</i>	Total number of segments in a log message. Long messages are divided into more than one segment. Note The <i>total_seg</i> depends on the Maximum Length setting in the remote logging targets page. See Table A-9 .
<i>seg_num</i>	Segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

Cisco ISE Message Codes

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.

See [Available Reports, page 26-6](#) for more information on the relevant troubleshooting reports per category.

Related Topics:

- [Setting Severity Levels for Message Codes, page 11-6](#)

Setting Severity Levels for Message Codes

You can set the log severity level and choose logging targets where the logs of selected categories will be stored.

-
- Step 1** Choose **Administration > System > Logging > Logging Categories**.
 - Step 2** Click the radio button next to the category that you want to edit, and click **Edit**.
 - Step 3** Modify the required field values.
 - Step 4** Click **Save**.
 - Step 5** Go to the Logging Categories page and verify the configuration changes that were made to the specific category.
-

Related Topics

[Logging Category Settings, page A-14](#)

Cisco ISE Message Catalogs

You can use the Message Catalog page to view all possible log messages and the descriptions. 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.

Debug Log Configuration Options

Debug logs capture bootstrap, application configuration, runtime, deployment, monitoring and reporting, and public key infrastructure (PKI) information.

You can configure the debug log severity level for individual components, and store the debug logs in the local server.

**Note**

A debug log configuration is not saved when a system is restored from a backup or upgraded.

Related Topics

[Configuring Debug Log Severity Levels, page 11-7](#)

Configuring Debug Log Severity Levels

You can configure the severity levels for the debug logs.

Step 1 Choose **Administration > System > Logging > Debug Log Configuration**. The Node List page appears, which contains a list of nodes and their personas. 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 Log Configuration page 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 a set of components.

**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 a component name, choose the desired log severity level from the drop-down list, and click **Save**.
- Choose a component name for which you want to configure the debug log severity level, and click **Edit**. In this page, choose the desired log severity level from the Log Level drop-down list, 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.

Related Topics

- [Cisco ISE Support Bundle, page 25-25](#)
- [Cisco ISE Debug Logs, page 25-27](#)

Collection Filters

You can configure collection filters to suppress syslog messages being sent to the monitoring and external servers. The suppression can be performed at the Policy Services Node level based on different attribute types. You can disable the suppression as well. You can define multiple filters with a specific attribute type and corresponding value.

Before sending syslog messages to a monitoring node or external server, Cisco ISE compares the values with fields in the syslog messages. If any match is found, then the corresponding message is not sent.

Related Topics

[Configuring Collection Filters, page 11-8](#)

Configuring Collection Filters

You can configure multiple collection filters based on various attribute types. It is recommended to limit the number of filters to 20. You can add, edit, or delete a collection filter.

-
- Step 1** Choose **Administration > System > Logging > Collection Filters**.
- Step 2** Click **Add**.
- Step 3** Choose the filter type from the **Attribute** list:
- User Name
 - MAC Address
 - Policy Set Name
 - NAS IP Address
 - Device IP Address
 - Disable Suppression
- Step 4** Enter the corresponding **Value** for the filter type you have selected.
- Step 5** Choose the result based on which the suppression should be filtered from the **Filter By** drop-down list. The result can be All, Passed, or Failed. You can also choose **Disable Suppression** to disable the suppression.

Step 6 Click **Submit**.

Related Topics

[Collection Filters, page 11-8](#)



Managing Backup and Restore Operations

This chapter describes the Cisco Identity Services Engine (ISE) database backup and restore operations, which include Cisco ISE application configuration, Cisco Application Deployment Engine operating system (ADE operating system) configuration and Cisco ISE Monitoring and Troubleshooting database.



Note

Backup and restore is not available for Inline Posture nodes in Cisco ISE, Release 1.2. For more information on other known issues, see [Release Notes for the Cisco Identity Services Engine, Release 1.2](#).

This chapter contains the following sections:

- [Backup Data Type, page 12-1](#)
- [Backup and Restore Repositories, page 12-2](#)
- [On-Demand and Scheduled Backups, page 12-3](#)
- [Cisco ISE Restore Operation, page 12-6](#)
- [Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 12-13](#)
- [Recovery of Lost Nodes in Standalone and Distributed Deployments, page 12-14](#)

Backup Data Type

Cisco ISE allows you to back up data from the primary or standalone Administration node and from the Monitoring node. Backup can be done from the CLI or user interface.

Cisco ISE allows you to back up the following type of data:

- Configuration data—Contains both application-specific and Cisco ADE operating system configuration data.
- Operational Data—Contains monitoring and troubleshooting data.

Restore operation, can be performed with the backup files of previous versions of Cisco ISE and restored on a later version, for example, if you have a backup from an ISE node from Cisco ISE, Release 1.1, you can restore it on Cisco ISE, Release 1.2.

Backup and Restore Repositories

Cisco ISE allows you to create and delete repositories through the Admin portal. You can create the following types of repositories:

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

For the SNS 3415 and SNS 3495 Appliances, there is no physical CD-ROM available. You can create the repository type as CD-ROM for the virtual CD-ROM created using the KVM.

**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.

Related Topics

- [Creating Repositories, page 12-2](#)
- [On-Demand and Scheduled Backups, page 12-3](#)

Creating Repositories

You can use the CLI and GUI to create repositories, but for Cisco ISE, Release 1.2, it is recommended to use the GUI due to the following reasons:

- Repositories that are created through the CLI are saved locally and do not get replicated to the other deployment nodes. These repositories do not get listed in the GUI's repository page.
- Repositories that are created on the primary administration node get replicated to the other deployment nodes.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > System > Maintenance > Repository
Step 2	Click Add to add a new repository.
Step 3	Enter the values as required to set up new repository.
Step 4	Click Submit to create the repository.

- Step 5** Verify that the repository is created successfully by clicking **Repository** in 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.
-

Related Topics

- [Repository Settings, page A-15](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

What to Do Next

- 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 1.2](#).



Note If the path that you provided while creating the repository does not exist, then you will get the following error: %Invalid Directory.

- Run an on-demand backup or schedule a backup. See [Performing an On-Demand Backup](#) and [Scheduling a Backup](#) for more information.

On-Demand and Scheduled Backups

Cisco ISE provides on-demand backups of the primary administration node and the primary monitoring node. Perform an on-demand backup when you want to backup data immediately.

Cisco ISE also allows you to schedule system-level backups that can be scheduled to run once, daily, weekly, or monthly. Because backup operations can be lengthy, you can schedule them so they are not a disruption. You can schedule a backup from the Cisco ISE CLI or through the Cisco ISE Admin portal.



Note If you upgrade to Cisco ISE, Release 1.2, the scheduled backup jobs need to be recreated.

Related Topics

- [Scheduling a Backup, page 12-5](#)
- [Performing an On-Demand Backup, page 12-4](#)
- [Performing a Backup from the CLI, page 12-6](#)
- [Backup History, page 12-6](#)
- [Backup Failures, page 12-6](#)
- [Cisco ISE Restore Operation, page 12-6](#)

Performing an On-Demand Backup

You can perform an On-demand backup to instantly backup the configuration data or monitoring data.

Before You Begin

- Before you perform this task, you should have a basic understanding of the [Backup Data Type](#) in Cisco ISE.
- Ensure that you have completed [Creating Repositories](#).
- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- To perform the following task, you must be a Super Admin or System Admin.



Note

For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing.

Step 1 Choose **Administration > System > Backup and Restore**.

Step 2 Click **Backup Now**.

Step 3 Enter the values as required to perform a backup.

Step 4 Click **OK**.

Step 5 Verify that the backup completed successfully.

Cisco ISE appends the backup filename with a timestamp and stores the file in the specified repository. In addition to the timestamp, Cisco ISE adds a CFG tag for configuration backups and OPS tag for operational backups. Ensure that the backup file exists in the specified repository.

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 a backup is running concurrently. Wait for the backup to complete before you make any node role changes.

Related Topics

- [On-Demand Backup Settings, page A-16](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Backup and Restore Repositories, page 12-2](#)
- [Scheduling a Backup, page 12-5](#)
- [Performing a Backup from the CLI, page 12-6](#)
- [Backup History, page 12-6](#)
- [Backup Failures, page 12-6](#)

Scheduling a Backup

You can use this page to schedule configuration or monitoring backups.

Before You Begin

- Before you perform this task, you should have a basic understanding of the [Backup Data Type](#) and [On-Demand and Scheduled Backups](#) operations in Cisco ISE.
- Ensure that you have configured repositories.
- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- To perform the following task, you must be a Super Admin or System Admin.
- If you have upgraded to Cisco ISE 1.2 from Cisco ISE 1.1 or earlier releases, you should reconfigure your scheduled backups. See the Known Upgrade Issues section in the *Cisco Identity Services Engine Upgrade Guide, Release 1.2*.



Note

For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing.

-
- Step 1** Choose **Administration > System > Backup and Restore**.
 - Step 2** Click **Create** to schedule a Configuration or an Operational backup.
 - Step 3** Enter the values as required to schedule a backup.
 - Step 4** Click **Save** to schedule the backup.
 - Step 5** Click the **Refresh** link at the top of this page to see the scheduled backup list.
-

You can create only one schedule at a time for a Configuration or Operational backup. You can enable or disable a scheduled backup, but you cannot delete it.

To schedule a backup from the CLI, you must use the **kron** CLI command. Although you can schedule backups from the CLI as well as the GUI, it is recommended to use the GUI for better options.

Related Topics

- [Scheduled Backup Settings, page A-16](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Performing an On-Demand Backup, page 12-4](#)
- [Performing a Backup from the CLI, page 12-6](#)
- [Backup History, page 12-6](#)
- [Backup Failures, page 12-6](#)
- [Backup and Restore Repositories](#)
- Refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#) for more information on the **kron** command.

Performing a Backup from the CLI

Although you can schedule backups both from the CLI as well as the GUI, it is recommended to use GUI for better options. But, you can perform Operational backup on the secondary monitoring node only from the CLI.

For information on how to perform a backup from the CLI, see the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

Backup History

Backup history provides basic information about scheduled and on-demand backups. It lists the name of the backup, backup file size, repository where the backup is stored, and time stamp that indicates when the backup was obtained. This information is available in the Operations Audit report and on the Backup and Restore page in the History table.

For failed backups, Cisco ISE triggers an alarm. The backup history page provides the failure reason. The failure reason is also cited in the Operations Audit report. If the failure reason is missing or is not clear, you can run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log for more information.

While the backup operation is in progress, you can use the **show backup status** CLI command to check the progress of the backup operation.

Backup history is stored along with the Cisco ADE operating system configuration data. It remains there even after an application upgrade and are only removed when you reimage the primary administration node.

Backup Failures

If backup fails, check the following:

- Make sure that no other backup is running at the same time.
- Check the available disk space for the configured repository.
 - Monitoring backup fails if the monitoring data takes up more than 75% of the allocated monitoring database size. For example, if your Monitoring node is allocated 600 GB, and the monitoring data takes up more than 450 GB of storage, then monitoring backup fails.
 - If the database disk usage is greater than 90%, a purge occurs to bring the database size to less than or equal to 75% of its allocated size.
- Verify if a purge is in progress. Backup and restore operations will not work while a purge is in progress.
- Verify if the repository is configured correctly.

Cisco ISE Restore Operation

You can restore configuration data on a primary or standalone administration node. After you restore data on the primary administration node, you must manually synchronize the secondary nodes with the primary administration node.

The process for restoring the operational data is different depending on the type of deployment.

**Note**

The new backup/restore user interface in Cisco ISE, Release 1.2 makes use of meta-data in the backup filename. Therefore, after a backup completes, you should not modify the backup filename manually. If you manually modify the backup filename, the Cisco ISE backup/restore user interface will not be able to recognize the backup file. If you have to modify the backup filename, you should use the Cisco ISE CLI to restore the backup.

Related Topics

- [Restoration of Configuration or Monitoring Backup from the CLI, page 12-8](#)
- [Restoring Configuration Backups from the GUI, page 12-10](#)
- [Restoration of Monitoring Database, page 12-10](#)
- [Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 12-13](#)

Data Restoration Guidelines

Following are guidelines to follow when you restore Cisco ISE backup data.

- If you obtain a backup from your primary Administration node in one timezone and try to restore it on another Cisco 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 Cisco 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.
- When you restore a backup on a primary Cisco ISE node with a different hostname than the one from which the backup was obtained, the primary Cisco ISE node becomes a standalone node. The deployment is broken and the secondary nodes become nonfunctional. You must make the standalone node the primary node, reset the configuration on the secondary nodes, and reregister them with the primary node. To reset the configuration on Cisco ISE nodes, enter the following command from the Cisco ISE CLI:
 - **application reset-config ise**
- We recommend that you do not change the system timezone after the initial Cisco ISE installation and setup.
- If you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data after you obtain a backup from the standalone Cisco ISE node or primary Administration node. Otherwise, if you try to restore data using the older backup, the communication between the nodes might fail.
- If you want to retain the existing certificate configuration on a Cisco ISE node after restore, then before you begin restore the data, ensure that you export the certificate along with the private key to the system running your client browser. Then, after you restore the data, import the certificate along with the private key in to the Cisco ISE node.
- 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.
- If you have a standalone administration node that fails, you must run the configuration backup to restore it. If your primary Administration node fails, you can use the distributed setup to promote your secondary Administration node to become the primary. You can then restore data on your primary Administration node after it comes up.

**Note**

Cisco ISE also provides the **backup-logs** CLI command that you can use to collect log and configuration files for troubleshooting purposes. For more information, refer to [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

Restoration of Configuration or Monitoring Backup from the CLI

To restore configuration data through the Cisco ISE CLI, use the **restore** command in the EXEC mode. Use the following command to restore data from a configuration or operational backup:

```
restore filename repository repository-name encryption-key hash | plain encryption-key name  
include-adeos
```

Syntax Description

<code>restore</code>	Type this command to restore data from a configuration or operational backup.
<i>filename</i>	Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters. Note You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
<code>repository</code>	Specifies the repository that contains the backup.
<i>repository-name</i>	Name of the repository you want to restore the backup from.
<code>encryption-key</code>	(Optional) Specifies user-defined encryption key to restore backup.
<code>hash</code>	Hashed encryption key for restoring backup. Specifies an <i>encrypted</i> (hashed) encryption key that follows. Supports up to 40 characters.
<code>plain</code>	Plaintext encryption key for restoring backup. Specifies an <i>unencrypted</i> plaintext encryption key that follows. Supports up to 15 characters.
<i>encryption-key name</i>	Enter the encryption key.
include-adeos	(Optional, applicable only for configuration backup) Enter this command operator parameter if you want to restore ADE-OS configuration from a configuration backup. When you restore a configuration backup, if you do not include this parameter, Cisco ISE restores only the Cisco ISE application configuration data.

Defaults

No default behavior or values.

Command Modes

EXEC

Usage Guidelines

When you use restore commands in Cisco ISE, the Cisco ISE server restarts automatically.

The 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.

Examples

```

ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key
plain Lab12345
Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore. Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Alert Process...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise/admin#

```

Related Commands

Command	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.
show backup history	Displays the backup history of the system.
show backup status	Displays the status of the backup operation.
show restore status	Displays the status of the restore operation.

For more information, refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

For information on checking the status of a restore operation, see the “Restore History” section on [page 12-12](#).

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 12-13](#) for the procedure to perform manual synchronization.

Related Topic

[Restoring Configuration Backups from the GUI, page 12-10](#)

Restoring Configuration Backups from the GUI

You can restore a configuration backup from the Admin portal. The GUI lists only the backups that are taken from Cisco ISE, Release 1.2. To restore backups that are prior to this release, use the restore command from the CLI.

-
- Step 1** Choose **Administration > System > Backup and Restore**.
- Step 2** Select the name of the backup from the list of Configurational backup and click **Restore**.
- Step 3** Enter the Encryption Key used during the backup.
- Step 4** Click **Restore**.
-

Related Topics

[Restoration of Configuration or Monitoring Backup from the CLI, page 12-8](#)

Restoration of Monitoring Database

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 standalone and distributed deployments.

You must use the CLI to restore an on-demand Monitoring database backup from Cisco ISE, Release 1.0, 1.0.4, or 1.1, to Cisco ISE, Release 1.2. Restoring a scheduled backup across Cisco ISE releases is NOT supported.



Note

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 Remote Syslog Collection Locations, page 11-4](#).

Related Topics

- [Restoring a Monitoring Backup in a Standalone Environment, page 12-10](#)
- [Restoring a Monitoring Backup with Administration and Monitor Personas, page 12-11](#)
- [Restoring a Monitoring Backup with a Monitoring Persona, page 12-12](#)

Restoring a Monitoring Backup in a Standalone Environment

The GUI lists only the backups that are taken from Cisco ISE, Release 1.2. To restore backups that are prior to this release, use the restore command from the CLI.

Before You Begin

You should have successfully performed the following procedures:

- [Purging Older Monitoring Data](#), page 25-30
- [Scheduling a Backup](#), page 12-5 or [Performing an On-Demand Backup](#), page 12-4.

-
Step 1	Choose Administration > System > Backup and Restore .
Step 2	Select the name of the backup from the list of Operational backup and click Restore .
Step 3	Enter the Encryption Key used during the backup.
Step 4	Click Restore .
-

Related Topics

- [Restoration of Configuration or Monitoring Backup from the CLI](#), page 12-8
- [Restoring a Monitoring Backup with Administration and Monitor Personas](#), page 12-11
- [Restoring a Monitoring Backup with a Monitoring Persona](#), page 12-12

Restoring a Monitoring Backup with Administration and Monitor Personas

You can restore a Monitoring backup in a distributed environment with Administration and Monitor personas.

Before You Begin

You should have successfully performed the following procedures:

- [Purging Older Monitoring Data](#), page 25-30
- [Scheduling a Backup](#), page 12-5 or [Performing an On-Demand Backup](#), page 12-4.

-
Step 1	Prepare to promote another Cisco ISE node as the primary Administration 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 12-13. 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 node to primary status. For more information, see Configuring a Primary Administration Node , page 3-12.
Step 3	Prepare to deregister the node to be backed up by assigning the Monitoring persona to another node in the deployment. For more information, see Changing Node Personas and Services , page 3-17. A deployment must have at least one functioning Monitoring node.
Step 4	Deregister the node to be backed up. For more information, see Removing a Node from Deployment , page 3-19.
Step 5	Restore the Monitoring backup to the newly deregistered node, as described in Restoring a Monitoring Backup in a Standalone Environment , page 12-10.
Step 6	Register the newly restored node with the current Administration node. For more information, see Registering a Secondary Cisco ISE Node , page 3-12.

- Step 7** Promote the newly restored and registered node as the primary Administration node. For more information, see [Configuring a Primary Administration Node, page 3-12](#).
-

Related Topics

- [Restoring a Monitoring Backup in a Standalone Environment, page 12-10](#)
- [Restoring a Monitoring Backup with a Monitoring Persona, page 12-12](#)

Restoring a Monitoring Backup with a Monitoring Persona

You can restore a Monitoring backup in a distributed environment with only Monitoring persona.

Before You Begin

You should have successfully performed the following procedures:

- [Purging Older Monitoring Data, page 25-30](#)
- [Scheduling a Backup, page 12-5](#) or [Performing an On-Demand Backup, page 12-4](#).

- Step 1** Prepare to deregister the node to be restored by assigning the Monitoring persona to another node in the deployment. For more information, see [Changing Node Personas and Services, page 3-17](#).

A deployment must have at least one functioning Monitoring node.

- Step 2** Deregister the node to be restored. For more information, see [Removing a Node from Deployment, page 3-19](#).



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 Monitoring Backup in a Standalone Environment, page 12-10](#).

- Step 4** Register the newly restored node with the current Administration node. For more information, see [Registering a Secondary Cisco ISE Node, page 3-12](#).

- Step 5** Promote the newly restored and registered node as the primary Administration node. For more information, see [Configuring a Primary Administration Node, page 3-12](#).
-

Related Topics

- [Restoring a Monitoring Backup in a Standalone Environment, page 12-10](#)
- [Restoring a Monitoring Backup with Administration and Monitor Personas, page 12-11](#)

Restore History

You can obtain information about all restore operations, log events, and statuses from the Operations Audit report.

**Note**

However, the Operations Audit report does not provide information about the start times corresponding to the previous restore operations.

For troubleshooting information, you have to run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log file.

While the restore operation is in progress, all Cisco ISE services are stopped. You can use the **show restore status** CLI command to check the progress of the restore operation.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Synchronizing Primary and Secondary Nodes in a Distributed Environment

In a distributed environment, sometimes the Cisco ISE database in the primary and secondary nodes are not synchronized automatically after restoring a backup file on the primary administration node. If this happens, you can manually force a full replication from the primary administration node to the 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. Cisco ISE allows you to navigate to other Cisco ISE Admin portal pages and make any configuration changes only after the synchronization is complete.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > System > Deployment .
Step 2	Check the check boxes next to the secondary ISE nodes with an Out of Sync replication status.
Step 3	Click Syncup and wait until 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 Admin portal again.
-

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Recovery of Lost Nodes in Standalone and Distributed Deployments

This section provides troubleshooting information that you can use to recover lost nodes in standalone and distributed deployments. Some of the following use cases use the backup and restore functionality and others use the replication feature to recover lost data:

- [Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment, page 12-14](#)
- [Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment, page 12-15](#)
- [Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment, page 12-15](#)
- [Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment, page 12-16](#)
- [Configuration Rollback, page 12-16](#)
- [Recovery of Primary Node in Case of Failure in a Distributed Deployment, page 12-17](#)
- [Recovery of Secondary Node in Case of Failure in a Distributed Deployment, page 12-17](#)

Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment

Scenario

In a distributed deployment, a natural disaster leads to a loss of all the nodes. After recovery, you want to use the existing IP addresses and hostnames.

For example, you have two nodes: N1 (primary Administration node) and N2 (secondary Administration node.) A backup of the N1 node, which was taken at time T1, is available. 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 the N1 and N2 nodes. See [“Replacing the Cisco ISE Appliance Hardware” section on page 3-20](#) for more information. N1 and N2 nodes will now have a standalone configuration.
2. Obtain a license with the UDI of the N1 and N2 nodes and install it on the N1 node.
3. You must then restore the backup on the replaced N1 node. See [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) 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.
4. You must log in to the N1 Admin portal to delete and reregister the N2 node. See the following for more information:
 - [“Removing a Node from Deployment” section on page 3-19](#)

- [“Registering a Secondary Cisco ISE Node” section on page 3-12](#)

Both the N1 and N2 nodes will have data reset to time T1.

Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment

Scenario

In a distributed deployment, a natural disaster leads to loss of all the nodes. The new hardware is reimaged at a new location and requires new IP addresses and hostnames.

For example, you have two ISE nodes: N1 (primary Administration node) and N2 (secondary Policy Service node.) A backup of the N1 node which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster. The Cisco 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 [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) 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 8-18](#) for more information.
3. You must log in to the Cisco ISE Admin portal on N1A, choose **Administration > System > Deployment**, and do the following:
 - a. Delete the old N2 node. See [“Removing a Node from Deployment” section on page 3-19](#) for more information.
 - b. Register the new N2A node as a secondary node. See [“Registering a Secondary Cisco ISE Node” section on page 3-12](#) for more information. Data from the N1A node will be replicated to the N2A node.

Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database was taken at time T1. 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 up after a reimage or you have introduced a new Cisco 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 [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) for more information.

Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database taken at time T1 is available. The N1 node is 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 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 3-20](#) 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 [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) 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 [“Restoration of Configuration or Monitoring Backup from the CLI” section on page 12-8](#) for more information. The restore script will sync the data from N1 to N2.

Recovery of Primary Node in Case of Failure in a Distributed Deployment

Scenario

In a multinode deployment, the primary administration node fails.

For example, you have two Cisco 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 in to the N2 Admin portal. Choose **Administration > System > Deployment** and configure N2 as your primary node. See [“Promoting Secondary Administration Node To Primary” section on page 3-17](#) for more information.

The N1 node is replaced with a new hardware, reimaged, and is in the standalone state.

2. From the N2 Admin portal, register the new N1 node as a secondary node. See [“Registering a Secondary Cisco ISE Node” section on page 3-12](#) 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 in to the N1 Admin portal and make it the primary node. N2 automatically becomes a secondary server. There is no data loss.

Recovery of Secondary Node in Case of Failure in a Distributed Deployment

Scenario

In a multinode deployment, a single secondary node has failed. No restore is required.

For example, 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 in to the N1 Admin portal and delete the N3 node. See [“Removing a Node from Deployment” section on page 3-19](#) for more information.
3. Reregister the N3A node. See [“Registering a Secondary Cisco ISE Node” section on page 3-12](#) for more information.

Data is replicated from N1 to N3A. No restore is required.



Setting Up Endpoint Protection Service

Endpoint Protection Service (EPS) is a service that runs on the Administration node that can be used for monitoring and controlling network access of endpoints. EPS supports wired and wireless deployments and requires an Advanced License.

This chapter describes how to set up and configure EPS:

- [Configuring Endpoint Protection Service, page 13-1](#)
- [Creating Authorization Profiles for Network Access through EPS, page 13-2](#)
- [Creating Exception Policies for Network Access through EPS, page 13-2](#)
- [Configuring Network Access Settings, page 13-3](#)
- [Endpoint Protection Service, page 13-4](#)
- [EPS Quarantine and Unquarantine Flow, page 13-5](#)
- [EPS NAS Port Shutdown Flow, page 13-5](#)

Configuring Endpoint Protection Service

Endpoint Protection Service (EPS) is disabled by default. You must enable EPS manually, and it remains enabled until you manually disable the service in the Admin portal.

You must have Super Admin and Policy Admin role privileges to enable EPS in Cisco ISE.

-
Step 1	Choose Administration > System > Settings > Endpoint Protection Service .
Step 2	Click the Service Status drop-down list, and choose Enabled .
Step 3	Click Save .
-

Related Topics

- [Creating Authorization Profiles for Network Access through EPS, page 13-2](#)
- [Creating Exception Policies for Network Access through EPS, page 13-2](#)

Creating Authorization Profiles for Network Access through EPS

You must create an authorization profile for use with EPS and the authorization profile appears in the list of Standard Authorization Profiles. An endpoint can be authenticated and authorized in the network, but restricted to access network.

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
 - Step 2** Click **Add**.
 - Step 3** Enter a unique name and description for the authorization profile, and leave the Access Type as **ACCESS_ACCEPT**.
 - Step 4** Check the **DACL Name** check box, and choose **DENY_ALL_TRAFFIC** from the drop-down list.
 - Step 5** Click **Submit**.
-

Related Topics

- [Creating Exception Policies for Network Access through EPS, page 13-2](#)
- [Configuring Network Access Settings, page 13-3](#)

Creating Exception Policies for Network Access through EPS

For EPS authorization, you must create a quarantine exception policy that is processed before all standard authorization policies. Exception authorization policies are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement. Standard authorization policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges.

Before You Begin

You should have successfully created standard authorization profiles for use with EPS.

-
- Step 1** Choose **Policy > Authorization**, and expand **Exceptions**.
 - Step 2** Choose **Enabled** or **Disabled** or **Monitor Only** option.
 - Step 3** Click **Create a New Rule**.
 - Step 4** Enter the exception rule name.
 - Step 5** Click the plus [+] sign to choose an identity group.
 - Step 6** Click the plus [+] sign to choose **Create New Condition (Advanced Option)**.
 - Step 7** Click the down arrow icon in the first field to display the dictionaries list and choose **Session > EPSSstatus**.
 - Step 8** Choose **Equals** from the drop-down list in the second field.
 - Step 9** Choose **Quarantine** from the drop-down list in the third field.
 - Step 10** Click **Save**.
-

Related Topics[Configuring Network Access Settings, page 13-3](#)

Configuring Network Access Settings

Endpoint Protection Service (EPS) allows you to reset the network access status of an endpoint to quarantine, unquarantine, or shutdown a port, which defines authorization to the network depending on the network access status.

You can quarantine or unquarantine endpoints, or shut down the network access server (NAS) ports to which endpoints are connected, by using their endpoint IP addresses or MAC addresses. You can perform quarantine and unquarantine operations on the same endpoint multiple times, provided they are not performed simultaneously. If you discover a hostile endpoint on your network, you can shut down the endpoint's access, using EPS to close the NAS port.

Before you Begin

- You must enable EPS.
- You must create authorization profiles and Exception type authorization policies for EPS.

-
Step 1	Choose Operations > Endpoint Protection Service .
Step 2	Enter the IP Address or MAC Address of an endpoint.
Step 3	Click the Operations drop-down list to choose one of the following actions: • Quarantine—Isolates the endpoint, restricting access on the network • Unquarantine—Reverses the quarantine process, allowing full access to the network • Shutdown—Closes the NAS port to which the endpoint is connected
Step 4	Click Submit .
-

Related Topics

- [EPS Operations Fail when IP Address or MAC Address is not Found, page 13-3](#)
- [Externally Authenticated Administrator Cannot Perform EPS Operations, page 13-4](#)
- [EPS Quarantine and Unquarantine Flow, page 13-5](#)
- [EPS NAS Port Shutdown Flow, page 13-5](#)

EPS Operations Fail when IP Address or MAC Address is not Found

An EPS operation that you perform on an endpoint fails when an active session for that endpoint does not contain information about the IP address. This also applies to the MAC address and session ID for that endpoint.

- When you want to change the authorization state of an endpoint through EPS, you must provide the IP address or the MAC address for the endpoint. If the IP address or the MAC address is not found in the active session for the endpoint, then you will see the following error message: No active session found for this MAC address, IP Address or Session ID.

Externally Authenticated Administrator Cannot Perform EPS Operations

If an externally authenticated administrator tries to issue CoA-Quarantine from a live session, Cisco ISE returns the following error message:

CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User not found internally. Possible use of unsupported externally authenticated user

If an externally authenticated administrator performs an EPS operation from Operations > Endpoint Protection Service in the Cisco ISE Admin portal using the IP address or MAC address of the endpoint, Cisco ISE returns the following error message:

Server failure: User not found internally. Possible use of unsupported externally authenticated user

Endpoint Protection Service

You can use Endpoint Protection Service (EPS) to change the authorization state without having to modify the overall authorization policy of the system. EPS allows you to set the authorization state when you quarantine an endpoint as a result of established authorization policies where authorization policies are defined to check for EPSStatus to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

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.

You can perform the following operations to monitor and control network access through EPS:

- **Quarantine**—Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the EPS status. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.
- **Unquarantine**—Allows you to reverse the quarantine status that permits full access to the network for an endpoint returning the endpoint to its original VLAN.
- **Shutdown**—Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shutdown on the NAS to which an endpoint is connected, you must manually reset the port on the NAS again to allow an endpoint to connect to the network, which is not available for wireless deployments.

Quarantine and unquarantine operations can be triggered from the session directory reports for active endpoints.



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.

Related Topics

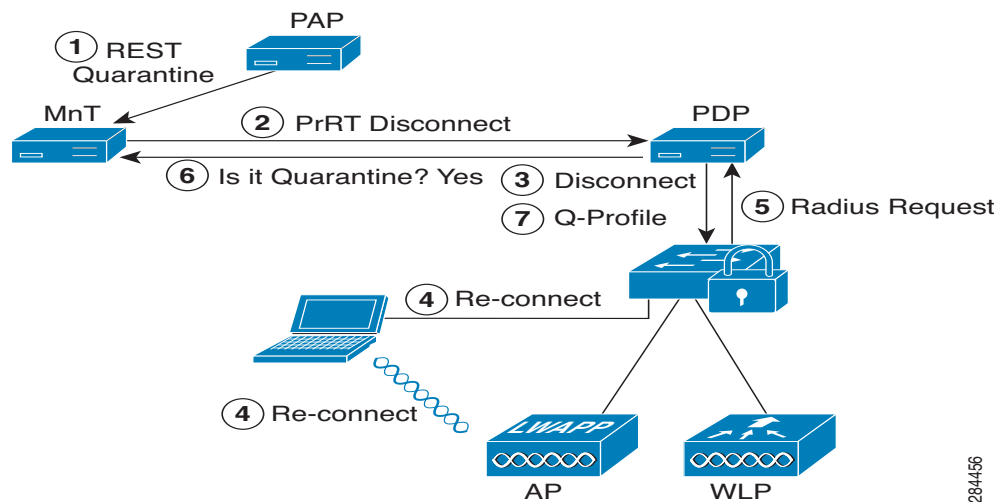
- [Configuring Network Access Settings, page 13-3](#)

EPS Quarantine and Unquarantine Flow

You can quarantine selected endpoints with EPS, to limit their access to the network. You can quarantine endpoints and establish exception authorization policies that assign different authorization profiles, depending on the status. An authorization profile acts as a container for permissions that you define in the authorization policies that allow access to specified network services. When the authorization is complete, the permissions are granted for a network access request. If the endpoint is then validated, you can unquarantine the endpoint to allow it full access to the network.

Figure 13-1 illustrates the quarantine flow, which assumes that authorization rules have been configured and the EPS session has been established.

Figure 13-1 EPS Quarantine Flow



1. A client device logs onto the network through a wireless device (WLC), and a quarantine REST API call is issued from the Administration node (PAP) to the Monitoring node (MnT).
2. The Monitoring node then calls PrRT through the Policy Services ISE node (PDP) to invoke a CoA.
3. The client device is disconnected.
4. The client device then reauthenticates and reconnects.
5. A RADIUS request for the client device is sent back to the Monitoring node.
6. The client device is quarantined while the check is made.
7. The Q-Profile authorization policy is applied, and the client device is validated.
8. The client device is unquarantined, and allowed full access to the network.

EPS NAS Port Shutdown Flow

You can shut down the NAS port to which an endpoint is connected by using the endpoint IP address or MAC address.

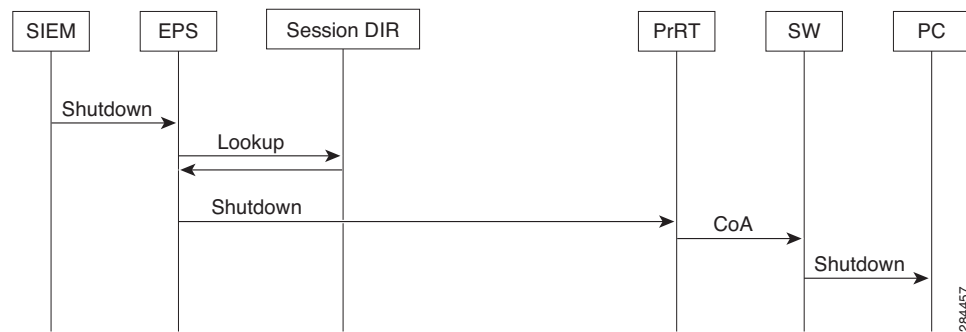
Shutdown allows you to close a NAS port based on a specified IP address for a MAC address, and you have to manually reinstate the port to bring the endpoint back into the network, which is effective only for endpoints that are connected through wired media.

Shutdown may not be supported on all devices. Most switches should support the shut down command, however. You can use the `getResult()` command to verify that the shutdown executed successfully.

Figure 13-2 illustrates the EPS shutdown flow.

For the client device in the illustration, the shutdown operation is performed on the NAS that the client device uses to access the network.

Figure 13-2 EPS Shutdown Flow





PART 4

Managing Users and End-User Portals



Managing Users and External Identity Sources

This chapter describes how to manage user accounts in Cisco ISE and the various identity sources that you can use to store user information for authentication and authorization purposes.

In this chapter, the term user refers to employees, contractors, and sponsor users. Guest users are covered in detail in [Chapter 16, “Supporting Authorized Network Access for Guests.”](#)

This chapter contains the following sections:

- [Cisco ISE Users, page 14-1](#)
- [Identity Sources, page 14-6](#)
- [Certificate Authentication Profiles, page 14-8](#)
- [Active Directory as an External Identity Source, page 14-9](#)
- [LDAP, page 14-19](#)
- [RADIUS Token Identity Sources, page 14-27](#)
- [RSA Identity Sources, page 14-32](#)
- [Identity Source Sequences, page 14-38](#)
- [Identity Source Details in Reports, page 14-39](#)

Cisco ISE Users

In this chapter, the term user refers to employees and contractors who access the network regularly as well as sponsor and guest users. A sponsor user is an employee or contractor of the organization who creates and manages guest-user accounts through the sponsor portal. A guest user is an external visitor who needs access to the organization’s network resources for a limited period of time.

You must create an account for any user to gain access to resources and services on the Cisco ISE network. Employees, contractors, and sponsor users are created from the Admin portal.

Related Topics

- [Managing Sponsor and Guest Accounts, page 16-3](#)
- [Cisco Identity Services Engine Sponsor Portal User Guide, Release 1.2](#)

User Identity

User identity is like a container that holds information about a user and forms their network access credentials. Each user's identity is defined by data and includes: a username, e-mail address, password, account description, associated administrative group, user group, and role.

User Groups

User groups are a collection of individual users who share a common set of privileges that allow them to access a specific set of Cisco ISE services and functions.

User Identity Groups

A user's group identity is composed of elements that identify and describe a specific group of users that belong to the same group. A group name is 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.

Default User Identity Groups

Cisco ISE comes with the following predefined user identity groups:

- Employee—Employees of your organization belong to this group.
- SponsorAllAccount—Sponsor users who can suspend or reinstate all guest accounts in the Cisco ISE network.
- SponsorGroupAccounts—Sponsor users who can suspend guest accounts created by sponsor users from the same sponsor user group.
- SponsorOwnAccounts—Sponsor users who can only suspend the guest accounts that they have created.
- Guest—A visitor who needs temporary access to resources in the network.
- ActivatedGuest—A guest user whose account is enabled and active.

User Role

A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. A user role is associated with a user group. For example, a network access user.

User Account Custom Attributes and Password Policies

Cisco ISE allows you to restrict a user's network access based on user attributes. Cisco ISE comes with a set of predefined user attributes and also allows you to create custom attributes. Both types of attributes can be used in conditions that define the authentication policy. You can also define a password policy for user accounts so that passwords meet specified criteria.

This section contains the following topics:

- [Custom User Attributes, page 14-3](#)
- [User Password Policy Settings, page 14-3](#)

Custom User Attributes

On the User Custom Attributes Setting page, you can use the Custom Attributes pane to define additional user-account attributes. Cisco ISE provides a list of predefined attributes that are not configurable. However, you can define custom attributes by configuring the following:

- Attribute name
- Data type

User Password Policy Settings

You can define the criteria that user-account passwords must meet in the User Password Policy page. Choose **Administration > Identity Management > Settings > User Password Policy**.

[Table A-34](#) describes the setting fields in the User Password Policy page.



Note

- Password lifetime feature is there to ensure that users and sponsors change their password regularly.
- This feature does not affect local "admin" users.
- If using "disable account" we strongly recommend using "reminder" functionality to avoid users getting locked.
- User expiry thread works at midnight and will disable all accounts that exceed the password lifetime.

Adding Users

Cisco ISE allows you to view, create, modify, duplicate, delete, change the status, import, export, or search for attributes of Cisco ISE users.

If you are using a Cisco ISE internal database, you must create an account for any new user who needs access to resources or services on a Cisco ISE network.

-
Step 1	Choose Administration > Identity Management > Identities > Users .
Step 2	Click Add (+) to create a new user.
Step 3	Enter values for the fields. Do not include spaces in the username.
Step 4	Click Submit to create a new user in the Cisco ISE internal database.
-

Related Topics

- [Cisco ISE Users, page 14-1](#)
- [User Identity Groups, page 14-2](#)
- [User Account Custom Attributes and Password Policies, page 14-2](#)
- [Exporting Cisco ISE User Data, page 14-4](#)
- [Importing Cisco ISE User Data, page 14-4](#)

Exporting Cisco ISE User Data

You might have to export user data from the Cisco ISE internal database. Cisco ISE allows you to export user data in the form of a password-protected csv file.

-
- Step 1** Choose **Administration > Identity Management > Identities > Users**.
- Step 2** Check the check box that corresponds to the user(s) whose data you want to export.
- Step 3** Click **Export Selected**.
- Step 4** Enter a key for encrypting the password in the Key field.
- Step 5** Click **Start Export** to create a users.csv file.
- Step 6** Click **OK** to export the users.csv file.
-

Related Topics

- [Cisco ISE Users, page 14-1](#)
- [User Identity Groups, page 14-2](#)
- [User Account Custom Attributes and Password Policies, page 14-2](#)
- [Adding Users, page 14-3](#)
- [Importing Cisco ISE User Data, page 14-4](#)

Importing Cisco ISE User Data

Cisco ISE allows you to import user data in the form of a csv file into its internal database. Instead of entering user accounts manually into Cisco ISE, you can import them.

-
- Step 1** Choose **Administration > Identity Management > Identities > Users**.
- Step 2** Click **Import** to import users from a comma-delimited text file.

**Tip**

(Optional) If you do not have a comma-delimited text file, click **Generate a Template** to create this type of file.

- Step 3** In the File text box, enter the filename containing the users to import, or click **Browse** and navigate to the location where the file resides.

- Step 4** Check the **Create new user(s) and update existing user(s) with new data** check boxes if you want to both create new users and update existing users.
- Step 5** Click **Save** to save your changes to the Cisco ISE internal database.
-

Related Topics

- [Cisco ISE Users, page 14-1](#)
- [User Identity Groups, page 14-2](#)
- [User Account Custom Attributes and Password Policies, page 14-2](#)
- [Adding Users, page 14-3](#)
- [Exporting Cisco ISE User Data, page 14-4](#)

Creating a User Identity Group

You must create a user identity group before you can assign a user to it.

-
- Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups > Add**.
- Step 2** Enter values in the Name and Description fields. Supported characters for the Name field are space # \$ & ' () * + - . / @ _ .
- Step 3** Click **Submit**.
-

Related Topics

- [Cisco ISE Users, page 14-1](#)
- [User Identity Groups, page 14-2](#)
- [Default User Identity Groups, page 14-2](#)
- [Exporting User Identity Groups, page 14-5](#)
- [Importing User Identity Groups, page 14-6](#)

Exporting User Identity Groups

Cisco ISE allows you to export locally configured user identity groups in the form of a csv file.

-
- Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups**.
- Step 2** Check the check box that corresponds to the user identity group that you want to export, and click **Export**.
- Step 3** Click **OK**.
-

Related Topics

- [Cisco ISE Users, page 14-1](#)
- [User Identity Groups, page 14-2](#)
- [Creating a User Identity Group, page 14-5](#)
- [Importing User Identity Groups, page 14-6](#)

Importing User Identity Groups

Cisco ISE allows you to import user identity groups in the form of a csv file.

-
Step 1	Choose Administration > Identity Management > Groups > Identity Groups > User Identity Groups .
Step 2	Click Generate a Template to get a template to use for the import file.
Step 3	Click Import to import network access users from a comma-delimited text file.
Step 4	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.
Step 5	Click Import .
Step 6	Click Save to save your changes to the Cisco ISE database.
-

Related Topics

- [Cisco ISE Users, page 14-1](#)
- [User Identity Groups, page 14-2](#)
- [Creating a User Identity Group, page 14-5](#)
- [Exporting User Identity Groups, page 14-5](#)

Identity Sources

Identity sources contain user information that Cisco ISE uses to validate credentials during user authentication, and to retrieve group information and other attributes that are associated with the user for use in authorization policies. They are databases that store user information in the form of records. You can add, edit, and delete user information from identity sources.

Cisco ISE supports internal and external identity sources. Both sources can be used as an authentication source for sponsor-user and guest-user authentication.

Related Topics

- [Internal Identity Sources, page 14-7](#)
- [External Identity Sources, page 14-7](#)

Internal Identity Sources

Cisco ISE has an internal user database that you can use to store user information. Users in the internal user database are called internal users. Cisco ISE also has an internal endpoint database that stores information about all the devices and endpoints that connect to it.

External Identity Sources

Cisco ISE allows you to configure the external identity source that contains user information. Cisco ISE connects to an external identity source to obtain user information for authentication. External identity sources also include certificate information for the Cisco ISE server and certificate authentication profiles. Cisco ISE uses authentication protocols to communicate with external identity sources.

[Table 14-1](#) lists authentication protocols and the external identity sources that they support.

Table 14-1 Authentication Protocols and Supported External Identity Sources

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 can optionally be added for authorization policy conditions.	Yes	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.

Related Topics

- [Certificate Authentication Profiles, page 14-8](#)
- [Active Directory as an External Identity Source, page 14-9](#)
- [LDAP, page 14-19](#)
- [RADIUS Token Identity Sources, page 14-27](#)
- [RSA Identity Sources, page 14-32](#)
- [Identity Source Sequences, page 14-38](#)
- [Identity Source Details in Reports, page 14-39](#)

Certificate Authentication Profiles

For each profile, you must specify the certificate field that should be used as the principal username and whether you want a binary comparison of the certificates.

Related Topics:

[Adding a Certificate Authentication Profile, page 14-8](#)

Adding a Certificate Authentication Profile

You must create a certificate authentication profile if you want to use the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) certificate-based authentication method. Instead of authenticating via the traditional username and password method, Cisco ISE compares a certificate received from a client with one in the server to verify the authenticity of a user.

Before You Begin

You must be a Super Admin or System Admin.

For Windows certificate-based authentication, you must specify the Subject Alternative Name or Subject Name.

If you are authenticating via Anyconnect 3.1, you must specify the Subject Alternative Name for Microsoft certificates when using the EAP-FAST protocol with client-certificate authentication.

If you are using certificates issued by other certificate authorities, you need to specify the Common Name.

-
Step 1	Choose Administration > Identity Management > External Identity Sources > Certificate Authentication Profile > Add .
Step 2	Enter the name and description for the certificate authentication profile.
Step 3	Choose the Principal Username X509 attribute.
Step 4	Check box if you want to validate certificate information for authentication against a selected Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory identity source. Check the Perform Binary Certificate Comparison with Certificate Retrieved from LDAP or Active Directory check box.

**Note**

If you check this check box, you must choose the LDAP or Active Directory identity source from the available list.

- Step 5** Choose the LDAP or Active Directory identity source against which you want to validate the certificate information for authentication.
- Step 6** Click **Submit** to add the certificate authentication profile or save the changes.

What To Do Next:

1. See [Chapter 19, “Managing Authentication Policies”](#) for information on how to create authentication policies.
2. See [Chapter 20, “Managing Authorization Policies and Profiles”](#) for information on how to create authorization profiles and policies.

Active Directory as an External Identity Source

Cisco ISE uses Microsoft Active Directory (AD) as an external identity source to access resources such as users, machines, groups, and attributes.

Cisco ISE supports Microsoft AD sites and services when integrated with AD.

User and Machine Authentication in Active Directory

User and machine authentication in Active Directory allows network access only to users and devices that are listed in Active Directory.

Active Directory Supported Authentication Protocols and Features

Active Directory supports features such as user and machine authentications, changing Active Directory user passwords, and so on with some protocols. [Table 14-2](#) lists the authentication protocols and the respective features that are supported by Active Directory.

Table 14-2 **Active Directory Supported Authentication Protocols**

Authentication Protocols	Features
EAP-FAST and Protected Extensible Authentication Protocol (PEAP)	User and machine authentication with the ability to change passwords using EAP-FAST and PEAP with an inner method of MS-CHAPv2 and EAP-GTC
Password Authentication Protocol (PAP)	Authentication and ability to change passwords
Microsoft Challenge Handshake Authentication Protocol Version 1 (MS-CHAPv1)	User and machine authentication
Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)	User and machine authentication

Table 14-2 Active Directory Supported Authentication Protocols

Authentication Protocols	Features
Extensible Authentication Protocol-Generic Token Card (EAP-GTC)	User and machine authentication
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	User and machine authentication using the certificate retrieval option
Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)	User and machine authentication
Lightweight Extensible Authentication Protocol (LEAP)	User authentication

Active Directory Attribute and Group Retrieval for Use in Authorization Policies

Cisco ISE retrieves user or machine attributes from Active Directory for use in authorization policy rules. These attributes are mapped to Cisco ISE policies and determine the authorization level for a user or machine. Cisco ISE retrieves user and machine Active Directory attributes after successful authentication and can also retrieve attributes for an authorization that is independent of authentication.

Cisco ISE performs user and group membership lookups via LDAP to an Active Directory. Group membership is used to map sponsor users to the corresponding sponsor group in ISE. And if the user is not directly in an Active Directory group, but is a member of a group that is a member of the Active Directory group (nested groups), the user authorization is rejected.

User authentication on an authorization policy fails if the rule contains an Active Directory group name with special characters such as `!@#$%^&*()_+~`

Active Directory Certificate Retrieval for Certificate-Based Authentication

Cisco ISE supports certificate retrieval for user and 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. Cisco ISE identifies this attribute as `userCertificate` and does not allow you to configure any other name for this attribute. Cisco 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 certificates, for example, Subject Alternative Name (SAN), Common Name, or Social Security Number (SSN). After Cisco ISE retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, Cisco ISE compares the certificates to check for one that matches. When a match is found, the user or machine is granted access to the network.

Active Directory User Authentication Process Flow

When authenticating or querying a user, Cisco ISE checks 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 in 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 Active Directory Multidomain Forests

Cisco ISE supports Active Directory with multidomain forests. Cisco 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 Cisco ISE is connected and the other domains.



Note

Cisco ISE does not support Microsoft Active Directory servers that reside behind a network address translator and have a Network Address Translation (NAT) address.

Refer to [Release Notes for Cisco Identity Services Engine, Release 1.2](#) for a list of Windows Server Operating Systems that support Active Directory services.

Guidelines for Setting Up Active Directory as an External Identity Source

Read the following statements carefully to ensure that these settings are configured properly for Cisco ISE to connect to Active Directory and successfully authenticate users:

- Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory.
- If you have a firewall between Cisco ISE and Active Directory, ensure that the following ports are open for communication between Cisco ISE and Active Directory.

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 = key distribution center.
3. LDAPS = Lightweight Directory Access Protocol over TLS/SSL.

- If Active Directory has a multidomain forest, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. For more information on establishing trust relationships, refer to *Microsoft Active Directory documentation*.

- All of the Cisco ISE nodes in the deployment need to be able to perform forward and reverse Domain Name Service (DNS) lookup to effectively interoperate with Active Directory. DNS servers that you configure in Cisco ISE using the **ip name-server** command should be able to accurately resolve the domain names in an Active Directory identity source. The DNS server that is part of an Active Directory deployment is usually configured in Cisco ISE. If you have to configure multiple DNS servers, you can use the **application configure ise** command to do so.
- You must have at least one global catalog server operational in the domain to which you are joining Cisco ISE.
- The Active Directory username that you provide when joining to an Active Directory domain should be predefined in Active Directory and must have one of the following permissions:
 - Add the workstation to the domain to which you are trying to connect.
 - On the computer where the Cisco ISE account was created, establish permissions for creating or deleting computer objects before joining Cisco ISE to the domain.
 - Permissions for searching users and groups that are required for authentication.

After you join Cisco ISE to the Active Directory domain, you will still need these permissions to:

- Join any secondary Cisco ISE servers to this domain
- Back up or restore data
- Upgrade Cisco ISE to a higher version, if the upgrade process involves a backup and restore

Related Topics

- [Specifying System Time and NTP Server Settings, page 5-3](#)
- [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#)

Configuring Active Directory as an External Identity Source

Before You Begin

- Ensure that Cisco ISE hostnames are 15 characters or less in length. Active Directory does not validate hostnames larger than 15 characters.
- Ensure that the Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- Ensure that the Microsoft Active Directory administrator account is valid, which is used for the join operation, and it is not configured with Change Password on Next Login in Microsoft Active Directory.
- To perform the following task, you must be a Super Admin or System Admin.



Note

Even when Cisco ISE is connected to Active Directory, there may still be operation issues. To identify them refer to the Authentication Report under **Operations > Reports**.

You must complete the following tasks to configure Active Directory as an external identity source.

- [Connecting to the Active Directory Domain, page 14-13](#)
- [Enabling Password Changes, Machine Authentications, and Machine Access Restrictions, page 14-13](#)
- [Configuring Active Directory User Groups, page 14-14](#)

Connecting to the Active Directory Domain

-
- Step 1** Connect to the Active Directory domain that contains the user and machine information.
- Step 2** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.
- Step 3** Enter the domain name and friendly name.
- Step 4** Click **Save Configuration**. After you save the configuration successfully, the deployment join/leave table is displayed with all the Cisco ISE nodes, node roles, and their status.
- 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 Cisco ISE nodes are joined to the domain.
- Step 5** Click **Join** to connect the Cisco ISE node to the Active Directory domain. You must do this explicitly even though you saved the configuration. You must join each of the secondary policy service nodes in your deployment individually.
- Step 6** Check the check box next to the Cisco ISE node and click **Test Connection** to verify if the Cisco ISE node can be connected to the Active Directory domain. You can do a basic or a detailed test. A detailed test may take longer to complete for a large Active Directory deployment.
- Step 7** Enter the Active Directory username and password and click **OK**.

**Note**

You cannot use an alternate User Principal Name (UPN) to join Cisco ISE to the Active Directory. If the 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, in the example.com domain there are two subdomains called sub1 and sub2. If the user belongs to sub1, then the username should be sub1\user1.

-
- Step 8** Click **OK**.
- Step 9** To join the Cisco ISE node to the Active Directory domain, check the check box next to the Cisco ISE node and click **Join**.
- Step 10** Enter the Active Directory username and password and click **OK**.
- You can select more than one node to join to the Active Directory domain.
- If the join operation is not successful, a failure message appears in the pop-up. You can click the failure message for each node to view detailed logs for that node.
- Step 11** Click **Close**.
-

What To Do Next

[Enabling Password Changes, Machine Authentications, and Machine Access Restrictions, page 14-13](#)

Enabling Password Changes, Machine Authentications, and Machine Access Restrictions

Before you begin

- You must join Cisco ISE to the Active Directory domain
- Configure the advanced settings.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.

- Step 2** Click the **Advanced Settings** tab.
 - Step 3** Check the **Enable Password Change** check box to allow users to change the user password in Active Directory.
 - Step 4** Check the **Enable Machine Authentication** check box to allow machine authentication.
 - Step 5** 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.
 - Step 6** Enter the Aging Time if you have enabled MARs.
This value is in hours and specifies the expiration time for machine authentication. For example, if you enable MARs and enter a value of 2, user authentication fails if a user tries to authenticate after 2 hours.
 - Step 7** Click **Save Configuration**.
-

What To Do Next

[Configuring Active Directory User Groups, page 14-14](#)

Configuring Active Directory User Groups

You must configure Active Directory User Groups for them to be available for use in authorization policies.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.
 - Step 2** Click the **Groups** tab.
If you want to add groups from the directory, you can search for them using a filter. For example, enter **cn=users** as the filter criteria and click **Retrieve Groups** to view user groups that begin with cn=users. You can also enter the asterisk (*) wildcard character to filter the results
 - Step 3** Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to an existing group.
 - Step 4** Enter a name for a new group if you choose to add a group.
 - Step 5** Check the check boxes next to the groups that you want to be available for use in authorization policies and click **OK**.
 - Step 6** Click **Save Configuration**.
-

What To Do Next

[Configuring Active Directory User Attributes, page 14-14](#)

Configuring Active Directory User Attributes

You must configure Active Directory user attributes to be able to use them in authorization policy conditions.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.
 - Step 2** Click the **Attributes** tab.

If you choose to add attributes from directory, enter the name of a user in the Example User field, and click **Retrieve Attributes** to obtain a list of attributes for users. For example, enter **admin** to obtain a list of administrator attributes. You can also enter the asterisk (*) wildcard character to filter the results.

- Step 3** Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to choose a list of attributes from the directory.



Note When you enter an example user name, 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.

- Step 4** Enter a name for a new attribute if you choose to add an attribute.
- Step 5** Check the check boxes next to the attributes from Active Directory that you want to select, and click **OK**.
- Step 6** Click **Save Configuration**.

What To Do Next

1. See [Chapter 19, “Managing Authentication Policies”](#) for information on how to create authentication policies.
2. See [Chapter 20, “Managing Authorization Policies and Profiles”](#) for information on how to create authorization profiles and policies.

Leaving the Active Directory Domain

If you no longer need to authenticate users or machines from Active Directory, you can leave the Active Directory domain.

When you reset the Cisco ISE application configuration from the command-line interface, it performs a leave operation disconnecting the ISE node from the Active Directory domain, if it is already joined. However, the Cisco ISE node account is not removed from the Active Directory domain. We recommend that you perform a leave operation from the Admin portal with the Active Directory credentials and it removes the node account from the Active Directory domain.

Before You Begin

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 Directory 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.

- Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.
- Step 2** Check the check box next to the Cisco ISE node and click **Leave**.
- Step 3** Enter the Active Directory username and password, and click **OK** to leave the domain and remove the configuration from the Cisco ISE database.
- Step 4** If you do not have the Active Directory credentials, check the **No Credentials Available** check box, and click **OK**.

If you check the **No Credentials Available** check box, the primary Cisco ISE node leaves 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 enter the Active Directory credentials, the Cisco ISE node leaves the Active Directory domain and deletes the configuration from the Active Directory database.



Note The Active Directory credentials that you provide here must have the Create Computer Objects or Delete Computer Objects permission on the computer where the Cisco ISE account was created.

Related Topics

[Deleting Active Directory Configurations, page 14-16](#)

Deleting Active Directory Configurations

You should delete Active Directory configurations if you are not going to use Active Directory as an external identity source. 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.

Before You Begin

Ensure that you have left the Active Directory domain.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.
 - Step 2** Check and ensure that the Local Node status is listed as Not Joined.
 - 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.

Related Topics

[Leaving the Active Directory Domain, page 14-15](#)

Enabling Active Directory Debug Logs

Active Directory debug logs are not logged by default. You must enable this option on the Cisco ISE node that has assumed the Policy Service persona in your deployment from which you want to obtain debug information.

-
- Step 1** Choose **Administration > System > Logging > Debug Log Configuration**.
 - Step 2** Click the radio button next to the Cisco ISE Policy Service node from which you want to obtain Active Directory debug information and click **Edit**.
 - Step 3** Click the **Active Directory** radio button, and click **Edit**.

- Step 4** Choose DEBUG from the drop-down list next to Active Directory.
- Step 5** Click **Save**.

Obtaining Active Directory Log File for Troubleshooting

If you have issues with Active Directory configuration, you can download and view the Active Directory debug logs to troubleshoot your problems.

Before You Begin

You must enable the Active Directory debug log configuration.

- Step 1** Choose **Operations > Troubleshoot > Download Logs**.
- Step 2** Click the node from which you want to obtain the Active Directory debug log file.
- Step 3** Click the **Debug Logs** tab.
- Step 4** Scroll down this page to locate the ad_agent.log file. Click this file to download it.

Related Topics

[Enabling Active Directory Debug Logs, page 14-16](#)

Supplemental Information for Setting Up Cisco ISE with Active Directory

This section provides pointers to help you set up Cisco ISE with Active Directory:

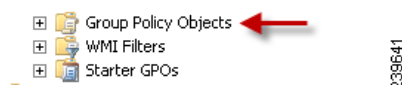
- [Configuring Group Policies in Active Directory, page 14-17](#)
- [Configuring Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory, page 14-18](#)
- [AnyConnect Agent for Machine Authentication, page 14-19](#)

Configuring Group Policies in Active Directory

For more information about how to access the Group Policy management editor, refer to *Microsoft Active Directory Documentation*.

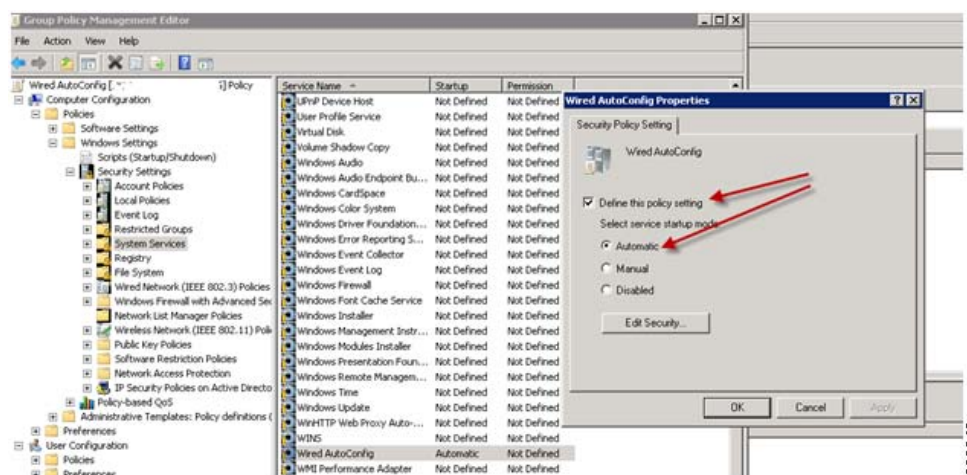
- Step 1** Open the Group Policy management editor as shown in [Figure 14-1](#) and create a new policy object or add to an existing domain policy.

Figure 14-1 Group Policy Objects



- Step 2** Create a new policy and enter a descriptive name for it. For example, you might use Wired Autoconfiguration.
- Step 3** Check the **Define this policy setting** check box, and click the **Automatic** radio button for the service startup mode as shown in Figure 14-2.

Figure 14-2 Policy Properties



- Step 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.

Configuring Odyssey 5.X Suppllicant 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 the supplicant.

- Step 1** Start Odyssey Access Client.
- Step 2** Choose **Odyssey Access Client Administrator** from the Tools menu.
- Step 3** Double-click the **Machine Account** icon.
- Step 4** From the Machine Account page, you must configure a profile for EAP-TLS authentications:
- Choose **Configuration > Profiles**.
 - Enter a name for the EAP-TLS profile.
 - On the Authentication tab, choose **EAP-TLS** as the authentication method.
 - On the Certificate tab, check the **Permit login using my certificate** check box, and choose a certificate for the supplicant machine.
 - On 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 fails.

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.

Cisco ISE integrates with an LDAP external database, which is also called an identity source, by using the LDAP protocol.

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP Directory Service

LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server and sending 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 a directory, which is a database that holds 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.

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

Multiple LDAP Instances

By creating more than one LDAP instance with different IP addresses or port settings, you can configure Cisco ISE to authenticate 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 Cisco ISE LDAP identity source instance.

Cisco 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 and group directory subtree combination for which Cisco ISE submits authentication requests.

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP Failover

Cisco ISE supports failover between a primary LDAP server and a secondary LDAP server. A failover occurs when an authentication request fails because Cisco ISE could not connect to an LDAP server because it is down or is otherwise unreachable.

If you establish failover settings and the first LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE always attempts to contact a second LDAP server. If you want Cisco ISE to use the first LDAP server again, you must enter a value in the Failback Retry Delay text box.



Note

Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies from the Admin portal, so the primary LDAP server must be accessible when you configure these items. Cisco ISE uses the secondary LDAP server only for authentications and authorizations at run time, according to the failover configuration.

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP Connection Management

Cisco 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 open 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.

Cisco ISE retains a list of open LDAP connections (including the binding information) for each LDAP server that is configured in Cisco 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.

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP User Authentication

LDAP can be used as an external database for Cisco ISE user authentication. Cisco ISE supports plain password authentication. User authentication includes:

- 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 a group's membership information for use in policies
- Retrieving values for specified attributes for use in policies and authorization profiles

To authenticate a user, Cisco 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.

We recommend that you protect the connection to the LDAP server using Secure Sockets Layer (SSL).

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP Group and Attribute Retrieval for Use in Authorization Policies

Cisco 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 successful authentication, Cisco 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 Cisco ISE Admin portal by choosing **Administration > Identity Management > External Identity Sources > LDAP**. These groups and attributes can be used by Cisco ISE to authorize the subject.

To authenticate a user or query the LDAP identity source, Cisco ISE connects to the LDAP server and maintains a connection pool.

Related Topics

- [Adding LDAP Identity Sources, page 14-24](#)
- [LDAP Connection Management, page 14-20](#)

LDAP Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco ISE must retrieve 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 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 the attribute that contains 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 stored in the group member attribute (either as DN's or plain usernames).

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP Attributes Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco 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, Cisco 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, Cisco ISE logs a debug message, but the authentication or lookup process does not fail.

You can optionally configure default values for the attributes that Cisco ISE can use when the conversion fails or when Cisco ISE does not retrieve any values for the attributes.

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP Certificate Retrieval

If you have configured certificate retrieval as part of user lookup, then Cisco 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.

Related Topics

[Adding LDAP Identity Sources, page 14-24.](#)

Errors Returned by the LDAP Server

The following errors can occur during the authentication process:

- Authentication Errors—Cisco ISE logs authentication errors in the Cisco ISE log files.

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)
- Initialization Errors—Use the LDAP server timeout settings to configure the number of seconds that Cisco ISE should wait 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.

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

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP User Lookup

Cisco ISE supports the user lookup feature with an 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 a user's group membership information for use in policies
- Retrieving values for specified attributes for use in policies and authorization profiles

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

LDAP MAC Address Lookup

Cisco 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 a MAC Address group information for the device for use in policies
- Retrieving values for specified attributes for use in policies

Related Topics

[Adding LDAP Identity Sources, page 14-24](#)

Adding LDAP Identity Sources

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.
- Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies. Therefore, your primary LDAP server must be reachable when you configure these items.

-
Step 1	Choose Administration > Identity Management > External Identity Sources > LDAP > Add .
Step 2	Enter the values.
Step 3	Click Submit to create an LDAP instance.
-

Related Topics

[LDAP Identity Source Settings, page A-29](#)

What To Do Next

- [Configuring Primary and Secondary LDAP Servers](#), page 14-25
- [Enabling Cisco ISE to Obtain Attributes from the LDAP Server](#), page 14-25
- [Retrieving Group Membership Details from the LDAP Server](#), page 14-26
- [Retrieving User Attributes From the LDAP Server](#), page 14-26

Configuring Primary and Secondary LDAP Servers

After you create an LDAP instance, you must configure the connection settings for the primary LDAP server. Configuring a secondary LDAP server is optional.

-
Step 1	Choose Administration > Identity Management > External Identity Sources > LDAP .
Step 2	Check the check box next to the LDAP instance that you want to edit and click Edit .
Step 3	Click the Connection tab to configure the primary and secondary servers.
Step 4	Enter the values as described in LDAP Connection Settings .
Step 5	Click Submit to save the connection parameters.
-

Related Topics

- [Adding LDAP Identity Sources](#), page 14-24
- [Enabling Cisco ISE to Obtain Attributes from the LDAP Server](#), page 14-25
- [Retrieving Group Membership Details from the LDAP Server](#), page 14-26
- [Retrieving User Attributes From the LDAP Server](#), page 14-26

LDAP Connection Tab Field Settings

The following table describes the fields in **Administration > Identity Management > External Identity Sources > LDAP** Edit page.

Enabling Cisco ISE to Obtain Attributes from the LDAP Server

For Cisco ISE to obtain user and group data from an LDAP server, you must configure LDAP directory details in Cisco ISE. 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 > LDAP .
Step 2	Check the check box next to the LDAP instance that you want to edit and click Edit .
Step 3	Click the Directory Organization tab.
Step 4	Enter the values as described in LDAP Directory Organization Settings .

- Step 5** Click **Submit** to save the configuration.
-

Retrieving Group Membership Details from the LDAP Server

You can add new groups or select groups from the LDAP directory.

- Step 1** Choose **Administration > Identity Management > External Identity Sources > LDAP**.
- Step 2** Check the check box next to the LDAP instance that you want to edit and click **Edit**.
- Step 3** Click the **Groups** tab.
- Step 4** Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to select the groups from the LDAP directory.
- a. If you choose to add a group, enter a name for the new group.
 - b. If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Your search criteria can contain the asterisk (*) wildcard character.
- Step 5** Check the check boxes next to the groups that you want to select and click **OK**.
The groups that you have selected will appear in the Groups page.
- Step 6** Click **Submit** to save the group selection.
-

Retrieving User Attributes From the LDAP Server

You can obtain user attributes from the LDAP server for use in authorization policies.

- Step 1** Choose **Administration > Identity Management > External Identity Sources > LDAP**.
- Step 2** Check the check box next to the LDAP instance that you want to edit and click **Edit**.
- Step 3** Click the **Attributes** tab.
- Step 4** Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to select attributes from the LDAP server.
- a. If you choose to add an attribute, enter a name for the new attribute.
 - b. If you are selecting from the directory, enter an example user and click **Retrieve Attributes** to retrieve the user's attributes. You can use the asterisk (*) wildcard character.
- Step 5** Check the check boxes next to the attributes that you want to select, then click **OK**.
- Step 6** Click **Submit** to save the attribute selections.
-

What To Do Next:

1. See [Chapter 19, “Managing Authentication Policies”](#) for information on how to create authentication policies.
2. See [Chapter 20, “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 a RADIUS server. A 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.

Cisco ISE supports any RADIUS RFC 2865-compliant server as an external identity source. Cisco 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 a user. RADIUS identity sources use the User Datagram Protocol (UDP) port for authentication sessions. The same UDP port is used for all RADIUS communication.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

RADIUS Token Server Supported Authentication Protocols

Cisco ISE supports the following authentication protocols for RADIUS identity sources:

- RADIUS PAP
- Protected Extensible Authentication Protocol (PEAP) with inner Extensible Authentication Protocol-Generic Token Card (EAP-GTC)
- EAP-FAST with inner EAP-GTC

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

Ports Used By the RADIUS Token Servers for Communication

RADIUS token servers use the UDP port for authentication sessions. This port is used for all RADIUS communication. For Cisco ISE to send RADIUS one-time password (OTP) messages to a RADIUS-enabled token server, you must ensure that the gateway devices between Cisco ISE and the RADIUS-enabled token server allow communication over the UDP port. You can configure the UDP port through the Admin portal.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

RADIUS Shared Secret

You must provide a shared secret while configuring RADIUS identity sources in Cisco ISE. This shared secret should be the same as the shared secret that is configured on the RADIUS token server.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

Failover in RADIUS Token Servers

Cisco ISE allows you to configure multiple RADIUS identity sources. Each RADIUS identity source can have primary and secondary RADIUS servers. When Cisco ISE is unable to connect to the primary server, it uses the secondary server.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

Configurable Password Prompt in RADIUS Token Servers

RADIUS identity sources allow you to configure the password prompt. You can configure the password prompt through the Admin portal.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

RADIUS Token Server User Authentication

Cisco ISE obtains the user credentials (username and passcode) and passes them to the RADIUS token server. Cisco ISE also relays the results of the RADIUS token server authentication processing to the user.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

User Attribute Cache in RADIUS Token Servers

RADIUS token servers, by default, do not support user lookups. However, the user lookup functionality is essential for the following Cisco 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.

Cisco 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 Cisco ISE nodes in a distributed deployment. You can configure the Time to Live (TTL) limit for the cache through the Admin portal. 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.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

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. Cisco ISE cannot distinguish among different errors while authenticating with a RADIUS server. RADIUS servers return an Access-Reject message for all errors. 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.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

RADIUS Server Returns the Same Message for All Errors

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. Cisco ISE provides an option to configure this message through the Admin portal as either an Authentication Failed or a User Not Found message. 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 14-3](#) lists the different failure cases that are possible with RADIUS identity servers.

Table 14-3 Error Handling

Failure Cases	Reasons for Failure
Authentication Failed	- User is unknown. - User attempts to log in with an incorrect passcode. - User login hours expired.
Process Failed	- RADIUS server is configured incorrectly in Cisco 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.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

Safeword Server Supports Special Username Format

The Safeword token server supports authentication with the following username format:

Username—Username, OTP

As soon as Cisco 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. Cisco ISE works with various token servers. While configuring a SafeWord server, you must check the SafeWord Server check box in the Admin portal for Cisco 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.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

Authentication Request and Response in RADIUS Token Servers

When Cisco 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)

Cisco 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.

Related Topics

- [Adding a RADIUS Token Server, page 14-31](#)
- [Deleting a RADIUS Token Server, page 14-32](#)

Adding a RADIUS Token Server

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > RADIUS Token > Add**.
- Step 2** Enter the values in the General and Connection tabs.
- Step 3** 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. Cisco ISE accepts 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 4** 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 5** 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 Cisco 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 6 Click **Submit** to save the RADIUS Token identity source.

What To Do Next

1. See [Chapter 19, “Managing Authentication Policies”](#) for information on how to create authentication policies.
2. See [Chapter 20, “Managing Authorization Policies and Profiles”](#) for information on how to create authorization profiles and policies.

Related Topics

[RADIUS Token Identity Sources Settings, page A-32](#)

Deleting a RADIUS Token Server

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.
- 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 fails.

Step 1 Choose **Administration > Identity Management > External Identity Sources > RADIUS Token**.

Step 2 Check the check box next to the RADIUS token server or servers that you want to delete, then click **Delete**.

Step 3 Click **OK** to delete the RADIUS token server or servers that you have selected.

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

Cisco 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.

Cisco 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 Cisco ISE connects with the RSA SecurID authentication technology by using the RSA SecurID Agent.

Cisco ISE Release 1.2 supports only one RSA realm.

This section contains the following topics:

- [Cisco ISE and RSA SecurID Server Integration, page 14-33](#)
- [Configuring RSA Prompts, page 14-37](#)
- [Configuring RSA Messages, page 14-37](#)

Cisco ISE and RSA SecurID Server Integration

These are the two administrative roles involved in connecting Cisco ISE with an RSA SecurID server:

- RSA Server Administrator—Configures and maintains RSA systems and integration
- Cisco ISE Administrator—Configures Cisco ISE to connect to the RSA SecurID server and maintains the configuration

This section describes the processes that are involved in connecting Cisco ISE with the RSA SecurID server as an external identity source. For more information on RSA servers, please refer to the RSA documentation.

RSA Configuration in Cisco 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 Cisco ISE servers as RSA SecurID agents in the realm. You have to browse and add this file to Cisco ISE. By the process of replication, the primary Cisco ISE server distributes this file to all the secondary servers.

RSA Agent Authentication Against the RSA SecurID Server

After the `sdconf.rec` file is installed on all Cisco ISE servers, the RSA agent module initializes, and authentication with RSA-generated credentials proceeds on each of the Cisco ISE servers. After the agent on each of the Cisco 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 Cisco ISE file system and is in a well-known place defined by the RSA agent.

RSA Identity Sources in a Distributed Cisco ISE Environment

Managing RSA identity sources in a distributed Cisco 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.

RSA Server Updates in a Cisco ISE Deployment

After you have added the `sdconf.rec` file in Cisco ISE, the RSA SecurID administrator might 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 Cisco ISE with the updated file. The replication process in Cisco ISE distributes the updated file to the secondary Cisco ISE servers in the deployment. Cisco 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).

Override 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. Cisco ISE servers and RSA SecurID servers operate through the agent module. The agent module that resides on Cisco 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 for each Cisco ISE server for the realm using a text file called `sdopts.rec` through the Admin portal. Refer to the RSA documentation for information on how to create this file.

RSA Node Secret Reset

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 Cisco 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 Cisco ISE server or a group of servers in your deployment (for example, after a key reset on the RSA server). You can use the Cisco ISE Admin portal to delete this file from a Cisco ISE server for the realm. When the RSA agent in Cisco ISE authenticates successfully the next time, it creates a new `securid` file.

**Note**

If authentications fail after upgrading to ISE 1.2, you must reset the RSA secret.

RSA Automatic Availability Reset

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 Cisco 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 recreated. You can use the Admin portal to delete the file from a specific Cisco ISE server for a specific realm. Cisco ISE coordinates with the RSA agent and ensures correct restart phasing.

The availability file `sdstatus.12` is deleted whenever the `securid` file is reset, or the `sdconf.rec` or `sdopts.rec` files are updated.

Related Topics

- [Importing the RSA Configuration File, page 14-35](#)
- [Configuring the Options File for a Cisco ISE Server and Resetting SecurID and `sdstatus.12` Files, page 14-35](#)

- [Adding RSA Identity Sources, page 14-35](#)

Adding RSA Identity Sources

To create an RSA identity source, you must import the RSA configuration file (sdconf.rec). See the [“Importing the RSA Configuration File” section on page 14-35](#) for more information.

Before You Begin

- You must obtain the sdconf.rec file from your RSA administrator.
- To perform the following task, you must be a Super Admin or System Admin.

Adding an RSA identity source involves the following tasks:

- [Importing the RSA Configuration File, page 14-35](#)
- [Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files, page 14-35](#)
- [Configuring Authentication Control Options for RSA Identity Source, page 14-36](#)

Importing the RSA Configuration File

You must import the RSA configuration file to add an RSA identity source in Cisco ISE.

-
Step 1	Choose Administration > Identity Management > External Identity Sources > RSA SecurID > Add .
Step 2	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 3	Enter the server timeout value in seconds. Cisco 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 to 199. The default value is 30 seconds.
Step 4	Check the Reauthenticate on Change PIN check box to force a reauthentication when the PIN is changed.
Step 5	Click Save .
-

Cisco ISE also supports the following scenarios:

- [Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files, page 14-35](#)
- [Configuring Authentication Control Options for RSA Identity Source, page 14-36](#)

Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files

-
Step 1	Log into the Cisco ISE server.
Step 2	Choose Administration > Identity Management > External Identity Sources > RSA SecurID > Add .

Step 3 Click the **RSA Instance Files** tab.

This page lists the sdopts.rec files for all the Cisco ISE servers in your deployment.

Step 4 Click the radio button next to the sdopts.rec file for a particular Cisco ISE server, and click **Update Options File**.

The existing file is displayed in the Current File region.

Step 5 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 6 Click **OK**.

Step 7 Click the row that corresponds to the Cisco ISE server to reset the securid and sdstatus.12 files for that server:

- 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.

- Click **Save** in this row to save the changes.

Step 8 Click **Save**.

Configuring Authentication Control Options for RSA Identity Source

You can specify how Cisco ISE defines authentication failures and 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 Cisco ISE should handle such failures while processing requests and reporting failures. Identity caching enables Cisco ISE to process requests that fail to authenticate against the Cisco ISE server a second time. The results and the attributes retrieved from the previous authentication are available in the cache.

Step 1 Choose **Administration > Identity Management > External Identity Sources > RSA SecurID > Add**.

Step 2 Click the **Authentication Control** tab.

Step 3 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 4 Click **Save** to save the configuration.

What To Do Next

1. See [Chapter 19, “Managing Authentication Policies”](#) for information on how to create authentication policies.
2. See [Chapter 20, “Managing Authorization Policies and Profiles”](#) for information on how to create authorization profiles and policies.

Related Topics

- [RSA Identity Sources, page 14-32](#)
- [Configuring RSA Prompts, page 14-37](#)
- [Configuring RSA Messages, page 14-37](#)

Configuring RSA Prompts

Cisco ISE allows you to configure RSA prompts that are presented to the user while processing requests sent to the RSA SecurID server.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > RSA SecurID**.
- Step 2** Click **Prompts**.
- Step 3** Enter the information as described in [RSA Prompt Settings](#).
- Step 4** Click **Submit**.
-

Related Topics

- [RADIUS Token Identity Sources, page 14-27](#)
- [Adding RSA Identity Sources, page 14-35](#)
- [Configuring RSA Messages, page 14-37](#)

Configuring RSA Messages

Cisco ISE allows you to configure messages that are presented to the user while processing requests sent to the RSA SecurID server.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > RSA SecurID**.
- Step 2** Click **Prompts**.
- Step 3** Click the **Messages** tab.

- Step 4** Enter the information as described in [RSA Message Settings](#).
- Step 5** Click **Submit**.
-

Related Topics

- [RADIUS Token Identity Sources, page 14-27](#)
- [Adding RSA Identity Sources, page 14-35](#)
- [Configuring RSA Prompts, page 14-37](#)

Identity Source Sequences

Identity source sequences define the order in which Cisco ISE looks for user credentials in the different databases. Cisco ISE supports the following identity sources:

- Internal Users
- Guest Users
- Active Directory
- LDAP
- RSA
- RADIUS Token Servers
- Certificate Authentication Profiles

If you have user information in more than one of the databases that are connected to Cisco ISE, you can define the order in which you want Cisco ISE to look for information in these identity sources. Once a match is found, Cisco ISE does not look any further, but evaluates the credentials, and returns the result to the user. This policy is the first match policy.

Related Topics

- [Creating Identity Source Sequences, page 14-38](#)
- [Deleting Identity Source Sequences, page 14-39](#)

Creating Identity Source Sequences

Before You Begin

Ensure that you have configured your external identity sources in Cisco ISE. See the [“Identity Source Sequences” section on page 14-38](#) for information on how to configure external identity sources.

To perform the following task, you must be a Super Admin or System Admin.

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 the Identity Source Sequence for Sponsors” section on page 16-8](#) for more information on how to configure Guest Portal authentication source.

- Step 1** Choose **Administration > Identity Management > Identity Source Sequences > Add**.
- Step 2** Enter a name for the identity source sequence. You can also enter an optional description.

- Step 3** Check the **Select Certificate Authentication Profile** check box and choose a certificate authentication profile, if you wish to use a certificate authentication profile for authentication.
- Step 4** Choose the database or databases that you want to include in the identity source sequence in the Selected List box.
- Step 5** Rearrange the databases in the Selected list in the order in which you want Cisco ISE to search the databases.
- Step 6** Choose one of the following options in the Advanced Search List area:
- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError**—Click this radio button if you want Cisco 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 Cisco ISE to continue searching the other selected identity sources in sequence, if the user is not found in the first selected identity source.
- While processing a request, Cisco ISE searches 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 Cisco ISE to search them.
- Step 7** Click **Submit** to create the identity source sequence that you can then use in policies.
-

Related Topics

- [Configuring a Simple Authentication Policy, page 19-21](#)
- [Configuring a Rule-Based Authentication Policy, page 19-22](#)

Deleting Identity Source Sequences

You can delete identity source sequences that you no longer use in policies.

Before You Begin

- Ensure that the identity source sequence that you are about to delete is not used in any authentication policy.
- To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Administration > Identity Management > Identity Source Sequences**.
- Step 2** Check the check box next to the identity source sequence or sequences that you want to delete, then click **Delete**.
- Step 3** Click **OK** to delete the identity source sequence or sequences.
-

Identity Source Details in Reports

Cisco ISE provides information about the identity sources through the following:

- [Authentications Dashlet, page 14-40](#)

- [Identity Source Reports, page 14-40](#)

Authentications Dashlet

From the Authentications dashlet, you can drill down to find more information including failure reasons.

[Figure 14-3](#) shows the Authentications page and highlights the magnifier icon that you must click to drill down for details.

Figure 14-3 Authentications Page

Cisco

Identity Services Engine

Home
Operations
Policy
Administration

Help
Feedback

Authentications
Reports
Endpoint Protection Service
Troubleshoot

Misconfigured Suppliers
3

Misconfigured Network Devices
4

RADIUS Drops
12

Client Stopped Responding
344

Repeat Counter
262

Show Live Sessions
Add or Remove Columns
Refresh

Refresh
Show
Latest 20 records
within
Last 24 hours

Time	Status	Details	Identity	Repeat Count	Endpoint ID	Network Device	Server	Event	Failure Reason
2013-05-17 13:55:54.979	Failed		dandk	00:25:00:43:0E:AD	WMBU-WLC1	ref-isa-pd01	CTS Peer Policy Download Failed	11512 Extracted EAP-Response/NAK packet requesting to use unsupported EAP protocol; EAP-negotiation failed	
2013-05-17 13:55:50.136	Failed		dandk	00:25:00:43:0E:AD	WMBU-WLC1	ref-isa-pd01	Authentication failed	11512 Extracted EAP-Response/NAK packet requesting to use unsupported EAP protocol; EAP-negotiation failed	

Last update: May 17, 13 03:58:57 866 PM UTC

Help

Records shown: 2

Notifications (0)

For more information on the Authentications page, see the [“Live Authentications” section on page 25-13](#).

Identity Source Reports

Cisco ISE provides various reports that include information about identity sources. See the [“Available Reports” section on page 26-6](#) for a description of these reports.

Related Topics

- [Running and Viewing Reports, page 26-2](#)
- [Exporting Reports, page 26-2](#)



Setting Up and Customizing End-User Web Portals

Cisco ISE allows you to make global customizations that effect the look, feel and behavior of the web pages users see in the Guest, Sponsor, and My Devices portals:

- [Available End-User Portals, page 15-1](#)
- [Specifying Ports and Ethernet Interfaces for End-User Portals, page 15-2](#)
- [Specifying the Fully Qualified Domain Name for Sponsor and My Devices Portals, page 15-3](#)
- [Customizing the Portal Language, Text, and Error Messages, page 15-4](#)
- [Customizing the Web Portal Images and Color Scheme, page 15-5](#)
- [Displaying Banner Messages to Users When Logging In or Out of Portals, page 15-6](#)

Available End-User Portals

Cisco ISE provides web-based portals for three primary sets of end users:

- Guests who need to temporarily access your enterprise network using the Guest portal
- Employees who are designated as sponsors who can create and manage guest accounts using the Sponsor portal.
- Employees who are using their personal devices on the enterprise network using the My Devices portal

Related Topics

- [Chapter 17, “Supporting Personal Devices”](#)
- [Chapter 16, “Supporting Authorized Network Access for Guests”](#)

End-User Portals in Distributed Environment

The end-user portals depend on the Administration, Policy Services, and Monitoring personas to provide configuration, session support, and reporting functionality.

Administration Node

Any configuration changes you make to users or devices on the end-user portals are written to the Administration node. If the primary Administration node fails, you can log into the end-user portals, but you cannot create, edit, or delete users or devices until the primary node comes back up or you promote the secondary node.

Policy Services Node

You must run the end-user portals on a Policy Services node, which handles all session traffic, including: network access, client provisioning, guest services, posture, and profiling. If the Policy Service node is part of a node group, and the node fails, the other nodes detect the failure and reset any pending sessions.

Monitoring Node

The Monitoring node collects, aggregates, and reports data about the end user and device activity on the My Devices, Sponsor, and Guest portals. If the primary Monitoring node fails, the secondary Monitoring node automatically becomes the primary Monitoring node.

Related Topics

- [Administration Node, page 3-2](#)
- [Policy Service Node, page 3-3](#)
- [Monitoring Node, page 3-5](#)
- [Enabling Policy Services for End-User Portals, page 15-2](#)
- [Registered Endpoints Report, page 17-7](#)
- [Monitoring Sponsor and Guest Activity, page 16-23](#)

Enabling Policy Services for End-User Portals

To support the end-user portals, you must enable portal-policy services on the node on which you want to host them.

-
Step 1	Choose Administration > System > Deployment .
Step 2	Click the node and click Edit .
Step 3	On the General Settings tab, check Policy Service .
Step 4	Check the Enable Session Services option.
Step 5	Click Save .
-

Specifying Ports and Ethernet Interfaces for End-User Portals

You can specify the port used for each web portal allowing you to use different ports for the end-user portals: Sponsor, Guest (and Client Provisioning), My Devices, and Blacklist portals. The Client Provisioning portal uses ports 8905 and 8909 for posture assessments and remediation, which you cannot change. Otherwise, it uses the same ports assigned to the Guest portal.

You can also partition portal traffic to specific Gigabit Ethernet interfaces. For example, you might not want the Admin portal (which always uses GigabitEthernet 0) available on the same network as guest users or employee devices.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > General > Ports**.
- Step 2** Enter the port value in the **HTTPS Port field** for each portal. By default, the Sponsor, Guest, My Devices portals use 8443, and the Blacklist portal uses port 8444.
- Step 3** Check the Gigabit Ethernet interfaces you want to enable for each portal.
- Step 4** Click **Save**.

If you have changed the port settings, all nodes (Administration, Policy Services, and Monitoring) restart automatically, which may take several hours to complete.

Related Topics

- [Tips for Assigning Ports and Ethernet Interfaces, page 15-3](#)
- [Ports Used by the Admin Portal, page 5-3](#)
- [Port Settings for Web Portals, page A-50](#)
- [Configuring Client Provisioning, page 22-1](#)

Tips for Assigning Ports and Ethernet Interfaces

Refer to these guidelines to help you decide how best to assign ports and Ethernet interfaces to the end-user portals:

- All port assignments must be between 8000-8999. This port range restriction is new in Cisco ISE 1.2. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction.
- You must assign the Blacklist portal to use a different port than the other end-user portals.
- Any portals assigned to the same HTTPS port also use the same Ethernet interfaces. For example, if you assign both the Sponsor and My Devices portals to port 8443, and you disable GigabitEthernet 0 on the Sponsor portal, that interface is also automatically disabled for the My Devices portal.
- You must configure the Ethernet interfaces using IP addresses on different subnets.

Specifying the Fully Qualified Domain Name for Sponsor and My Devices Portals

You can set the Sponsor and My Devices portals to use an easy-to-remember fully-qualified domain names (FQDN), such as: mydevices.companyname.com or sponsor.companyname.com. Alternatively, Cisco ISE also supports wildcard certificates to address certificate name mismatch issues.

You must configure DNS to resolve to at least one policy services node. If you have more than one policy services node that will provide portal services, you should configure high availability for the portal. For example, you could use a load balancer or DNS round-robin services.

Before You Begin

You must also update DNS to ensure the FQDN of the new URL resolves to a valid policy service node IP address. Additionally, to avoid certificate warning messages due to name mismatches, you should also include the FQDN of the customized URL in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE policy service node.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > General > Ports**.
- Step 2** Scroll to the Portal FQDNs section, and check the appropriate setting:
- Default Sponsor Portal FQDN
 - Default My Devices Portal FQDN
- Step 3** Enter a fully qualified domain name.
- Step 4** Click **Save**, and all nodes (Administration, Policy Services, and Monitoring) restart automatically, which may take several hours to complete.
- Step 5** Configure the network DNS server so that it resolves the FQDN to the Sponsor or My Devices portal nodes.
-

Related Topics

- [Port Settings for Web Portals, page A-50](#)
- [Wildcard Certificates, page 8-4](#)

Customizing the Portal Language, Text, and Error Messages

The Sponsor, Guest, and My Devices portals can be set to display in any of the languages supported by Cisco ISE. If you need to support additional languages, you can create custom templates.

You can further customize the language display for each portal by modifying the UI text and error messages used by each portal.

Related Topics

[Cisco ISE Internationalization and Localization, page 2-10](#)

Adding a Custom Language Template

If you want to support any additional languages, you can create a custom language template. Each language template must use a unique browser locale mapping.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest, Sponsor, or My Devices > Language Template**.
- Step 2** Click **Add** to create a new language template.
- Step 3** Enter a unique **Name** and **Description** for the language template, followed by a valid **Browser Locale Mapping**.
- Step 4** Update the text strings in each section with localized content.

Step 5 Click **Save**.

Related Topics

- [My Devices Portal Language Template Settings, page A-53](#)
- [Guest Portal Language Template Settings, page A-55](#)
- [Sponsor Language Template Settings, page A-52](#)

Customizing Portal UI Fields and Error Messages

You can fully customize the text and error messages used by the Guest, Sponsor, and My Devices portals. The Guest portal customizations also include the fields used by the Self-Provisioning portal and the Mobile Device Management (MDM) enrollment and compliance pages.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest, Sponsor, or My Devices > Language Template**.
- Step 2** Choose one of the languages from the list.
- Step 3** Update the text strings in each section with localized content.
- Step 4** Click **Save**.
-

Related Topics

- [My Devices Portal Language Template Settings, page A-53](#)
- [Guest Portal Language Template Settings, page A-55](#)
- [Sponsor Language Template Settings, page A-52](#)

Customizing the Web Portal Images and Color Scheme

You can customize the look-and-feel of the end-user portals by uploading your company's logos, background images, or color schemes. These changes apply to the My Devices, Sponsor, and Guest portals, but you can assign different images and colors to the mobile Guest portal.

These settings allow you to change the appearance of the portals without having to upload customized HTML files to the Cisco ISE server. However, if you want to create themes unique to specific Guest portals, you must upload your custom HTML files instead.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > General > Portal Theme**.
- Step 2** Upload the graphics and change the color settings in the **Style Settings** section to customize the standard portals.
- Step 3** Upload the graphics and change the color settings in the **Mobile Device Style Settings** to customize the Guest mobile portal.
- Step 4** Click **Save**.
-

Related Topics

- [General Portal Theme Settings, page A-49](#)
- [Customized Guest Portal, page 16-12](#)

Displaying Banner Messages to Users When Logging In or Out of Portals

You can display messages to users when they log into one of the end-user portals. The pre-login banner displays on the login page for each portal. The post-login banner displays briefly for about 15 seconds on the bottom right side of the Sponsor and My Devices portals, and it does not apply to the Guest portal. You can customize the displayed text for each portal individually.

Enabling Banner Messages

If you want to display messages to users before or after they log into one of the end-user portals, you need to enable them. This option enables the setting on each portal, but you can then customize the displayed text specifically for each portal.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > General > Portal Theme**.
- Step 2** Check the **Display pre-login banner** and **Display post-login banner** options enable the banners.
-

Related Topics

- [General Portal Theme Settings, page A-49](#)
- [Customizing the Sponsor Portal Banner Messages, page 15-6](#)
- [Customizing the My Devices Portal Banner Messages, page 15-7](#)
- [Customizing the Guest Portal Login Banner Message, page 15-7](#)

Customizing the Sponsor Portal Banner Messages

You can customize the text that displays to sponsor users before and after logging into the Sponsor portal.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Sponsor > Language Template**.
- Step 2** Click the language, such as English.
- Step 3** Click **Configure Common Items** and update the **Pre-Login Banner Text** and **Post-Login Banner Text** fields.
- Step 4** Click **Save**.
-

Related Topics

- [General Portal Theme Settings, page A-49](#)
- [Enabling Banner Messages, page 15-6](#)

Customizing the My Devices Portal Banner Messages

You can customize the text that displays to employees before and after logging into the My Devices portal.

-
Step 1	Choose Administration > Web Portal Management > Settings > My Devices > Language Template .
Step 2	Click the language, such as English.
Step 3	Click Configure Login Page and update the Pre-Login Banner Text and Post-Login Banner Text fields.
Step 4	Click Save .
-

Related Topics

- [General Portal Theme Settings, page A-49](#)
- [Enabling Banner Messages, page 15-6](#)

Customizing the Guest Portal Login Banner Message

You can customize the text that displays to guests before logging into the Guest portal.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Language Template .
Step 2	Click the language, such as English.
Step 3	Click Configure Login Page and update the Pre-Login Banner Text fields.
Step 4	Click Save .
-

Related Topics

- [General Portal Theme Settings, page A-49](#)
- [Enabling Banner Messages, page 15-6](#)



Supporting Authorized Network Access for Guests

This chapter provides information on managing network user access, sponsor accounts, and how to create the necessary policies for these network users.

This chapter contains the following sections:

- [Cisco ISE Guest Services, page 16-1](#)
- [Guest Services End-User Portals, page 16-1](#)
- [Managing Sponsor and Guest Accounts, page 16-3](#)
- [Configuring the Sponsor Portal, page 16-8](#)
- [Configuring the Guest Portal, page 16-10](#)
- [Monitoring Sponsor and Guest Activity, page 16-23](#)
- [Guest Deployment Scenarios, page 16-26](#)

Cisco ISE Guest Services

Cisco Identity Services Engine (ISE) guest services enables you to provide secure network access to guests, visitors, contractors, consultants, and customers. You can support guest users with both base and advanced Cisco ISE licenses, and you can choose from several deployment options depending on your company's infrastructure and feature requirements.

Related Topics

- [Guest Deployment Scenarios, page 16-26](#)
- [Chapter 7, "Cisco ISE Licenses"](#)

Guest Services End-User Portals

Cisco ISE provides web-based portals to manage guest access to the network.

Sponsor Portal

The Sponsor portal is one of the primary components of Cisco ISE guest services. Using the Sponsor portal, sponsors can create and manage temporary accounts for authorized visitors to securely access the corporate network or the Internet. After creating an account, sponsors also can use the Sponsor portal to provide account details to the guest by printing, emailing, or texting.

Related Topics

- [Chapter 15, “Setting Up and Customizing End-User Web Portals”](#)
- [Configuring the Sponsor Portal, page 16-8](#)

Guest Portal

When people outside your company attempt to use your company's network to access the Internet, they are routed to the Guest portal. You can use the Guest portal to identify and authorize temporary access to internal networks and services to external users. Sponsors can create temporary usernames and passwords for authorized visitors who can then access the network by entering these credentials in the Guest portal login page.

Cisco ISE enables you to create multiple Guest portals, which you can use to allow guest access based on different criteria. For example, you might have a Guest portal for monthly contractors that is separate from the portal used for daily visitors. You also have the option to route mobile users to a mobile-optimized version of the Guest portal.

Related Topics

- [Guest Deployment Scenarios, page 16-26](#)
- [Configuring the Guest Portal, page 16-10](#)

Support for Multiple Guest Portals

Cisco ISE provides you with the ability to host multiple portals on the Cisco ISE server, including a predefined DefaultGuestPortal. The default portal themes have standard Cisco branding that you can customize through the Admin portal. You can also choose to customize a portal by uploading HTML pages that are specific to your organization.

Related Topics

- [Configuring the Guest Portal, page 16-10](#)

Mobile Guest Portal

Cisco ISE enables you to deliver a mobile-optimized version of the Guest portal, which provides an improved user experience for guests accessing your network using their mobile devices. Because this is an optional feature, you must enable it when you create the Guest portal.

Related Topics

- [Providing a Mobile-Optimized Guest Portal, page 16-11](#)

Device Registration Web Authentication Portal

The Device Registration Web Authentication (DRW) portal is an alternative Guest portal that does not require guests to enter usernames and passwords. Instead, Cisco ISE works together with the wireless LAN controller (WLC) to grant network access directly to the guest's device.

If you support the DRW portal, Cisco ISE provides you with a default guest identity group, GuestEndpoints, which enables you to cohesively track guest devices.

Related Topics

- [Device Registration WebAuth, page 16-30](#)

Client Provisioning Portal

The Client Provisioning portal provides posture assessments and remediations for guest users. When guests request network access, you can route them to the Client Provisioning portal and require them to first download the client provisioning agent.

The Client Provisioning portal is available only with a Central WebAuth (CWA) guest deployment. If you select this option, the guest login flow performs a CWA and the Guest portal will be redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) to the network access device to reauthenticate the client connection once the posture has been assessed.

Related Topics

- [NAD with Central WebAuth Process Flow, page 16-26](#)
- [Configuring Client Provisioning, page 22-1](#)

Managing Sponsor and Guest Accounts

Guest services require two special types of users—guests and sponsors. From the Admin portal, you must define the access privileges and feature support for sponsors. Sponsors then access the Sponsor portal to create and manage guest accounts.

Guest Accounts

Guests typically represent authorized visitors, contractors, customers, or other temporary users who require access to your network. However, you can also use guest accounts for employees if you prefer to use one of the guest deployment scenarios to allow employees to access the network. Only sponsors can create guest users, and you must access the Sponsor portal to view a list of guest users.

Guest Role and Identity Groups

The guest identity group is defined by the guest role. When sponsors create a guest account, they must associate the account with a guest role. Guest roles allow a sponsor to assign different levels of access to a guest account. These guest roles are associated with particular network access policies. For example, Cisco ISE includes these default guest roles:

- **Guest:** Users must first sign into through the Guest captive portal before they will be able to access other parts of the network (such as with Central Web Authentication (CWA)).
- **ActivatedGuest:** Users can bypass the Guest portal and access the network by providing credentials to the native supplicant on their device (such as with IEEE 802.1X (dot1x) authentication.)

You can also create additional user identity groups specific to your organization to use with sponsor accounts (**Administration > Identity Management > Groups > User Identity Groups.**)

Related Topics

[Creating a User Identity Group, page 14-5](#)

Configuring Guest Roles

When you create new identity groups to use as guest roles, you must indicate which of the default behaviors to apply to them: Guest or Activated Guest.

Before You Begin

Create a new user identity group to use for guests.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Guest Roles Configuration.**
- Step 2** Select the identity group you created.
- Step 3** Click > or < to assign the identity group to one of the following groups:
- **Guest:** Users must first sign into through the Guest captive portal before they will be able to access other parts of the network (such as with Central Web Authentication (CWA)).
 - **ActivatedGuest:** Users can bypass the Guest portal and access the network by providing credentials to the native supplicant on their device (such as with IEEE 802.1X (dot1x) authentication.)
- Step 4** Click **Save.**
-

What to Do Next

Create or modify sponsor groups to use this guest role.

Related Topics

- [Creating a User Identity Group, page 14-5](#)
- [Creating Sponsor Groups, page 16-5](#)

Sponsor Accounts and Identity Groups

Sponsors are a special type of internal user who can create guest accounts using the Sponsor portal. Like other internal users, Cisco ISE authenticates sponsors through a local database, or through external Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory identity stores. If you are not using an external source, you must create user accounts in Cisco ISE (**Administration > Identity Management > Identities > Users.**)

You must then assign users to the appropriate sponsor identity group. The sponsor identity groups specify the users who can use the Sponsor portal, and they are mapped in the default to the default sponsor groups in the sponsor group policies.

Cisco ISE includes these default sponsor user identity groups:

- SponsorAllAccount
- SponsorGroupAccounts
- SponsorOwnAccounts

You can also create additional user identity groups specific to your organization to use with sponsor accounts (**Administration > Identity Management > Groups > User Identity Groups**).

Related Topics

[Adding Users, page 14-3](#)

[Creating a User Identity Group, page 14-5](#)

Sponsor Groups

The sponsor group configuration defines the permissions and settings for sponsor users. The policies map user identity groups to sponsor groups.

Cisco ISE includes these default sponsor groups:

- SponsorAllAccounts—Sponsors who can manage all guest accounts in your Cisco ISE network.
- SponsorGroupGrpAccounts—Sponsors who can manage only guest accounts created by sponsor users from the same sponsor group.
- SponsorGroupOwnAccounts—Sponsors who can manage only the guest accounts that they have created.

These sponsor groups have names similar to the default user identity groups to assist you in associating the correct identity group and sponsor group when creating the sponsor policies.

You can customize the features available to particular sponsor groups thereby limiting or expanding functionality of the Sponsor portal. For example:

- You can restrict sponsors from viewing guest accounts created by other sponsors.
- You can restrict access to different functions, such as creating accounts, modifying accounts, and sending account details to guests by e-mail or SMS text messages.
- You can set the sponsor group permission to prevent a group of sponsors from logging in for a short period of time while some configuration is being changed.

Related Topics

- [Creating Sponsor Groups, page 16-5](#)
- [Creating a Sponsor Group Policy, page 16-6](#)
- [Sponsor Group Settings, page A-47](#)

Creating Sponsor Groups

You can create additional sponsor groups in addition to the default sponsor groups provided by Cisco ISE.

-
- Step 1** Choose **Administration > Web Portal Management > Sponsor Groups**.
- Step 2** Click **Add**.
- Step 3** Update the fields on each of these tabs:
- **General**—provide the name and description for the new sponsor group
 - **Authorization Levels**—identify the features available to sponsors in this group, such as: creating accounts, sending notifications, and suspending accounts.
 - **Guest Roles**—choose the guest roles to which the sponsor can assign the guest user.
 - **Time Profiles**—choose the time profiles for which the sponsor can set on the guest accounts.
- Step 4** Click **Submit**.
-

Related Topics

- [Sponsor Groups, page 16-5](#)
- [Sponsor Group Settings, page A-47](#)

Sponsor Group Policies

Sponsor group policies associate user identity groups with sponsor groups. Each sponsor group policy contains at least one identity group, and it can also contain other attribute conditions with which you define the sponsor group. You can map internal users or users from an external identity store (such as LDAP or Active Directory) to sponsor groups.

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 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 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.

Creating a Sponsor Group Policy

The sponsor group policy specifies the conditions that determine access and functionality available to a sponsor when logging into the Sponsor portal.

The sponsor group policy comprises:

- one or more identity groups
- one or more attributes or conditions

Before You Begin

You can apply existing conditions to your Sponsor Group Policies. If needed, define additional conditions, before creating your policies.

-
- Step 1** Choose **Administration > Web Portal Management > Sponsor Group Policy**.

- Step 2** Click the Action icon and choose an option.
- Step 3** Enter a name for the new policy.
- Step 4** Choose the identity group to be associated with the policy.
- Step 5** (Optional) Choose additional conditions by choosing one of these options:
- **Select Existing Condition from Library** to choose an existing simple, compound, or time and date condition
 - **Create New Condition** to choose an attribute, operator, and value from the expression builder.
- Step 6** Choose the sponsor group to associate with this sponsor group policy.
- Step 7** Click **Save**.
-

Related Topics

- [Creating Simple Conditions, page 18-2](#)
- [Creating Compound Conditions, page 18-3](#)
- [Adding Users, page 14-3](#)
- [Creating Sponsor Groups, page 16-5](#)

Mapping Active Directory Groups to Sponsor Groups

You can map external identity groups to sponsor groups.

Before You Begin

Before beginning this task, you must configure the Active Directory identity groups.

-
- Step 1** Choose **Administration > Web Portal Management > Sponsor Group Policy**.
- Step 2** Click the Action icon and choose an option.
- Step 3** Enter a name for the new policy.
- Step 4** Choose **Any** as the Identity Group because there is no group mapping with the internal groups.
- Step 5** Choose the condition you created for the Active Directory identity store
- Step 6** Choose the sponsor group to associate with this AD condition.
- Step 7** Click **Save**.
-

Related Topics

- [Active Directory as an External Identity Source, page 14-9](#)
- [Configuring Active Directory User Groups, page 14-14](#)

Configuring the Sponsor Portal

You must configure some settings for the Sponsor portal before sponsors can access it to create accounts for guest users.

Sponsor Identity Source Sequence

Sponsor identity source sequences are used with the login credentials of the sponsor to authenticate and authorize sponsors for access to the Sponsor portal. The identity source sequence defines which stores should be accessed and in what order they should be accessed to resolve the authentication of a sponsor user, and it can include the local Cisco ISE identity stores and external stores.

Cisco ISE includes a default sponsor identity source sequence (Sponsor_Portal_Sequence), which includes the default identity store, Internal Users.

Related Topics

- [Specifying the Identity Source Sequence for Sponsors, page 16-8](#)
- [Creating Identity Source Sequences, page 14-38](#)

Specifying the Identity Source Sequence for Sponsors

To allow a sponsor user to log into the Sponsor portal, you must choose an identity source sequence to be used for all sponsor accounts. This sequence is used with the login credentials of the sponsor to authenticate and authorize the sponsor for access to the Sponsor portal.

Before You Begin

Create the identity source sequence. Or, you can use the Sponsor_Portal_Sequence, which is the default sequence included with Cisco ISE.

-
Step 1	Choose Administration > Web Portal Management > Settings > Sponsor > Authentication Source .
Step 2	Choose the identity source sequence from the Identity Store Sequence drop-down list.
Step 3	Click Save .
-

Related Topics

- [Sponsor Identity Source Sequence, page 16-8](#)
 - [Identity Source Sequences, page 14-38](#)
 - [Creating Identity Source Sequences, page 14-38](#)
-

Customizing Guest Notifications

When sponsors create guest accounts, they can provide the account credentials to guest users by printing, emailing, or texting the details. When you create sponsor groups, you determine whether to authorize sponsors to use these notifications.

Customizing E-mail Notifications

You can specify the subject and the body of the e-mail that will be sent to guests with their account details.

Before You Begin

Configure the SMTP server to enable notifications and configure the sponsor groups to support the email notification.

-
Step 1	Choose Administration > Web Portal Management > Settings > Sponsor > Language Template .
Step 2	Click the language for which you want to apply the policy, for example, English.
Step 3	Click Configure Email Notification .
Step 4	Enter the subject of the e-mail in the Subject field.
Step 5	Enter the e-mail body in the Layout field using HTML tags for formatting.
Step 6	Click Save .
-

Related Topics

- [Configuring the SMTP Server to Support Notifications, page 5-5](#)
- [Creating Sponsor Groups, page 16-5](#)
- [E-Mail Notification Template, page D-1](#)

Customizing SMS Text Message Notifications

You can specify the short message service (SMS) gateway, the subject and the message of the SMS text message that will be sent to guests with their account details.

Before You Begin

- Configure the SMTP server, which is used to send e-mail to the SMS gateway to deliver the SMS text message.
- Configure the sponsor groups to support the SMS text notification.
- You must have an account with a third-party SMS gateway. Cisco ISE sends the text messages as e-mail messages to the gateway, which are then forwarded through SMS to the specified user.

-
Step 1	Choose Administration > Web Portal Management > Settings > Sponsor > Language Template .
Step 2	Click the language for which you want to apply the policy.
Step 3	Click Configure SMS Text Message Notification .
Step 4	Enter the subject of the text message in the Subject field.

- Step 5** Enter the address of a third-party SMS gateway in the **Destination** field.
- Step 6** Enter the text body in the **Layout** field using HTML tags for formatting.
- Step 7** Click **Save**.
-

Related Topics

- [Configuring the SMTP Server to Support Notifications, page 5-5](#)
- [Creating Sponsor Groups, page 16-5](#)
- [SMS Text Message Notification Template, page D-2](#)

Customizing Print Notifications

You can specify the page header and the body of the page that will be printed for guests with their account details.

Before You Begin

Configure the sponsor groups to support the print notification.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Sponsor > Language Template**.
- Step 2** Click the language for which you want to apply the policy, for example, English.
- Step 3** Click **Configure Print Notification**.
- Step 4** Enter a title in the **Page Header** field.
- Step 5** Enter the body of the printout in the **Layout** field using HTML tags for formatting.
- Step 6** Click **Save**.
-

Related Topics

- [Creating Sponsor Groups, page 16-5](#)
- [Print Notification Template, page D-3](#)

Configuring the Guest Portal

You must configure settings for the Guest portal before allowing guests to use it to access the network. Some settings apply globally to all Guest portals and other require you to set them for each portal individually.

Adding a New Guest Portal

You can add a new Guest portal or edit an existing one.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations**.
- Step 2** Click **Add**.
- Step 3** Update the fields on each of these tabs:
- **General**—enter a portal name and description and choose a portal type.
 - **Operations**—enable the customizations for the specific portal
 - **Customization**—choose a language template for displaying the Guest portal with localized content
 - **File Uploads**—displays only if you have chosen a portal type requiring you to upload custom HTML files.
 - **File Mapping**— identify and choose the HTML files uploaded for the particular guest pages. Displays only if you have chosen a portal type requiring you to upload custom HTML files.
 - **Authentication**—indicate how users should be authenticated during guest login.
- Step 4** Click **Submit**.
-

Related Topics

- [Multi-Portal Configuration Settings, page A-56](#)
- [Cisco ISE Authentication Policies, page 19-1](#)
- [Configuring a Simple Authentication Policy, page 19-21](#)
- [Configuring a Rule-Based Authentication Policy, page 19-22](#)

Providing a Mobile-Optimized Guest Portal

You can allow mobile users to access a mobile-optimized version of the Guest portal.

Before You Begin

Create a Guest portal or modify the DefaultGuestPortal. This setting is specific to each Guest portal.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration**.
- Step 2** Check the Guest portal to update and click **Edit**.
- Step 3** Click the **Operations** tab.
- Step 4** Check **Enable Mobile Portal**.
- Step 5** Click **Save**.
-

Related Topics

- [Adding a New Guest Portal, page 16-10](#)
- [Multi-Portal Configuration Settings, page A-56](#)
- [Customizing the Web Portal Images and Color Scheme, page 15-5](#)

Customized Guest Portal

You have two options available for customizing the Guest portal:

- Apply the same custom color schemes, banners, and logos to all Guest, Sponsor, and My Devices portals by choosing **Administration > Web Portal Management > Settings > General > Portal Theme**. (See [“Customizing the Web Portal Images and Color Scheme”](#) section on page 15-5 for details.)
- Create custom HTML pages for complete control over the Guest portal look and feel.

When you create custom HTML files, these changes apply only to the Guest portal. The other portals use the settings defined in the portal theme. To better synchronize the look and feel amongst the portals, upload your custom logos and banners to the portal theme too.

Related Topics

- [Sample HTML for Custom Pages for the Guest Portal, page D-3](#)
- [Creating Custom HTML Files for Guest Portal, page 16-13](#)
- [Uploading HTML Files for Guest Portal, page 16-14](#)
- [Mapping HTML Files to Guest Portal Pages, page 16-15](#)

HTML Pages Required for Custom Guest Portals

To support a fully-customized guest portal, you must provide a minimum set of HTML pages based on the features you want to support:

- Login Page—Required
- Successful Guest Login Page—Required
- Error Page—Required
- Acceptable Use Policy Page—Required only if you require guests to acknowledge an acceptable use policy.
- Change Password Page—Required only if you require guests to change their passwords when signing in for the first time.
- Self-Registration Page—Required only if you allow guests to create their own accounts (self service).
- Self-Registration Result Page—Required only if you allow guests to create their own accounts (self service).
- Device Registration Page—Required if you are supporting device registration for guest users.

Related Topics

- [Requiring Guests to Change Password, page 16-17](#)
- [Requiring an Acceptable Use Policy for Guests, page 16-19](#)
- [Allowing Guests to Add Devices, page 16-22](#)
- [Allowing Guests to Create Accounts, page 16-22](#)

Sequence of Customized HTML Pages Used by Guest Portal

The sequence and display of the customized HTML pages depends on the features you have enabled in the Cisco ISE Admin. Some example sequences include:

- Basic sequences
 - Login Page (required) > Successful Guest Login Page (required)
 - Login Page (required) > Change Password Page > Successful Guest Login Page (required)
- Device registration sequences
 - Login Page (required) > Device Registration Page > Successful Guest Login Page (required)
 - Login Page (required) > Change Password Page > Device Registration Page > Successful Guest Login Page (required)
- Acceptable use policy sequences
 - Login Page (required) > Acceptable Use Policy Page > Successful Guest Login Page (required)
 - Login Page (required) > Acceptable Use Policy Page > Change Password Page > Successful Guest Login Page (required)
 - Login Page (required) > Acceptable Use Policy Page > Change Password Page > Device Registration Page > Successful Guest Login Page (required)
- Self-registration sequences
 - Login Page (required) > Self-Registration Page > Self-Registration Result Page > Successful Guest Login Page (required)

Related Topics

- [Requiring Guests to Change Password, page 16-17](#)
- [Requiring an Acceptable Use Policy for Guests, page 16-19](#)
- [Allowing Guests to Add Devices, page 16-22](#)
- [Allowing Guests to Create Accounts, page 16-22](#)

Creating Custom HTML Files for Guest Portal

You must manually code the custom HTML pages to use for the Guest portal. When you use your own HTML pages, the details policy, language templates, and portal themes do not apply. So, if these features are important to you, you need to write the HTML code to deliver similar functionality, or use the standard portal theme pages instead.

Before You Begin

Familiarize yourself with the Cisco-provided HTML pages (see the [“Sample HTML for Custom Pages for the Guest Portal” section on page D-3.](#)) At a minimum, you must create the Login, Guest Success, and Error Page files.

-
- Step 1** Open an HTML or text editing application.
 - Step 2** Enter your custom HTML code using the Cisco-provided sample HTML pages as a reference.
 - Step 3** Create and save a separate HTML file for each page:
 - Login Page (required)

- Successful Guest Login Page (required)
 - Error Page (required)
 - Acceptable Use Policy Page
 - Change Password Page
 - Self-Registration Page
 - Self-Registration Result Page
 - Device Registration Page
-

What to Do Next

After creating the HTML pages, you must upload them to Cisco ISE and map them to the appropriate Guest portal pages.

Related Topics

- [Sample HTML for Custom Pages for the Guest Portal, page D-3](#)
- [Uploading HTML Files for Guest Portal, page 16-14](#)
- [Mapping HTML Files to Guest Portal Pages, page 16-15](#)

Uploading HTML Files for Guest Portal

Upload the HTML files to fully customize the Guest portal.

Before You Begin

You must create the custom HTML files.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations .
Step 2	Choose one of these portal types: • Custom Default Portal • Custom Device Web Authorization Portal
Step 3	Click the File Uploads tab.
Step 4	Click Update File to select and upload each HTML file.
Step 5	Click Submit .
-

Related Topics

- [Sample HTML for Custom Pages for the Guest Portal, page D-3](#)
- [Creating Custom HTML Files for Guest Portal, page 16-13](#)
- [Mapping HTML Files to Guest Portal Pages, page 16-15](#)

Mapping HTML Files to Guest Portal Pages

After uploading the custom HTML files, you must map them to the appropriate page in the Guest portal.

Before You Begin

You must create and upload the custom HTML files.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations .
Step 2	Choose one of these portal types: • Custom Default Portal • Custom Device Web Authorization Portal
Step 3	Click the File Mapping tab.
Step 4	Click the drop-down menus to assign the uploaded HTML page to the appropriate file.
Step 5	Click Submit .
-

- [Sample HTML for Custom Pages for the Guest Portal, page D-3](#)
- [Creating Custom HTML Files for Guest Portal, page 16-13](#)
- [Uploading HTML Files for Guest Portal, page 16-14](#)

Configuring the Guest Username and Password Policies

You must set username and password policies for guest accounts.

Configuring the Guest Username Policy Based on Names or E-mail Accounts

You can create a guest username based on the e-mail address or the first and last name of the guest. This is a global setting affecting all Guest portals, but changes do not affect the existing accounts.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Username Policy .
Step 2	Choose one of these options: • Create username from email address • Create username from the first name and last name
Step 3	Enter the Minimum Username length for the guest usernames. The valid range is 1-20.
Step 4	Click Save .
-

Related Topics

- [Guest Username Policy Settings, page A-61](#)

Configuring the Username Policy for Random Guest Accounts

You can create a guest username based upon a random mixture of alphabetic, numeric or special characters. The random guest username policy is used when the sponsor creates random accounts. This is a global setting affecting all Guest portals, but changes do not affect the existing accounts.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Username Policy**.
- Step 2** Enter the characters that will be used to generate the random usernames.
- Step 3** Enter the minimum number to use from each set of characters.
- Step 4** Click **Save**.
-

Related Topics

- [Guest Username Policy Settings, page A-61](#)

Configuring the 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.

This is a global setting affecting all Guest portals. However, changes to the guest password policy do not affect the existing accounts until the guest user passwords have expired and need to be changed.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Password Policy**.
- Step 2** Enter the allowable alphabetic, numeric, and special characters.
- Step 3** Enter the minimum number to use from each set of characters.
- Step 4** Click **Save**.
-

Setting the Guest Password Expiration Time

You can set the number of days after which the guest password will expire, requiring the guest to reset their password. This is a global setting affecting all Guest portals.

Before You Begin

To use this option, you must also set the option requiring guests to change their passwords at expiration.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy**.
- Step 2** Enter the number of days in the **Guest Password Expiration** field.
- Step 3** Click **Save**.
-

Related Topics

- [Requiring Guests to Change Password, page 16-17](#)

- [Guest Portal Policy Settings, page A-59](#)

Requiring Guests to Change Password

You can allow or require guest users to change their password after their initial account credentials are created by the sponsor. If guest users change their passwords, sponsors cannot provide guests with their login credentials if they are lost. The sponsor must create a new guest account.

You can either allow guests to change their passwords, or you can require that they do it at expiration and at first login.

Before You Begin

Create a Guest portal or modify the DefaultGuestPortal. This setting is specific to each Guest portal.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration .
Step 2	Check the Guest portal to update and click Edit .
Step 3	Click the Operations tab.
Step 4	Check either or both options: • Allow guest users to change password • Require guest users to change password at expiration and first login
Step 5	Click Save .
-

Related Topics

- [Adding a New Guest Portal, page 16-10](#)
- [Multi-Portal Configuration Settings, page A-56](#)

Specifying the Maximum Failed Login Attempts

You can set the maximum number of failed login that can occur before a guest account is suspended, requiring the sponsor to reinstate the account. This is a global setting affecting all Guest portals.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Portal Policy .
Step 2	Enter the value in the Maximum Login Failures field.
Step 3	Click Save .
-

Related Topics

[Guest Portal Policy Settings, page A-59](#)

Defining Guest Features

You can specify required information and allowable parameters for the Guest portals.

Specifying the Required Data for Guest Accounts

The details policy specifies the data required to create a guest account. You must define the fields that appear when sponsors create a new guest account or when guests register themselves, such as: name, company, email, and phone. This is a global setting affecting all Guest portals.

Before You Begin

If you create custom portals by uploading your own HTML pages, the details policy does not apply to your custom HTML code. So, if this functionality is important to you, you will need to write the HTML code to deliver similar functionality, or use the standard portal pages instead.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Details Policy**.
 - Step 2** Specify whether each field is mandatory, optional or unused.
 - Step 3** Click **Save**.
-

What to Do Next

You can fully customize these field names. For example, if you want to change the name of the Optional Data fields to a field commonly used by your company, you can change the text that displays on the Guest portal. See [Customizing Portal UI Fields and Error Messages, page 15-5](#) for details.

Limiting the Number of Supported Devices per Guest

You can limit the number of devices that can be registered to each guest.

This is a global setting affecting all Guest portals. You can set this value below the maximum number of devices currently registered to a guest account, but this change will not affect the existing registered devices.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy**.
 - Step 2** Enter the value in the **Device Registration Portal Limit** field.
 - Step 3** Click **Save**.
-

Related Topics

[Guest Portal Policy Settings, page A-59](#)

Restricting Guests to One Active Network Session

You can restrict guests to having only one device connected to the network at a time. When guests attempt to connect with a second device, the currently-connected device is automatically disconnected from the network.

This is a global setting affecting all Guest portals.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy**.
 - Step 2** Check the **Allow only one guest session per user** option.

- Step 3** Click **Save**.
-

Related Topics

[Guest Portal Policy Settings, page A-59](#)

[Guest Devices Keep Losing Network Access, page G-34](#)

Requiring an Acceptable Use Policy for Guests

You can display an acceptable use policy which guests must accept to fully enable their account. If guests do not accept the policy, they will not obtain network access.

Before You Begin

Create a Guest portal, or use an existing one. The acceptable use policy is specific to each Guest portal.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration**.
- Step 2** Check the Guest portal to update and click **Edit**.
- Step 3** Click the **Operations** tab.
- Step 4** Choose one of these options to determine whether guest users must agree to an acceptable use policy:
- Not Used
 - First Login
 - Every Login
- Step 5** Click **Save**.
-

Related Topics

[Multi-Portal Configuration Settings, page A-56](#)

Customizing the Acceptable Use Policy for Guests

If you require guests to acknowledge an acceptable use policy, you must update the templates to reflect your company's policy. This is a global change that impacts all Guest portals.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Language Template**.
- Step 2** Click the language for which you want to apply the policy.
- Step 3** Click **Configure Acceptable Use Policy Page** and update the title and text to follow your company's policy.
- Step 4** Click **Save**.
-

Related Topics

[Multi-Portal Configuration Settings, page A-56](#)

Creating New Guest Time Profiles.

You can create custom guest time profiles that sponsors can use when creating guest accounts.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Time Profiles .
Step 2	Click Add .
Step 3	Assign a name and description to the time profile. This name will display to sponsors when creating guest accounts.
Step 4	Choose a time zone to be used for the time restrictions.
Step 5	Choose an account type and duration.
Step 6	Enter the day of the week and “from” and “to” times for the restriction times to prevent guest users from accessing the network or to log them off during these times.
Step 7	Click the settings icon to add additional restrictions.
Step 8	Click Submit .
-

Related Topics

- [Guest Time Profile Settings, page A-60](#)
- [Default Guest Time Profiles, page 16-20](#)

Default Guest Time Profiles

Time profiles provide a way to give different levels of time access to different guest accounts. Sponsors must assign a time profile to a guest when creating an account, but they cannot make changes to the time profiles. However, you can customize them and specify which time profiles can be used by particular sponsor groups. Beginning with Cisco ISE 1.2 time profiles are referred to as the *account duration* in the Sponsor portal.

Cisco ISE 1.2 includes these default time profiles, which replace the profiles available previously:

- **DefaultFirstLoginEight**—the account is available for 8 hours starting when the guest user first successfully connects to the Guest portal. This replaces the **DefaultFirstLogin** time profile.
- **DefaultEightHours**—the account is available for 8 hours starting when sponsors first create the account. This replaces the **DefaultOneHour** time profile.
- **DefaultStartEnd**—sponsors can specify dates and times on which to start and stop network access.

If you upgrade to Cisco ISE 1.2, the older time profiles are still available, but you can delete them if you are not using them. If the older time profiles are assigned to a sponsor group, a message alerts you before deleting. If you perform a new installation of Cisco ISE 1.2, only the new time profiles display.

Related Topics

- [Guest Time Profile Settings, page A-60](#)
- [Creating New Guest Time Profiles., page 16-20](#)

Enabling Posture for Guest Users

If you are implementing the Guest portal using the Central WebAuth (CWA) guest deployment, you can enable posture policies for guest users, such as checking for virus protection software.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations .
Step 2	Click Add .
Step 3	Click the Operations tab.
Step 4	Check the Guest users should download the posture client option.
Step 5	Click Submit .
-

Related Topics

- [Self-Provisioning Portal, page 17-2](#)
- [Specifying Ports and Ethernet Interfaces for End-User Portals, page 15-2](#)
- [Multi-Portal Configuration Settings, page A-56](#)

Specifying the Identity Source Sequence for Guests

To allow a guest user to log into the Guest portal, you must choose an identity source sequence to be used for each Guest portal. This sequence is used with the login credentials of the guest to authenticate and authorize the guest for network access.

You can set up multiple authentication sources that are checked in sequence, which can be useful when you have users in multiple stores or want to use a blend of employees and traditional guests in the same flow.

Before You Begin

- Create the identity source sequence, or you can use the Guest_Portal_Sequence, which is the default included with Cisco ISE.
- Create a Guest portal, or use an existing one. This setting is specific to each Guest portal.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration .
Step 2	Check the Guest portal to update and click Edit .
Step 3	Click the Authentications tab.
Step 4	Choose the appropriate identity source sequence.
Step 5	Click Save .
-

Related Topics

[Multi-Portal Configuration Settings, page A-56](#)

Allowing Guest Users to Create Own Accounts and Add Devices

Sponsors typically create login credentials for guest users, but you can bypass this role and allow guests to create their own accounts using self service and self registration.

Allowing Guests to Create Accounts

You can allow users to create their own accounts when they are redirected to the Guest portal.

Before You Begin

Create a Guest portal and set the guest role and time profile.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration .
Step 2	Check the Guest portal to update and click Edit .
Step 3	Click the Operations tab.
Step 4	Check the Guest users should be allowed to do self service option.
Step 5	Click Save .
-

Related Topics

- [Multi-Portal Configuration Settings, page A-56](#)
- [Setting the Guest Role for Self Registration, page 16-23](#)
- [Setting the Time Profile for Self Registration, page 16-23](#)

Allowing Guests to Add Devices

You can allow guests to add devices regardless whether they are signing in using credentials created by the sponsor or by registering on their own.

Before You Begin

Create a Guest portal, or use an existing one. This setting is specific to each Guest portal.

-
Step 1	Choose Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration .
Step 2	Check the Guest portal to update and click Edit .
Step 3	Click the Operations tab.
Step 4	Check the Guest users should be allowed to do device registration option.
Step 5	Click Save .
-

Related Topics

- [Multi-Portal Configuration Settings, page A-56](#)

Setting the Guest Role for Self Registration

You must choose the default guest role to assign to the guest user after self registration. The guest role is used by authorization policies to change the type of access guests have to the network and also:

- Ties the guest user to the associated identity group based on the policies defined in the system
- Controls whether or not the user is treated as an activated guest or not

This is a global setting affecting all Guest portals.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy**.
- Step 2** Choose the default guest role from the **Self Registration Guest Role** field.
- Step 3** Click **Save**.
-

Related Topics

- [Guest Portal Policy Settings, page A-59](#)
- [Allowing Guests to Create Accounts, page 16-22](#)

Setting the Time Profile for Self Registration

Choose the default time profile to assign to the guest user after self-registration. The time profiles determine the time periods in which guests can register access the network. Only CreateTime and FirstLogin type time profiles are available, and both are treated as FromCreation accounts when creating a self-registered guest user account.

This is a global setting affecting all Guest portals.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Portal Policy**.
- Step 2** Choose the selected time profile from the **Self Registration Time Profile** field.
- Step 3** Click **Save**.
-

Related Topics

- [Guest Portal Policy Settings, page A-59](#)
- [Allowing Guests to Create Accounts, page 16-22](#)

Monitoring Sponsor and Guest Activity

Cisco ISE provides the following ways to view and monitor sponsor and guest activities:

- [Suspended and Expired Guest Accounts, page 16-24](#)
- [Purging Expired Guest Accounts, page 16-24](#)
- [Metric Meter, page 16-24](#)
- [Guest Activity Report, page 16-25](#)
- [Guest Accounting Report, page 16-25](#)

- [Guest Sponsor Summary, page 16-25](#)
- [Audit Logging for Guest and Sponsor Portals, page 16-26](#)

Suspended and Expired Guest Accounts

When guest accounts are suspended or expired, the affected guest users cannot access the network.

Guest accounts can be suspended in two ways:

- Guest reached the maximum number of login attempts (as defined in **Administration > Web Portal Management > Settings > Guest > Portal Policy**).
- Sponsor manually suspended the account from the Sponsor portal.

When any guest account reaches the end of its account duration (as defined by the sponsor when creating the account), the account expires.

Sponsor users can reactivate or reinstate suspended and expired accounts. However, expired accounts are automatically purged based on the criteria you set (in **Administration > Web Portal Management > Settings > General > Purge**.) After an account is purged, sponsors must create new accounts.

Purging Expired Guest Accounts

Cisco ISE automatically purges expired guest accounts every 15 days, but you can modify the settings with these conditions:

- If the Cisco ISE server is down when the purge is schedule to run, it will not run again until the next time the server is running at the time of the scheduled purge.
- The system checks every 15 minutes to see if it is time to run the purge. Thus, depending on the timing of this automated process and scheduled purge, there might be up to a 15 minute delay in starting the purge.

You can force expired guest user accounts to purge immediately without waiting for a scheduled purge.

-
Step 1	Choose Administration > Web Portal Management > Settings > General > Purge .
Step 2	Choose one of these options: • Check the Enable purge settings for expired guest accounts check box to schedule a purge and specify the frequency and time of day when a purge should occur. • Click Purge Now to immediately purge the expired guest-user records.
Step 3	Click Save .
-

Related Topics

- [Guest Purge Settings, page A-52](#)

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

The Guest Activity report provides details about the websites that guest users are visiting. You can use this report for security auditing purposes to demonstrate when guest users accessed the network and what they did on it. This report is available at: **Operations > Reports > Endpoints and Users > Guest Activity**.

To use this report you must first:

- Enable the passed authentications logging category. Choose **Administration > Logging > Logging Categories** and select Passed authentications.
- Enable these options on the firewall used for guest traffic:
 - Inspect HTTP traffic and send data to Cisco ISE Monitoring node. Cisco ISE only requires the the IP address and accessed URL for the Guest Activity report so, if possible, limit the data to include just this information.
 - Send syslogs to Cisco ISE Monitoring node

Related Topics

- [Reporting, page 26-1](#)
- [Configuring Integrated URL Logging and Reporting of Guest Traffic in a Cisco Network](#)

Guest Accounting Report

The Guest Accounting report displays the guest login history for an indicated time period. All users assigned to the ActivatedGuest or Guest identity groups appear in this report. This report is available at: **Operations > Reports > Endpoints and Users > Guest Accounting**.

Related Topics

[Reporting, page 26-1](#)

Guest Sponsor Summary

The Guest Sponsor Summary report displays all guest users created by each sponsor, and it also indicates the number of self-registered guest users. You can click on a sponsor name to display details about the guest users. This report is available at: **Operations > Reports > Endpoints and Users > Guest Sponsor Summary**.

Related Topics

[Reporting, page 26-1](#)

Audit Logging for Guest and Sponsor Portals

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.

Guest login flow gets logged in the audit logs regardless whether the guest login has passed or failed.

Related Topics

[Chapter 25, “Monitoring and Troubleshooting,”](#)

Guest Deployment Scenarios

Cisco ISE supports several deployment options enable secure guest access. You can provide wired or wireless guest connectivity and local or central web authorization.

NAD with Central WebAuth Process Flow

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 network access device (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 the client's device is connected to a NAD, the guest service interaction takes the form of a failed MAC Authentication Bypass (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 device re-connects and the NAD initiates a MAB request.
5. The Cisco ISE server processes the MAB request and does not find an endpoint 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 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 HTTP or 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**

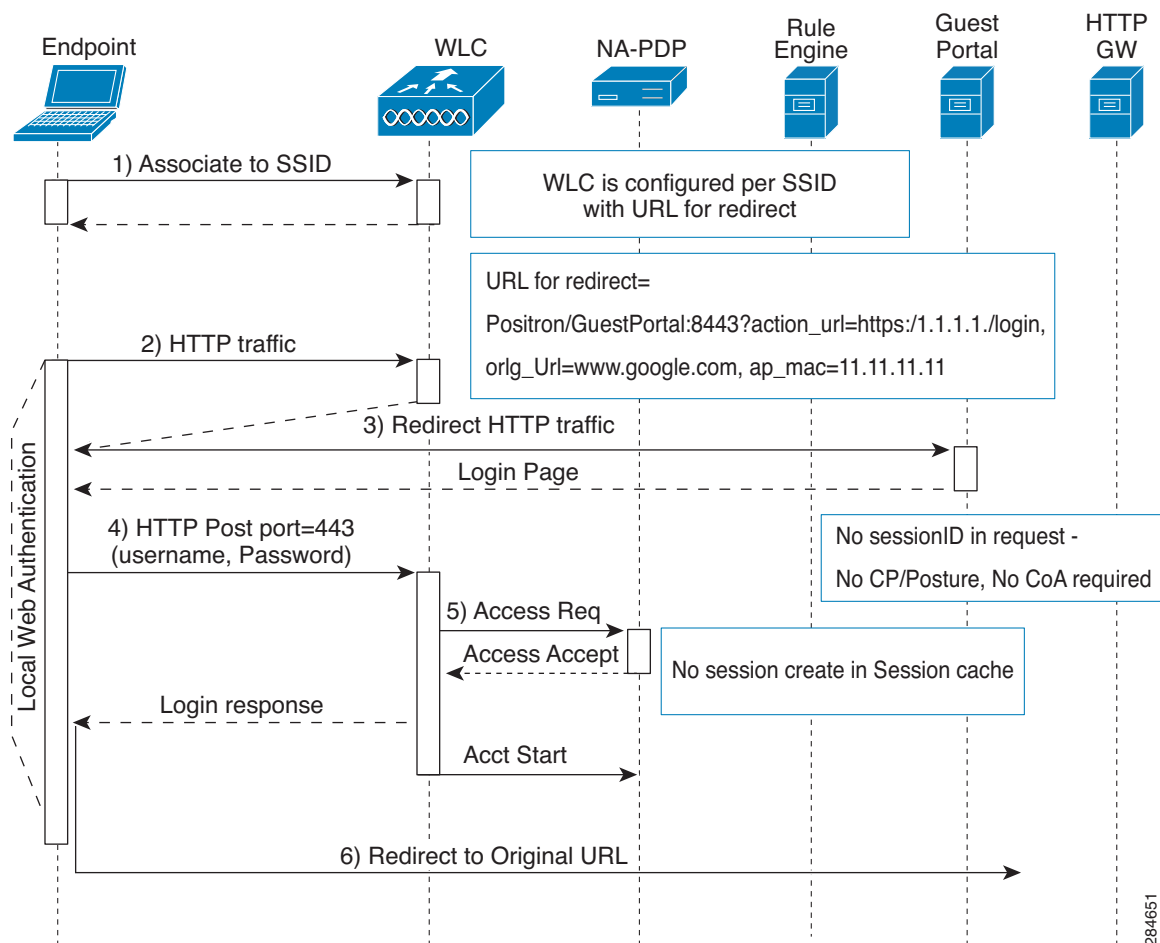
“NetworkAccess:UseCase=GuestFlow” applies for Active Directory and LDAP users logging in as guest users.

Wireless LAN Controller with Local WebAuth

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 16-1.

Figure 16-1 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.

IP Address and Port Values Required for the Login.html 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, but you can change this value so ensure that the value you assign to the switch matches the setting in Cisco ISE.

```
<!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.

HTTPS Server Enabled on the NAD

To use web-based authentication, you must enable the HTTPS server within the switch using the **ip http secure-server** command.

Support for Customized Authentication Proxy Web Pages on the NAD

You can upload custom pages for success, expiry, and failure to the NAD. Cisco ISE does not require any specific customizations so you can create these pages using the standard configuration instructions included with the NAD.

Configuring Web Authentication on the NAD

You need to complete the web authentication on the NAD by replacing the default HTML pages with your custom files.

Before You Begin

Create four substitute HTML pages to use instead of the switch default HTML pages during web-based authentication.

Step 1 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 2 After copying your HTML files to the switch, perform the following commands in global configuration mode:

a.	ip admission proxy http login page file <i>device:login-filename</i>	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 <i>device:success-filename</i>	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 <i>device:fail-filename</i>	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 <i>device:expired-filename</i>	Specifies the location of the custom HTML file to use in place of the default login expired page.

Step 3 Configure the customized authentication proxy web pages following the guidelines provided by the switch.

Step 4 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

Using device registration web authentication (DRW), you can allow guests’ devices to connect to your network without requiring guest account credentials.

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, Cisco 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.

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 Web Portal 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 Web Portal 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 (DRW) to perform VLAN IP Release and Renew, thereby re-authorizing the CoA type for both wired and wireless to Change of Auth.

Creating the Device Registration WebAuth Guest Portal

You can configure Device Registration WebAuth (DRW).

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Multi-Portal Configurations**.
 - Step 2** Enter a unique name in the **Name** field. 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
 - Step 3** Choose one of the following:
 - **Device Web Authorization Portal**—to use standard HTML pages provided by Cisco ISE
 - **Custom Device Web Authorization Portal**—to upload customized HTML pages and images.
 - Step 4** Choose **GuestEndpoints** from the Endpoint Identity Group option. Cisco ISE provides this default identity group to use for the DRW portal.

Step 5 Click **Submit**.

What to Do Next

[Creating a DRW Authorization Profile, page 16-32](#)

Related Topics

[Cisco ISE Authorization Profiles, page 20-2](#)

Creating a DRW Authorization Profile

Device Registration WebAuth requires that you set up a special authorization profile.

Before You Begin

You must first create the DRW Guest Portal so you can use its name when configuring the authorization profile.

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

Step 2 Create an authorization profile using the name of the DRW Guest portal that you created previously.

What to Do Next

[Creating a DRW Authorization Policy Rule, page 16-32](#)

Related Topics

[Cisco ISE Authorization Profiles, page 20-2.](#)

Creating a DRW Authorization Policy Rule

After the guest user verifies the Accept User Policy, Cisco ISE creates an endpoint, which displays in the internal endpoint identity store. The endpoint is created using the MAC address and has the AUP Accepted attribute set to true.

Step 1 Choose **Policy > Authorization > Standard** to create a new authorization policy.

Step 2 Select the **GuestEndpoints** endpoint identity group for conditions.

Step 3 Select the DRW authorization profile for permissions.

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`

Related Topics

[Configuring Authorization Policies, page 20-8.](#)



Supporting Personal Devices

This chapter provides information about allowing employees to use their personal devices on your corporate network.

This chapter contains the following sections:

- [Personal Devices on a Corporate Network, page 17-1](#)
- [Personal Devices Portals, page 17-1](#)
- [Employee Accounts, page 17-3](#)
- [Supporting Device Registration Using Native Supplicants, page 17-3](#)
- [Supporting the My Devices Portal, page 17-4](#)
- [Managing Personal Devices Added by Employees, page 17-6](#)
- [Deployment Scenarios for Employee-Owned Personal Devices, page 17-9](#)

Personal Devices on a Corporate Network

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users and their devices. A Cisco ISE Advanced License provides the tools you need to allow employees to securely use personal devices on a corporate network.

Users have two ways of adding their personal devices to the network: using native supplicants or the My Devices portal. You can create native supplicant profiles so that when a user logs in, based on the profile that you associate with that user's authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard needed to set up the user's personal device to access the network. Native supplicant profiles are not available for all devices, but users can use the My Devices portal to add those devices manually.

Personal Devices Portals

Cisco ISE provides several web-based portals to support employee-owned personal devices.

Self-Provisioning Portal

Employees access the Self-Provisioning portal when registering personal devices using native supplicants. The first time employees attempt to access the network using a personal device, they will be guided automatically through registering and installing the supplicant. After they have registered a device, they can use the My Devices portal to manage it.

Related Topics

- [Supporting Device Registration Using Native Supplicants, page 17-3](#)

My Devices Portal

Some network devices are not supported by native supplicants. If the operating system is not supported or if the devices do not have web browsers (such as printers, Internet radios, and other devices), these devices still need to access the network. To add these types of devices to your company's network, employees need to use the My Devices portal.

Employees can add and manage new devices by entering the MAC address for the device. When employees add devices using the My Devices portal, Cisco ISE adds the devices to the Endpoints page as members of the RegisteredDevices endpoint identity group. The devices are profiled like any other endpoint in Cisco ISE and goes through a registration process for network access.

Regardless of whether or not employees register their devices using the native supplicant or the My Devices portal, all employees can use the My Devices portal to manage their personal devices.

Related Topics

- [Setting Up and Customizing End-User Web Portals, page 15-1](#)
- [Supporting the My Devices Portal, page 17-4](#)
- [Operating Systems Supported by Native Supplicants, page 17-3](#)

Blacklist Portal

Employees can indicate whether they have lost a device, which adds it to the Blacklist endpoint identity group, which prevents others from using the device to obtain unauthorized network access. If users attempt to connect to the network using one of these devices, they are redirected to the Blacklist portal. If the device is found, employees can reinstate it and regain network access without having to register the device again.

You can configure the port settings (default is port 8444) for the Blacklist portal using the Admin portal. Employees do not access this portal directly.

Related Topics

- [Setting Up and Customizing End-User Web Portals, page 15-1](#)

Employee Accounts

When you add employees or contractors to Cisco ISE, you can authorize them to use personal devices on the network. Whether you have added them using external identity stores or created internal users, you can authorize them to use personal devices on your network.

Cisco ISE authenticates users through a local database, or through external Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory identity stores.

Cisco ISE includes the Employee user identity group for internal users.

Related Topics

[Adding Users, page 14-3](#)

Supporting Device Registration Using Native Supplicants

You can create native supplicant profiles to support personal devices on the Cisco ISE network. Based on the profile that you associate with that user's authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard needed to set up the user's personal device to access the network.

The first time employees attempt to access the network using a personal device, they will be guided automatically through registration and supplicant configuration. After they have registered the device, they can use the My Devices portal to manage their devices.

- [Operating Systems Supported by Native Supplicants, page 17-3](#)
- [Allowing Employees to Register Personal Devices Using Native Supplicants, page 17-3](#)

Operating Systems Supported by Native Supplicants

Native supplicants are supported for these operating systems:

- Android (excluding Amazon Kindle, B&N Nook)
- Mac OS X (for Apple Mac computers)
- Apple iOS devices (Apple iPod, iPhone and iPad)
- Microsoft Windows 7, Vista, and XP

Allowing Employees to Register Personal Devices Using Native Supplicants

The self-provisioning flow enables employees to connect devices to the network directly using native supplicants, which are available for Windows, MacOS, iOS, and Android devices.

If you do not want to enable this feature, employees can still add personal devices using the My Devices portal. By default, this feature is disabled when upgrading and enabled when performing a fresh installation of Cisco ISE.

Before You Begin

You must create the native supplicant profiles.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations**.
- Step 2** Choose a portal and click **Edit**.
- Step 3** Click **Operations**.
- Step 4** Check **Enable Self-Provisioning Flow**.
-

Related Topics

- [Creating Native Supplicant Profiles, page 22-25](#)
- [Configuring Personal Device Registration Behavior, page 22-26](#)

Supporting the My Devices Portal

Employees can use the My Devices portal to register and manage their personal devices. The My Devices portal includes online help that provides employees with assistance in using the portal. However, there are several things you need to do to prepare the portal before employees can access it.

Related Topics

[My Devices Portal, page 17-2](#)

Specifying the Identity Store Sequence Used for Employee Authentication

To allow an employee to log into the My Devices portal, you must specify an identity store sequence. This sequence is used with the login credentials of an employee to authenticate and authorize the employee for access to the My Devices portal. Cisco ISE includes a default identity store sequence for employees: `MyDevices_Portal_Sequence`.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > My Devices > Authentication Source**.
- Step 2** Choose an identity store sequence from the **Identity Store Sequence** drop-down list.
- Step 3** Click **Save**.
-

Related Topics

- [My Devices Portal Settings, page A-54](#)
- [Creating Identity Source Sequences, page 14-38](#)

Enabling the My Devices Portal

By default, the My Devices portal is enabled. If you disable it, a customizable error message notifies users that the portal is unavailable when they attempt to go to the URL.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > My Devices > Portal Configuration**.
- Step 2** Uncheck the **Enable My Devices Portal** check box.
- Step 3** Click **Save**.
-

Related Topics

[My Devices Portal Settings, page A-54](#)

Implementing an Acceptable Use Policy for Employees

You can require employees to acknowledge an acceptable use policy when using the My Devices portal.

Customizing the Acceptable Use Policy for Employees

If you require employees to acknowledge an acceptable use policy, you must update the templates to reflect your company's policy.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > My Devices > Language Template**.
- Step 2** Click the language for which you want to apply the policy.
- Step 3** Click **Configure Acceptable Use Policy Page** and update the title and text to follow your company's policy.
- Step 4** Click **Save**.
-

Related Topics

- [Requiring an Acceptable Use Policy for Employees, page 17-5](#)
- [My Devices Portal Language Template Settings, page A-53](#)

Requiring an Acceptable Use Policy for Employees

You can display an acceptable use policy on the login page and the device registration page of the My Devices portal.

Before You Begin

Update the Acceptable Use text with your company's policy.

-
- Step 1** Choose **Administration > Web Portal Management > Settings > My Devices > Portal Configuration**.
- Step 2** Check the **Enable the Acceptable Use Policy Link** check box.
- Step 3** Click **Save**.
-

Related Topics

- [Customizing the Acceptable Use Policy for Employees, page 17-5](#)
- [My Devices Portal Settings, page A-54](#)

Limiting the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 100 personal devices.

-
Step 1	Choose Administration > Web Portal Management > Settings > My Devices > Portal Configuration .
Step 2	Enter the maximum number of devices that an employee can register in the Device Management field. By default, this value is set to 5 devices.
Step 3	Click Save .
-

Related Topics

[My Devices Portal Settings, page A-54](#)

Customizing Help Desk Contact Details

This setting allows you to customize the e-mail address and phone number associated with the Contact link on the login and main page of the My Devices portal.

Before You Begin

If you want to change the Contact link name, you need to update the name in the My Devices Language Template settings (**Administration > Web Portal Management > Settings > My Devices > Language Template > Configure Miscellaneous Items**).

-
Step 1	Choose Administration > Web Portal Management > Settings > My Devices > Portal Configuration .
Step 2	Enter the help desk contact information in the Email Address and Phone Number fields.
Step 3	Click Save .
-

Related Topics:

[My Devices Portal Settings, page A-54](#)

[My Devices Portal Language Template Settings, page A-53](#)

Managing Personal Devices Added by Employees

When an employee registers a device using a native supplicant or adds a device to the My Devices portal, it displays in the Endpoints list. Although employees can disassociate a device from their account by deleting it, the device remains in the Cisco ISE database. As a result, employees might need your assistance in resolving errors they encounter when working with their devices.

Displaying Devices Added by an Employee

You can locate devices added by a specific employee using the Portal User field displayed on the Endpoints listing page. This might be useful if you need to delete any devices registered by a specific user. By default, this field does not display so you must enable it first before searching by it.

-
- Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.
 - Step 2** Click the Settings icon and choose **Columns**.
 - Step 3** Select **Portal User** to display this information in the Endpoints listing.
 - Step 4** Click the **Show** drop-down list and choose **Quick Filter**.
 - Step 5** Enter the user's name in the **Portal User** field to display only the endpoints assigned to that particular user.
-

Related Topics

[Filtering Data on Listing Pages, page 2-8](#)

Registered Endpoints Report

The Registered Endpoints report provides information about the endpoints that are registered through the device registration portal. (For information on supplicant provisioning statistics and related data, see [Viewing Client Provisioning Reports, page 22-30](#).)

You can query the endpoint database for endpoints that are assigned to the RegisteredDevices endpoint identity group. You can also generate reports for a specific user that have the PortalUser attribute set to a non-null value.

The Registered Endpoints Report provides information about a list of endpoints that are registered through the device registration portal by a specific user for a selected period of time.

-
- Step 1** Log into your Cisco ISE user interface.
 - Step 2** Choose **Operations > Reports > Catalog**.
 - Step 3** In the Reports navigation pane, click **My Devices**.
 - Step 4** Choose **Registered Endpoints**.
 - Step 5** Click **Run**.

You can run a query on the following: Users, MAC address of a registered device, identity group, endpoint policy, and generate a report.

Errors When Adding Devices to My Devices Portal

Employees cannot add a device that is already added if another employee has previously added the device so that it already exists in the Cisco ISE endpoints database.

If employees are attempting to add a device that supports a native supplicant, recommend that they use that instead. That registration process will overwrite the original registration and switch ownership to the new user.

If the device is a MAC Authentication Bypass (MAB) device, such as a printer, then you must resolve ownership of the device, and if appropriate, remove the device from the endpoints database so that the new owner can successfully add the device.

Devices Deleted from My Devices Portal Remain in Endpoints Database

When an employee deletes a device from the My Devices portal, the device is removed from their list of registered devices, but the device remains in the Cisco ISE endpoints database and display in the RegisteredDevices endpoint identity group. You can permanently delete the device from the Endpoints page (**Administration > Identity Management > Identities > Endpoints**).

Deployment Scenarios for Personal Devices Using Native Supplicants

The deployment flows to support personal devices using native supplicants vary slightly based on these factors:

- **Single or dual SSID**—With single SSID, the same WLAN is used for certificate enrollment, provisioning, and network access. In a dual SSID deployment, there are two SSIDs: one provides enrollment and provisioning and the other provides secure network access.
- **Windows, MacOS, iOS, or Android device**—The native supplicant flow starts similarly regardless of device type by redirecting employees using a supported personal device to the Self-Provisioning portal to confirm their device information. At this point, the process diverges based on device type.

Employee Connects to Network

- **Single SSID**—Employee connects the device to the 802.1x SSID by entering the corporate username and password.
- **Dual SSID**—Employees connect to the open guest provisioning SSID, are redirected to the Guest portal, and enter their user credentials in the standard Guest portal.

Employee's Credentials are Authenticated

Cisco ISE authenticates the user against the corporate Active Directory or other corporate identity stores and provides an authorization policy.

Device is Redirected to the Self-Provisioning Portal

The device is redirected to the Self-Provisioning portal. The device's MAC address is automatically pre-configured, but employees can verify and add a description..

Native Supplicant is Configured (MacOS, Windows, iOS)

The native supplicant is configured; the process varies by device.

- **MacOS and Windows devices**—user clicks on the **Register** button on the Self-Provisioning portal to download and install the supplicant provisioning wizard, which configures the supplicant and provides the certificate (if required).

- iOS devices—the Cisco ISE policy server sends a new profile using Apple's iOS over-the-air to the iPad, which includes:
 - The issued certificate (if configured) embedded with the iPad's MAC address and employee's Active Directory username
 - A Wi-Fi supplicant profile that enforces the use of MSCHAPv2 or EAP-TLS for 802.1X authentication.
- Android devices—users are prompted to download the Cisco ISE prompts and routes employee to download the Cisco Network Setup Assistant from Google Play. After installing the app, the employee opens it, and starts the setup wizard, which generates authentication parameters and initiates a certificate request (if required) for device certification.

Change of Authorization Issued

Cisco ISE initiates a Change Of Authorization (CoA) and connects the MacOS X , Windows, and Android devices to the secure dot1x network. For single SSID, iOS devices also connect automatically, but for dual SSID, the wizard prompts iOS users to manually connect to the new network.



PART 5

Enabling and Configuring Cisco ISE Services



Setting Up Policy Conditions

Cisco ISE is a policy-based, network-access-control solution, which offers the following services: network-access, guest, posture, client provisioning, and profiler services. While configuring Cisco ISE, you create authentication, authorization, guest, posture, and profiler policies. Policy conditions are basic building blocks of policies. There are two types of policy conditions, simple and compound.

This chapter describes the policy conditions and how you can create them for the various services that Cisco ISE offers.

This chapter contains the following sections:

- [Simple and Compound Conditions, page 18-1](#)
- [Policy Evaluation, page 18-2](#)
- [Creating Simple Conditions, page 18-2](#)
- [Creating Compound Conditions, page 18-3](#)
- [Profiler Conditions, page 18-4](#)
- [Posture Conditions, page 18-5](#)
- [Creating Time and Date Conditions, page 18-8](#)

Simple and Compound Conditions

Cisco ISE uses rule-based policies to provide network access, profiler, posture, and guest services. These rule-based policies consist of rules that are made up of conditions. Cisco ISE allows you to create conditions as individual, reusable policy elements that can be referred from other rule-based policies. There are two types of conditions:

- **Simple condition**—A simple condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. You can save simple conditions and use them in other rule-based policies.

Simple condition takes the form: A operand B, where A can be any attribute from the Cisco ISE dictionary and B can be one of the values that the attribute A can take. The Device Type is used as an attribute for all network devices that can include all device types as its value, which means that A Equals B in the following form:

DEVICE:Device Type Equals All Device Types

- **Compound condition**—A compound condition is made up of one or more simple conditions that are connected by the AND or OR operator. Compound conditions are built on top of simple conditions. You can save and reuse compound conditions in other rule-based policies.

Compound condition can 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 Cisco ISE dictionary such as the username and device type.

This is an example of a compound condition:

DEVICE:Model Name Matches Catalyst6K AND Network Access:Use Case Equals Host Lookup.

You cannot delete conditions that are used in a policy or are part of a compound condition.

Related Topics

- [Creating Simple Conditions, page 18-2](#)
- [Creating Compound Conditions, page 18-3](#)

Policy Evaluation

Typically, policies consist of rules, where each rule consists of conditions to be satisfied that 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.

At run-time, Cisco ISE evaluates the policy conditions and then applies the result that you define based on whether the policy evaluation returns a true or a false value.

During policy-condition evaluation, Cisco ISE compares an attribute with a value. It is possible that 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, in the 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.

Creating Simple Conditions

You can create simple conditions and reuse them when you define authentication, authorization, or guest policies.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

-
- Step 1** Choose **Policy > Policy Elements > Conditions**.
 - Step 2** Click the arrow next to **Authentication** or **Authorization** or **Guest**, and then click **Simple Conditions**.
 - Step 3** Click **Add**.
 - Step 4** Enter appropriate values for the Name, Description, Attribute, Operator, and Value fields.

**Note**

If you specify any Identity Group in simple conditions, ensure that 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 following form:

```
(InternalUser:IdentityGroup) : Equal : (Identity Group Name).
```

Step 5 Click **Submit** to save the condition.

What to Do Next

- See the [“Creating a Rule-Based Authentication Policy” section on page 16-27](#) for information on how to define a rule-based authentication policies using simple conditions.
- See the [“Configuring Authorization Policies” section on page 17-8](#) for information on how to create authorization policies using simple conditions.
- See the [“Creating a Sponsor Group Policy” section on page 16-6](#) for information on how to define sponsor group policies using simple conditions.

Creating Compound Conditions

You can create compound conditions and reuse them when you define authentication policies.

Before You Begin

- Cisco ISE includes predefined compound conditions for some of the most common use cases. You can edit these predefined conditions to suit your requirements.
- To perform the following task, you must be a Super Admin or Policy Admin.

-
- Step 1** Choose **Policy > Policy Elements > Conditions**.
- Step 2** Click the arrow next to **Authentication** or **Authorization** or **Guest** and then click **Compound Conditions**.
- Step 3** Click **Add**.
- 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.
- Step 6** Click the action icon at the end of this row to add more conditions.
- 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 operand from the drop-down list. You can choose AND or OR and the same operand will be used between all the conditions in this compound condition.
- Step 9** Click **Submit** to create the compound condition.
-

What to Do Next

- See the [“Creating a Rule-Based Authentication Policy”](#) section on page 16-27 for information on how to define a rule-based authentication policies using compound conditions
- See the [“Configuring Authorization Policies”](#) section on page 17-8 for information on how to create authorization policies using compound conditions.
- See the [“Creating a Sponsor Group Policy”](#) section on page 16-6 for information on how to define sponsor group policies using compound conditions.

Profiler Conditions

Profiling conditions are policy elements and are similar to other conditions. However unlike authentication, authorization, and guest conditions, the profiling conditions can be based on a limited number of attributes. The Profiler Conditions page lists the attributes that are available in Cisco ISE and their description.

Profiler conditions can be one of the following:

- **Cisco Provided**—Cisco ISE includes predefined profiling conditions when deployed and they are identified as Cisco Provided in the Profiler Conditions page. You cannot delete Cisco Provided profiling conditions.

You can also find Cisco Provided conditions in the System profiler dictionaries in the following location: Policy > Policy Elements > Dictionaries > System.

For example, MAC dictionary. 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.

- **Administrator Created**—Profiler conditions that you create as an administrator of Cisco ISE or predefined profiling conditions that are duplicated are identified as Administrator Created. You can create a profiler condition of DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP, and NMAP types using the profiler dictionaries in the Profiler Conditions page.

Creating a Profiler Condition

Endpoint profiling policies in Cisco ISE allow you to categorize discovered endpoints on your network, and assign them to specific endpoint identity groups. These endpoint profiling policies are made up of profiling conditions that Cisco ISE evaluates to categorize and group endpoints.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

-
Step 1	Choose Policy > Policy Elements > Conditions > Profiling > Add .
Step 2	Enter values for the fields as described in the Profiler Condition Settings, page B-9 .
Step 3	Click Submit to save the profiler condition.
Step 4	Repeat this procedure to create more conditions.
-

Related Topics

- [Simple and Compound Conditions, page 18-1](#)
- [Policy Evaluation, page 18-2](#)
- [Profiler Condition Settings, page B-9](#)

Posture Conditions

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.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web for the first time. This process is called the initial posture update.

After an initial posture update, Cisco ISE also creates Cisco defined simple and compound conditions. Cisco defined simple conditions have pc_ as their prefixes and compound conditions have pr_ as their prefixes.

You can also configure Cisco ISE to download the Cisco-defined conditions periodically as a result of dynamic posture updates through the web. You cannot delete or edit Cisco defined posture conditions.

A user defined condition or a Cisco defined condition includes both simple conditions and compound conditions.

Related Topics

- [Downloading Posture Updates, page 23-9](#)
- [Simple and Compound Conditions, page 18-1](#)
- [Policy Evaluation, page 18-2](#)
- [Posture Conditions Settings, page B-10](#)

Simple Posture Conditions

You can use the Posture navigation pane to manage the following simple conditions:

- **File Conditions**—A 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 condition that checks for the existence of a registry key or the value of the registry key on the client.
- **Application Conditions**—A condition that checks if an application (process) is running or not running on the client.
- **Service Conditions**—A condition that checks if a service is running or not running on the client.
- **Dictionary Conditions**—A condition that checks a dictionary attribute with a value.

Related Topics

- [Simple and Compound Conditions, page 18-1](#)
- [Policy Evaluation, page 18-2](#)
- [Posture Conditions Settings, page B-10](#)

Creating Simple Posture Conditions

You can create file, registry, application, service, and dictionary simple conditions that can be used in posture policies or in other compound conditions.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

-
Step 1	Choose Policy > Policy Elements > Conditions > Posture .
Step 2	Choose any one of the following: File, Registry, Application, Service, or Dictionary Simple Condition.
Step 3	Click Add .
Step 4	Enter the appropriate values in the fields.
Step 5	Click Submit .
-

Related Topics

- [Simple and Compound Conditions, page 18-1](#)
- [Policy Evaluation, page 18-2](#)
- [File Condition Settings, page B-10](#)
- [Registry Condition Settings, page B-11](#)
- [Application Condition Settings, page B-12](#)
- [Service Conditions Settings, page B-13](#)
- [Dictionary Simple Conditions Settings, page B-16](#)

Compound Posture Conditions

Compound conditions are made up of one or more simple conditions, or compound conditions. You can make use of the following compound conditions while defining a Posture policy.

- **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

Related Topics

- [Simple and Compound Conditions, page 18-1](#)
- [Policy Evaluation, page 18-2](#)
- [Posture Compound Condition Settings, page B-13](#)
- [Antivirus Compound Condition Settings, page B-13](#)
- [Antispyware Compound Condition Settings, page B-15](#)

- [Dictionary Compound Condition Settings, page B-16](#)
- [Antivirus and Antispyware Support Chart, page 18-7](#)

Cisco-Predefined Condition for Enabling Automatic Updates in Windows Clients

The `pr_AutoUpdateCheck_Rule` is a Cisco predefined condition, which is downloaded to the Compound Conditions page. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

Cisco-Preconfigured Antivirus and Antispyware Conditions

Cisco ISE loads preconfigured antivirus and antispyware compound conditions in the AV and AS Compound Condition pages, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These compound conditions can check if the specified antivirus and antispyware products exist on all the clients. You can also create new antivirus and antispyware compound conditions in Cisco ISE.

Antivirus and Antispyware Support Chart

Cisco ISE uses an antivirus and antispyware support chart, which provides the latest version and date in the definition files for each vendor product. Users must frequently poll antivirus and antispyware support charts for updates. The antivirus and antispyware vendors frequently update antivirus and antispyware definition files, look for the latest version and date in 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.

The antivirus and antispyware support chart is available on Cisco.com at:

http://www.cisco.com/en/US/docs/security/ise/1.1/release_notes/win-avas-3-4-27-1.pdf

Creating Compound Posture Conditions

You can create compound conditions that can be used in posture policies for posture assessment and validation.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

-
- Step 1** Choose **Policy > Policy Elements > Conditions > Posture > Compound Conditions > Add**.
- Step 2** Enter appropriate values for the fields.
- Step 3** Click **Validate Expression** to validate the condition.
- Step 4** Click **Submit**.
-

Related Topics

- [Simple and Compound Conditions, page 18-1](#)
- [Policy Evaluation, page 18-2](#)
- [Posture Compound Condition Settings, page B-13](#)
- [Antivirus Compound Condition Settings, page B-13](#)
- [Antispyware Compound Condition Settings, page B-15](#)
- [Dictionary Compound Condition Settings, page B-16](#)

Creating Time and Date Conditions

Time and date conditions allow you to limit or extend permission to access to Cisco ISE system resources.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

-
- Step 1** Choose **Policy > Policy Elements > Conditions > Time and Date > Add**.
- Step 2** Enter appropriate values in the fields.
- In the Standard Settings area, specify the time and date to provide access.
 - In the Exceptions area, specify the time and date range to limit access.
- Step 3** Click **Submit**.
-

Related Topics

- [Simple and Compound Conditions, page 18-1](#)
- [Policy Evaluation, page 18-2](#)



Managing Authentication Policies

Using the Cisco Identity Services Engine (Cisco ISE) Admin portal, you can define authentication policies that determine who accesses the resources on your network. This chapter contains the following topics:

- [Cisco ISE Authentication Policies, page 19-1](#)
- [Simple Authentication Policies, page 19-4](#)
- [Rule-Based Authentication Policies, page 19-6](#)
- [Protocol Settings for Authentication, page 19-10](#)
- [Network Access Service, page 19-14](#)
- [Cisco ISE Acting as a RADIUS Proxy Server, page 19-18](#)
- [RADIUS Server Sequence, page 19-19](#)
- [Policy Modes, page 19-19](#)
- [Configuring a Simple Authentication Policy, page 19-21](#)
- [Configuring a Rule-Based Authentication Policy, page 19-22](#)
- [Policy Sets, page 19-23](#)
- [Authentication Policy Built-In Configurations, page 19-26](#)
- [Viewing Authentication Results, page 19-28](#)

Cisco ISE Authentication Policies

Authentication policies define the protocols that Cisco ISE uses to communicate with the network devices, and the identity sources that it uses 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 a policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

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 is available in Cisco ISE that is used for authentications. Any updates to the authentication policy will override the default settings.

Related Topics

- [Policy Condition Evaluation, page 19-2](#)
- [Supported Authentication Protocols, page 19-2](#)
- [Supported Authentication Types and Database, page 19-3](#)
- [Types of Authentication Failures, page 19-3](#)
- [Authentication Policy Terminology, page 19-4](#)

Policy Condition Evaluation

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.

Supported Authentication Protocols

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)

This section contains the following topics:

- [Supported Authentication Types and Database, page 19-3](#)
- [Authentication Policy Terminology, page 19-4](#)
- [Simple Authentication Policies, page 19-4](#)
- [Rule-Based Authentication Policies, page 19-6](#)

Supported Authentication Types and Database

The authentication type is based on the protocols that are chosen. [Table 14-1 on page 14-7](#) 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
 - Guest 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.

By default, the identity source that Cisco ISE will look up for user information is the internal users database.

Types of Authentication Failures

If you choose the identity method as 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:

- Reject—A reject response is sent.
- Drop—No response is sent.
- Continue—Cisco ISE continues with the authorization policy.

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

The following are some of the commonly used terms in the authentication policy pages:

- 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.

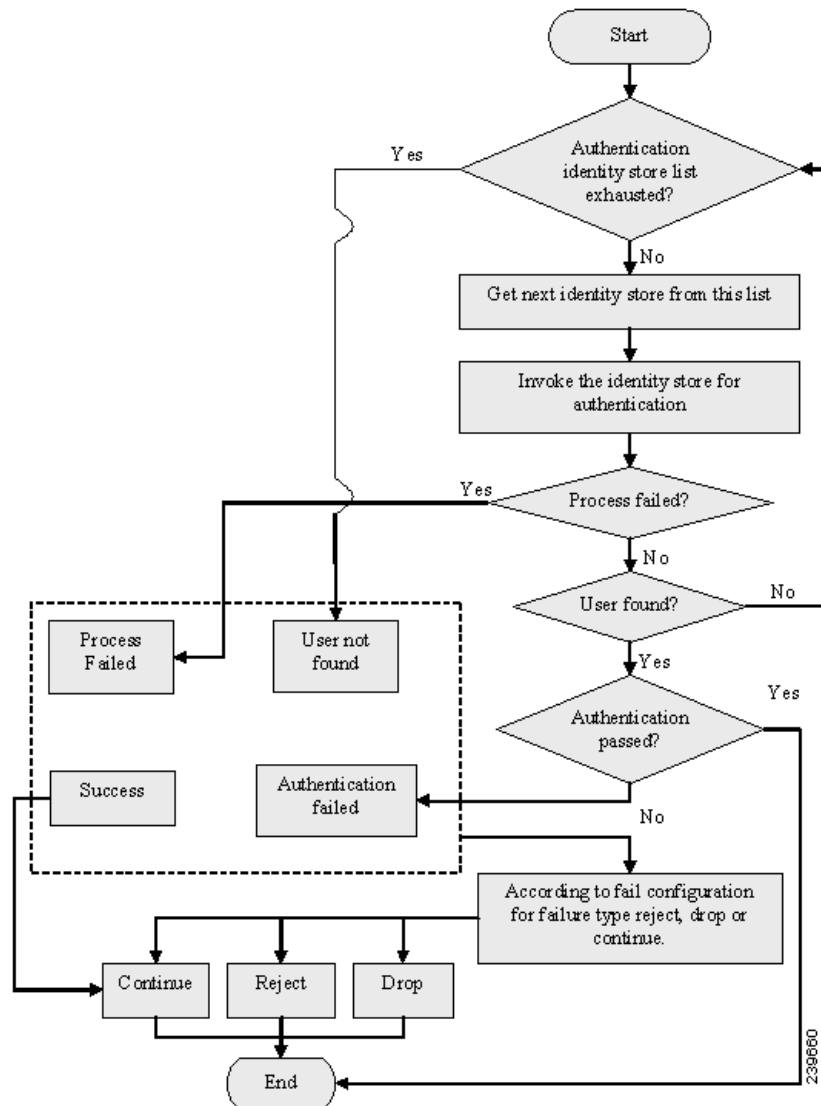
The procedure for configuring a simple authentication policy includes defining an allowed protocols service and configuring a simple authentication policy. See the [“Defining Allowed Protocols for Network Access” section on page 19-14](#) for information on how to create an allowed protocols service.

Related Topics

- [Simple Authentication Policy Flow, page 19-5](#)
- [Guidelines for Configuring Simple Authentication Policies, page 19-6](#)
- [Configuring a Simple Authentication Policy, page 19-21](#)
- [Rule-Based Authentication Policies, page 19-6](#)

Simple Authentication Policy Flow

Figure 19-1 Simple Authentication Policy Flow



The result of a simple policy can be any one of the following:

- Authentication passed
- Authentication failed

An authentication can fail happens due to any of the following reasons:

- Bad credentials or disabled user.
- User not found.
- Authentication process fails.

Guidelines for Configuring Simple Authentication Policies

The following are guidelines that you must adhere to while configuring simple authentication policies:

- If you wish to use the RADIUS server sequence, then you must define this access service before you define the policy. See the [“Cisco ISE Acting as a RADIUS Proxy Server” section on page 19-18](#) 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 Users and External Identity Sources” section on page 14-1](#) 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 14-38](#) 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.
- Host authentication is performed with the MAC address only (MAB).

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. See [Table 19-1](#), which lists the fixed attributes that are supported by dictionaries, which can be used in policy conditions.

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. The two types of conditions are:

- Simple condition
- Compound condition

Related Topics

- [Simple and Compound Conditions, page 18-1](#)
- [Creating Simple Conditions, page 18-2](#)
- [Creating Compound Conditions, page 18-3](#)
- [Configuring a Rule-Based Authentication Policy, page 19-22](#)

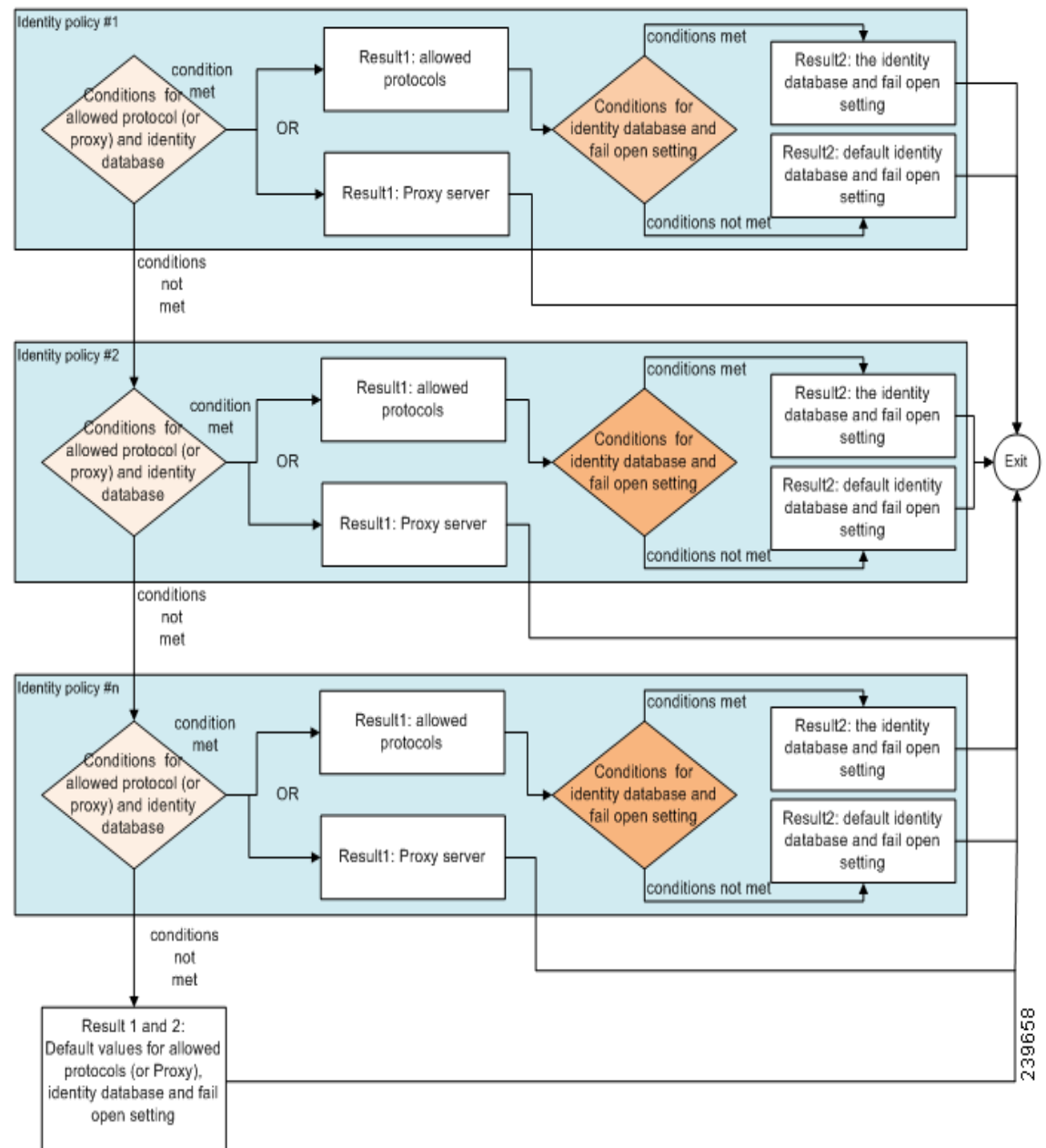
Rule-Based Authentication Policy Flow

In rule-based policies, you can define multiple rules as illustrated in Figure 19-2. 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.

We recommend that you use only three, or at most four databases in an identity source sequence.

Figure 19-2 Rule-Based Authentication Policy Flow



Supported Dictionaries for Rule-Based Authentication Policies

Cisco ISE supports the following dictionaries:

- System-defined dictionaries
 - CERTIFICATE
 - DEVICE
 - RADIUS
- RADIUS vendor dictionaries
 - *Airespace*
 - *Cisco*
 - *Cisco-BBSM*
 - *Cisco-VPN3000*
 - *Microsoft*
 - *Network access*

See the [“Dictionaries and Dictionary Attributes” section on page 10-1](#) for more information on the dictionaries in Cisco ISE.

Attributes Supported by Dictionaries

[Table 19-1](#) lists the fixed attributes that are supported by dictionaries, which can be used in policy conditions.

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 will only see the following network access attributes: Device IP Address, ISE Host Name, Network Device Name, Protocol, and Use Case.

Table 19-1 List of Attributes Supported by 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

Table 19-1 *List of Attributes Supported by Dictionaries (continued)*

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Network Access	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 19-1 *List of Attributes Supported by Dictionaries (continued)*

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Certificate	Common Name	No	Yes
	Country		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	Issuer		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
	Issuer - Street Address		
	Issuer - Domain Component		
	Issuer - User ID		

Protocol Settings for Authentication

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:

- [Guidelines for Using EAP-FAST as Authentication Protocol, page 19-11](#)

- [Configuring EAP-FAST Settings, page 19-11](#)
- [Generating the PAC for EAP-FAST, page 19-12](#)
- [Configuring EAP-TLS Settings, page 19-12](#)
- [Configuring PEAP Settings, page 19-13](#)
- [Configuring RADIUS Settings, page 19-13](#)

Guidelines for Using EAP-FAST as Authentication Protocol

The following are a few guidelines for using EAP-FAST as an authentication protocol:

- It is highly recommended to enable EAP-TLS inner method when the EAP-FAST accept client certificate is enabled on authenticated provisioning. EAP-FAST accept client certificate on authenticated provisioning is not a separate authentication method, but a shorter form of client certificate authentication that uses the same certificate credentials type to authenticate a user, but does not require to run an inner method.
- Accept client certificate on authenticated provisioning works with PAC-less full handshake and authenticated PAC provisioning. It does not work for PAC-less session resume, anonymous PAC provisioning, and PAC-based authentication.
- EAP attributes are displayed per identity (so in EAP chaining displayed twice) are shown in authentication details in monitoring tool in order user then machine even if authentication happens in different order.
- When EAP-FAST authorization PAC is used then EAP authentication method shown in live logs is equal to the authentication method used for full authentication (as in PEAP) and not as Lookup.
- In EAP chaining mode when tunnel PAC is expired then ISE falls back to provisioning and AC requests User and Machine authorization PACs - Machine Authorization PAC cannot be provisioned. It will be provisioned in the subsequent PAC-based authentication conversation when AC requests it.
- When Cisco ISE is configured for chaining and AC for single mode then AC response with IdentityType TLV to ISE. However, the second identity authentication fails. You can see from this conversation that client is suitable to perform chaining but currently is configured for single mode.
- Cisco ISE supports retrieval attributes and groups for both machine and user in EAP-FAST chaining only for AD. For LDAP and Internal DB ISE uses only the last identity attributes.
- For EAP-TLS to perform machine authentication, it is required to use binary certificate comparison: **Administration > External Identity Sources > Certificate authenticatoin profiles > Pick a profile > “Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory”** needs to be checked. Also, a certificate needs to be present in that AD or LDAP.

Configuring EAP-FAST Settings

You can configure the runtime characteristics of the EAP-FAST protocol from the Global Options page.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Administration > System > Settings > Protocols**.

- Step 2** Choose **EAP-FAST > EAP Fast Settings**.
- Step 3** Enter the details as required to define the EAP-FAST protocol.
- Step 4** Click **Revoke** if you want to revoke all the previously generated master keys and PACs.
- Step 5** Click **Save** to save the EAP-FAST settings.
-

Related Topics

- [EAP-FAST Settings, page A-22](#)
- [Generating the PAC for EAP-FAST, page 19-12](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

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.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

- 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**.
- Step 4** Enter the details as required to generate machine PAC for the EAP-FAST protocol.
- Step 5** Click **Generate PAC**.
-

Related Topics

- [Generate PAC for EAP-FAST Settings, page A-22](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Configuring EAP-TLS Settings

You can configure the runtime characteristics of the EAP-TLS protocol from the Global Options page.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

- Step 1** Choose **Administration > System > Settings**.
- Step 2** From the Settings navigation pane on the left, click **Protocols**.
- Step 3** Choose **EAP-TLS**.
- Step 4** Enter the details as required to define the EAP-TLS protocol.

- Step 5** Click **Save** to save the EAP-TLS settings.
-

Related Topics

- [EAP-TLS Settings, page A-23](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Configuring PEAP Settings

You can configure the runtime characteristics of the PEAP protocol from the Global Options page.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

- Step 1** Choose **Administration > System > Settings**.
- Step 2** From the Settings navigation pane on the left, click **Protocols**.
- Step 3** Choose **PEAP**.
- Step 4** Enter the details as required to define the PEAP protocol.
- Step 5** Click **Save** to save the PEAP settings.
-

Related Topics

- [PEAP Settings, page A-23](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Configuring RADIUS Settings

You can configure the RADIUS settings to detect the clients that fail to authenticate and to suppress the repeated reporting of successful authentications.

- Step 1** Choose **Administration > System > Settings**.
- Step 2** From the Settings navigation pane, click **Protocols**.
- Step 3** Choose **RADIUS**.
- Step 4** Enter the details as required to define the RADIUS settings.
- Step 5** Click **Save** to save the settings.
-

Related Topics

- [RADIUS Settings, page A-24](#)

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:

- [Defining Allowed Protocols for Network Access, page 19-14](#)
- [Cisco ISE Acting as a RADIUS Proxy Server, page 19-18](#)

Related Topics

- [Simple Authentication Policies, page 19-4](#)
- [Configuring a Rule-Based Authentication Policy, page 19-22](#)

Defining Allowed Protocols for Network Access

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.

Before You Begin

Before you begin this procedure, you should have a basic understanding of the protocol services that are used for authentication.

Review the [Cisco ISE Authentication Policies](#) to understand authentication type and the protocols that are supported by various databases.

Review the [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 for Authentication” section on page 19-10](#) for more information.

To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy > Policy Elements > Results > Authentication > Allowed Protocols**.

If Cisco ISE is set to operate in FIPS mode, some protocols are disabled by default and cannot be configured.

Step 2 Click **Add**.

Step 3 Enter the required information.

Step 4 Select the appropriate authentication protocols and options for your network.

Step 5 If you choose to use PACs, make the appropriate selections.

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 6 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.

You can now create a simple or rule-based authentication policy.

If you disable EAP-MSCHAP as inner method and enable EAP-GTC and EAP-TLS inner methods for PEAP or EAP-FAST, ISE starts EAP-GTC inner method during inner method negotiation. Before the first EAP-GTC message is sent to the client, ISE executes identity selection policy to obtain GTC password prompt from the identity store. During the execution of this policy, Network Access:EapAuthentication attribute is equal to EAP-GTC. If EAP-GTC inner method is rejected by the client and EAP-TLS is negotiated, identity store policy is not executed again. In case identity store policy is based on Network Access:EapAuthentication attribute, it might have unexpected results since the real EAP authentication is EAP-TLS but was set after identity policy evaluation.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Allowed Protocols Services Settings, page B-19](#)
- [PAC Options, page B-22](#)
- [Guidelines for Using EAP-FAST as Authentication Protocol, page 19-11](#)

Enabling MAB from Non-Cisco Devices

Configure the following settings sequentially, as described in [Table 19-2](#) to configure MAB from non-Cisco devices.

Table 19-2 *Settings for Enabling MAB from Non-Cisco Devices*

	Task	More Information
Step 1	Ensure that the MAC address of the endpoints that are to be authenticated are available in the Endpoints database. You can add these endpoints or have them profiled automatically by the Profiler service.	See the “Creating a Network Device Definition in Cisco ISE” section on page 9-3 for more information.
Step 2	Create an Allowed Protocol service based on the type of MAC authentication used by the non-Cisco device (PAP, CHAP, or EAP-MD5). 1. Choose Policy > Policy Elements > Results > Authentication > Allowed Protocols. 2. Enter a name for the Allowed Protocol service. For example, MAB for NonCisco Devices 3. Select the protocol based on the MAC authentication type used by the non-Cisco device: – PAP—Check the Allow PAP/ASCII check box and check the Detect PAP as Host Lookup check box. – CHAP—Check the Allow CHAP check box and check the Detect CHAP as Host Lookup check box. – EAP-MD5—Check the Allow EAP-MD5 check box and check Detect EAP-MD5 as Host Lookup check box. For each of the protocol listed above, it is recommended to check the following check boxes: – Check Password—Enable this for checking of the trivial MAB password to authenticate the sending network device. – Check Calling-Station-Id equals MAC address—Enable this as an extra security check, when Calling-Station-Id is being sent. 4. Save the Allowed Protocol service.	See Defining Allowed Protocols for Network Access and Allowed Protocols Services Settings for details.
Step 3	Configure an authentication policy rule for enabling MAB from non-Cisco devices. 1. Choose Policy > Authentication. 2. Select the Rule-Based authentication policy. 3. Insert a new rule for MAB. 4. Select the Allowed Protocol service (MAB for NonCisco Devices) that you created in Step 2 in this rule. 5. Select the Internal Endpoints database as the Identity Source in this rule. 6. Save the authentication policy.	See Configuring a Rule-Based Authentication Policy , page 19-22 for more information.

Enabling MAB from Cisco Devices

Configure the following settings sequentially, as described in [Table 19-3](#) to configure MAB from Cisco devices.

Table 19-3 Settings for Enabling MAB from Cisco Devices

	Task	More Information
Step 1	Ensure that the MAC address of the endpoints that are to be authenticated are available in the Endpoints database. You can add these endpoints or have them profiled automatically by the Profiler service.	See the “Creating a Network Device Definition in Cisco ISE” section on page 9-3 for more information.
Step 2	Create an Allowed Protocol service based on the type of MAC authentication used by the Cisco device (PAP, CHAP, or EAP-MD5). 1. Choose Policy > Policy Elements > Results > Authentication > Allowed Protocols. 2. Enter a name for the Allowed Protocol service. For example, MAB for Cisco Devices. 3. Check the Process Host Lookup check box. 4. Select the protocol based on the MAC authentication type used by the Cisco device: – PAP—Check the Allow PAP/ASCII check box and check the Detect PAP as Host Lookup check box. – CHAP—Check the Allow CHAP check box and check the Detect CHAP as Host Lookup check box. – EAP-MD5—Check the Allow EAP-MD5 check box and check Detect EAP-MD5 as Host Lookup check box. For each of the protocol listed above, it is recommended to check the following check boxes: – Check Password—Enable this for checking of the trivial MAB password to authenticate the sending network device. – Check Calling-Station-Id equals MAC address—Enable this as an extra security check, when Calling-Station-Id is being sent. 5. Save the Allowed Protocol service.	See Defining Allowed Protocols for Network Access and Allowed Protocols Services Settings for details.
Step 3	Configure an authentication policy rule for enabling MAB from Cisco devices. 1. Choose Policy > Authentication. 2. Select the Rule-Based authentication policy. 3. Insert a new rule for MAB. 4. Select the Allowed Protocol service (MAB for Cisco Devices) that you created in Step 2 in this rule. 5. Select the Internal Endpoints database as the Identity Source in this rule. 6. Save the authentication policy.	See Configuring a Rule-Based Authentication Policy , page 19-22 for more information.

Cisco ISE Acting as a RADIUS Proxy Server

Cisco ISE can function both as a RADIUS server and as a RADIUS proxy server. When it acts as a proxy server, Cisco ISE receives authentication and accounting requests from the network access server (NAS) and forwards them to the external RADIUS server. Cisco ISE accepts the results of the requests and returns them to the NAS.

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. The 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. In both simple and rule-based authentication policies, you can use the RADIUS server sequences to proxy the requests to a RADIUS server.

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:

- [Configuring External RADIUS Servers, page 19-18](#)
- [Defining RADIUS Server Sequences, page 19-19](#)

Configuring External RADIUS Servers

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.

Before You Begin

- 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 [“RADIUS Server Sequence” section on page 19-19](#).

- To perform the following task, you must be a Super Admin or System Admin.

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 required.

Step 4 Click **Submit** to save the external RADIUS server configuration.

Related Topics

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

RADIUS Server Sequence

RADIUS server sequences in Cisco ISE allow you to proxy requests from a NAD to an external RADIUS server that will process the request and return the result to Cisco ISE, which forwards the response to the NAD.

RADIUS Server Sequences 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.

Related Topics

- [Cisco ISE Acting as a RADIUS Proxy Server, page 19-18](#)
- [Defining RADIUS Server Sequences, page 19-19](#)
- [Configuring External RADIUS Servers, page 19-18](#)

Defining RADIUS Server Sequences

You can add RADIUS Server Sequences from this page.

Before You Begin

- Before you begin this procedure, you should have a basic understanding of the [Proxy Service](#) and must have successfully completed the task for [Configuring External RADIUS Servers](#).
- To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > Network Resources > RADIUS Server Sequences .
Step 2	Click Add .
Step 3	Enter the values as required.
Step 4	Click Submit to save the RADIUS server sequence to be used in policies.
-

What to do Next

See the “[Configuring a Rule-Based Authentication Policy](#)” section on [page 19-22](#) for information on how to configure a simple authentication policy using the RADIUS server sequence that you created.

Related Topics

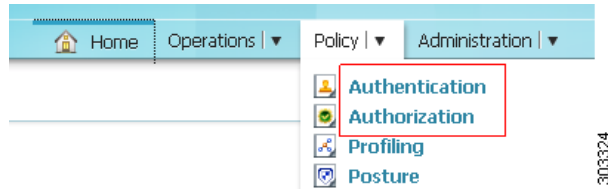
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [RADIUS Server Sequence, page 19-19](#)

Policy Modes

Cisco ISE provides two types of policy modes, the Simple mode and the Policy Set mode. You can select either one of these to configure authentication and authorization policies. When you change the policy mode, you are prompted to login again to the Cisco ISE interface. If you switch from the Policy Set mode to the Simple mode, all the policy set data is deleted except the default policy. The Policy menu options change based on the policy mode selection.

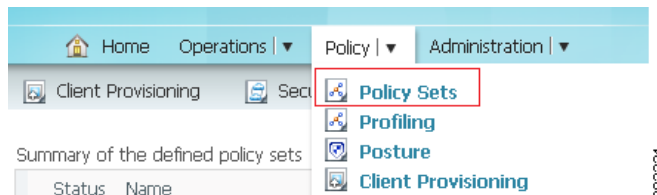
- Simple Mode—If you select Simple mode, you can define authentication and authorization policies separately in the Policy menu.

Figure 19-3 Simple Mode Policy Menu



- Policy Set Mode—If you select Policy Set mode, you can create policy sets and logically group authentication and authorization within the same group. You can have several groups based on what you need.

Figure 19-4 Policy Set Mode Policy Menu



Related Topics

- [Guidelines for Changing Policy Modes, page 19-20](#)
- [Changing Policy Modes, page 19-21](#)
- [Simple Authentication Policies, page 19-4](#)
- [Configuring a Rule-Based Authentication Policy, page 19-22](#)
- [Policy Sets, page 19-23](#)
- [Managing Authorization Policies and Profiles](#)

Guidelines for Changing Policy Modes

The following are the guidelines for changing the policy modes:

- After you do a fresh install or upgrade from Cisco ISE, Release 1.1, the Simple Mode policy model is selected by default.
- If you choose to switch to Policy Set Mode from Simple Mode, the authentication and authorization policies are migrated to the default policy set.
- If you choose to switch to Simple Mode from Policy Set Mode, the authentication and authorization of the default policy set are migrated to be the authentication and authorization policies. All other policy set policies are deleted.

Changing Policy Modes

You can use this page to change the policy modes.

Step 1 Choose **Administration > System > Settings > Policy Sets**.

Step 2 Enable or Disable the Policy Set mode.

Step 3 Click **Save**.

You will be prompted to login again, for the new policy mode to come into effect.

Related Topics

- [Simple Authentication Policies, page 19-4](#)
- [Rule-Based Authentication Policies, page 19-6](#)
- [Policy Sets, page 19-23](#)
- [Managing Authorization Policies and Profiles](#)

Configuring a 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 for Network Access](#)” section on page 19-14 for information on how to create an allowed protocols service.

Before You Begin

- Before you begin this procedure, you should have successfully completed the task for [Defining Allowed Protocols for Network Access](#).
- 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 [RADIUS Server Sequence](#).
- To configure a simple authentication policy using the RADIUS server sequence, you should have a basic understanding of the [Cisco ISE Authentication Policies](#) to understand authentication type and the protocols that are supported by various databases.
- To perform the following task, you must be a Super Admin or System Admin.

You can also use this process to configuring a simple policy using RADIUS server sequence.

Step 1 Choose **Policy > Authentication**.

Step 2 Click OK on the message that appears.

Step 3 Enter the values as required.

Step 4 Click **Save** to save your simple authentication policy.

Related Topics

- [Simple Authentication Policy Configuration Settings, page B-1](#)

- [Cisco ISE Authentication Policies](#), page 19-1
- [Cisco ISE Acting as a RADIUS Proxy Server](#), page 19-18
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Configuring a Rule-Based Authentication Policy

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. See [Table 19-1 lists the fixed attributes that are supported by dictionaries, which can be used in policy conditions.](#), page 19-8.



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 [“Cisco ISE Acting as a RADIUS Proxy Server”](#) section on page 19-18 for more information.

Before You Begin

- Before you begin this task, you should have a basic understanding of the [“Rule-Based Authentication Policies”](#) section on page 19-6, have read the [“Configuring a Rule-Based Authentication Policy”](#) section on page 19-22, and have completed the following tasks successfully:
 - [Defining Allowed Protocols for Network Access](#)
 - [Creating Identity Source Sequences](#) if you want to use an identity source sequence
 - [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 19-26 for more information on these predefined policies. You can edit these policies to suit your requirements.
- To perform the following task, you must be a Super Admin or System Admin.
- If your users are defined in external identity sources, ensure that you have configured these identity sources in Cisco ISE. See [Chapter 14, “Managing Users and External Identity Sources”](#) for information on how to configure the external identity sources.



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.

-
- Step 1** Choose **Policy > Authentication**.
- Step 2** Click the **Rule-Based** radio button.
- Step 3** Click OK on the message that appears.

- Step 4** 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** Enter the values as required to create a new authentication policy.
- Step 6** Click **Save** to save your rule-based authentication policies.
-

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.

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.

You cannot specify the “UserName” attribute when configuring an authentication policy when the EAP-FAST client certificate is sent in the outer TLS negotiation. Cisco recommends using certificate fields like “CN” and “SAN,” for example.

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.

Related Topics

- [Rule-Based Authentication Policy Configuration Settings, page B-2](#)
- [Cisco ISE Authentication Policies, page 19-1](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Policy Sets

Policy sets enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type and similar parameters.

Policy sets are first-match policies. Each policy has a condition that can be a simple or a compound condition, and have the following supported dictionaries:

- Airspace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Device, Microsoft
- NetworkAccess
- RADIUS

Once the policy set is matched and selected, its authentication and authorization policies are evaluated. In addition, a global authorization exception policy is available as part of the policy set model.

There is always one policy set defined, which is the default policy set.

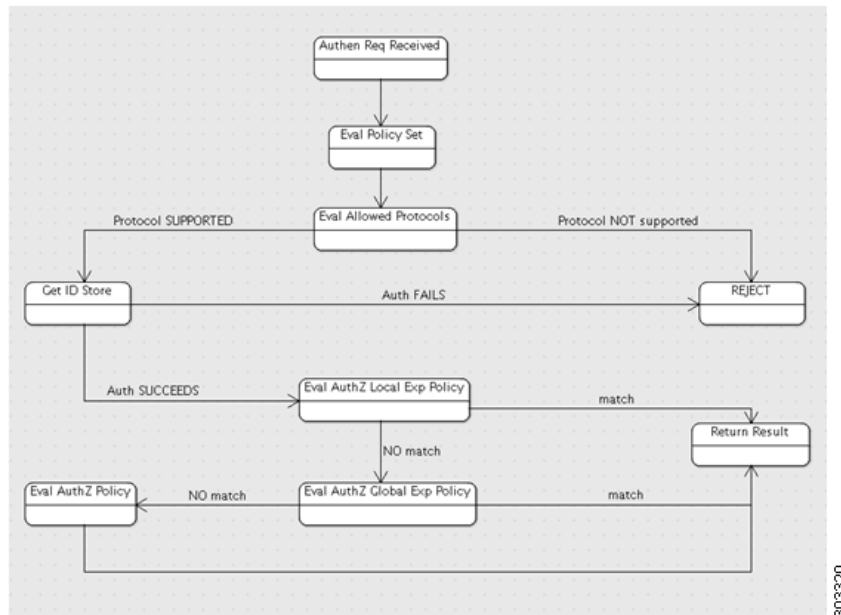
Related Topics

- [Policy Set Evaluation Flow, page 19-24](#)

- [Guidelines for Creating Policy Sets, page 19-25](#)
- [Global Authorization Exception Policy, page 19-25](#)
- [Configuring Policy Sets, page 19-25](#)

Policy Set Evaluation Flow

Figure 19-5 Policy Set Authentication and Authorization Evaluation Flow



The sequence of policy set and the authentication and authorization evaluation flow is as follows:

1. Evaluate policy set (by evaluating the policy set condition). As a result, one policy set is selected.
2. Evaluate allowed protocols rules of the selected policy set.
3. Evaluate ID store rules of the selected policy set.
4. Evaluate authorization rules of the selected policy set, based on the following paradigm:
 - a. Evaluate the local exception policy in case it is defined
 - b. If no match is found in Step 1 above, evaluate global exception policy if defined
 - c. If no match is found in Step 2 above, evaluate authorization rules

If none of the policy set matches, the default policy set will be selected.

Guidelines for Creating Policy Sets

The following are the guidelines for creating policy sets:

- Rules should be specified with names, conditions, and results. You cannot save a policy set as long as all the authentication and authorization rules are not defined.
- You can duplicate rules as long as they are from the same rule type (authentication or authorization) and only from the same policy set.
- Rules cannot be shared by different policy sets; each policy set has its own rule, however conditions can be shared in case you use the condition library.

Global Authorization Exception Policy

The global authorization exception policy allows you to define rules that apply to all policy sets. The global authorization exception policy is added to each authorization policy of all the policy set. Global authorization exception policy can be updated by selecting the Global Exceptions option from the policy set list.

Each authorization policy can have local exception rule, global exception rule, and regular rules. Once you configure the local authorization exception rule, (for some authorization policies) the global exception authorization rules are displayed in read-only mode in conjunction to the local authorization exception rule. The local authorization exception rule can overwrite the global exception rule. The authorization rules are processed in the following order: first the local exception rule, then the global exception rule, and finally, the regular rule of the authorization policy.

Configuring Policy Sets

You can use this page to configure Policy sets.

Before You Begin

You should have selected the policy mode as Policy Set to be able to configure Policy sets. To do this, go to **Administration > System > Settings > Policy Sets**.

-
Step 1	Choose Policy > Policy Sets .
Step 2	Click the Default policy. The default policy is displayed in the right.
Step 3	Click the plus (+) sign on top and choose Create Above .
Step 4	Enter the name, description and a condition for this group policy.
Step 5	Define the authentication policy.
Step 6	Define the authorization policy.
Step 7	Click Submit . After you configure a policy set, Cisco ISE logs you out. You must log in again to access the Admin portal.
-

Related Topics

- [Changing Policy Modes, page 19-21](#)
- [Configuring a Rule-Based Authentication Policy, page 19-22](#)

- [“Configuring Authorization Policies” section on page 20-8](#)
- [Policy Set Evaluation Flow, page 19-24](#)
- [Guidelines for Creating Policy Sets, page 19-25](#)
- [Global Authorization Exception Policy, page 19-25](#)

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 19-4](#) describes the defaults that relate to authentication policies.

Table 19-4 Authentication Policy Configuration Defaults

Name	Path in the User Interface	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 19-4 Authentication Policy Configuration Defaults (continued)

Name	Path in the User Interface	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 a 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. See Network 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 a 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. See Network 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.
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

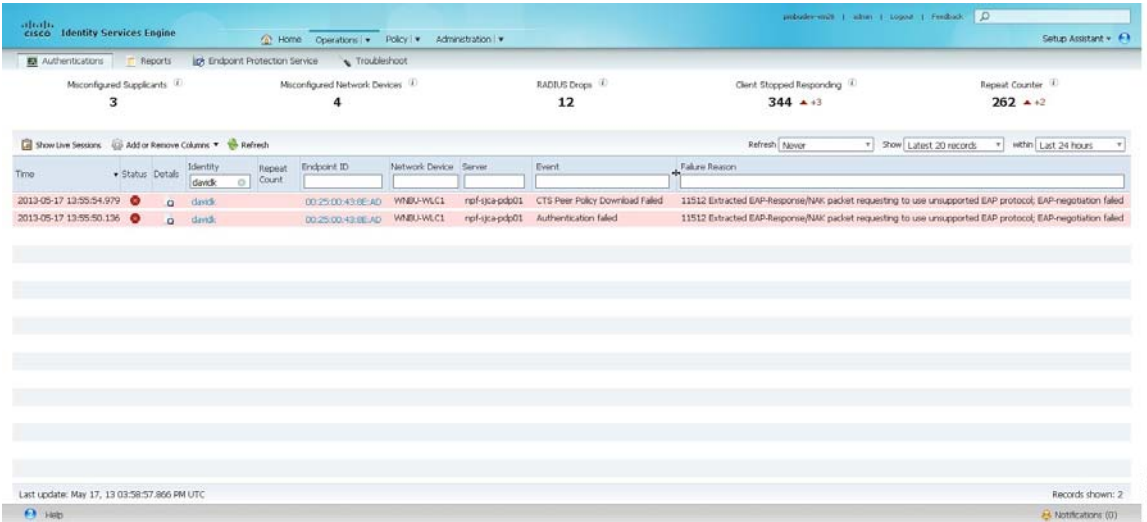
Cisco ISE provides various ways to view real-time authentication summary.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

- Step 1** Choose **Operations > Authentications** to view real-time authentication summary. A page similar to the one shown in [Figure 19-6](#) appears.

Figure 19-6 *Live Authentications Page*

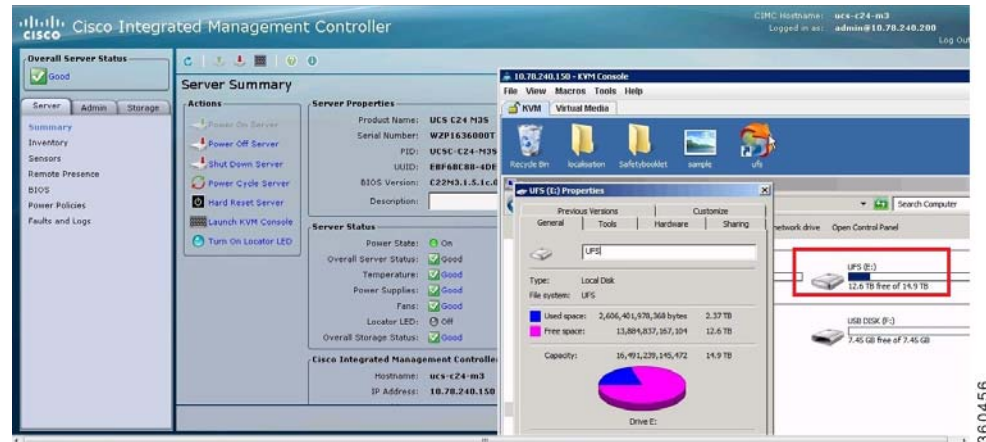


- Step 2** You can view the authentication summary in the following ways:
- Hover your mouse cursor over the Status icon to view the results of the authentication and a brief summary. A pop-up that is similar to the one shown in [Figure 19-6](#) appears.
 - Enter your search criteria in any one or more of the text boxes that appear at the top of the list, and press **Enter**, to filter your results.
 - Click the magnifier icon in the Details column to view a detailed report.

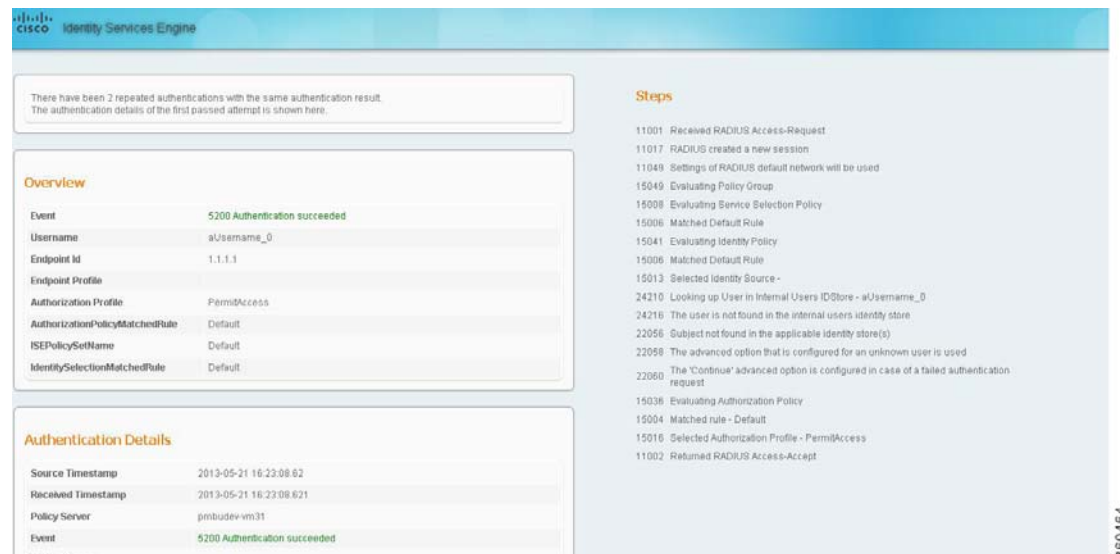


Note As the Authentication Summary report or dashboard collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.

- Step 3** Click **Show Live Sessions** to view the real-time session summary. A page similar to the one shown in [Figure 19-7](#) appears.

Figure 19-7 *Live Sessions Page*

Step 4 Click the **Details** icon corresponding to the desired entry in the Live Session page to view the drill-down report of the live authentications. A page similar to the one shown in [Figure 19-8](#) appears.

Figure 19-8 *Live Authentication Details Drill-down Report*

Related Topics

[Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Authentication Dashlet

The Cisco ISE dashboard provides a summary of all authentications that take place in your network. It provides at-a-glance information about authentications and authentication failures in the Authentications dashlet.

The Authentications dashlet provide the following statistical information about the RADIUS authentications that Cisco ISE has handled:

- 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 of failed RADIUS authentications requests that Cisco ISE has processed.

For information on dashboard and dashlets and how to access more information, see the [“Cisco ISE Dashboard” section on page 25-2](#) and [Monitoring Database, page 25-29](#).

Authentication Reports and Troubleshooting Tools

Apart from the authentication details, Cisco ISE provides various reports and troubleshooting tools that you can use to efficiently manage your network.

There are various 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. The following is a list of authentication reports:

- AAA Diagnostics
- RADIUS Accounting
- RADIUS Authentication
- Authentication Summary

For more information on how to generate and use reports, see [Chapter 26, “Reporting.”](#)



Managing Authorization Policies and Profiles

Authorization policies are used when creating authorization profiles in Cisco Identity Services Engine (Cisco ISE).

An authorization policy is composed of authorization rules. Authorization rules have three elements: name, attributes, and permissions. The permissions element 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:

- [Cisco ISE Authorization Policies, page 20-1](#)
- [Authorization Policies and Supported Dictionaries, page 20-4](#)
- [Configuring Authorization Policies, page 20-8](#)
- [Permissions for Authorization Profiles, page 20-10](#)
- [Downloadable ACLs, page 20-11](#)
- [Machine Access Restriction for Active Directory User Authorization, page 20-13](#)

Cisco ISE Authorization Policies

Authorization policies are a component of the Cisco ISE network authorization service. This service allows you to define authorization policies and configure authorization profiles for specific users and groups that access your network resources.

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”).

Related Topic

- For more information on endpoint identity groups, see [Identified Endpoints Grouped in Endpoint Identity Groups, page 21-42](#).

Cisco ISE Authorization Profiles

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 and network access is authorized accordingly.

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.

Related Topics

- [Authorization Policy Terminology, page 20-2](#)
- [Authorization Policies and Supported Dictionaries, page 20-4](#)
- [Configuring Authorization Policies, page 20-8](#)
- [Chapter 18, “Setting Up Policy Conditions”](#)
- [Permissions for Authorization Profiles, page 20-10](#)
- [Configuring Permissions for Downloadable ACLs, page 20-13](#)

Authorization Policy Terminology

The following is basic terminology used for Cisco ISE authorization policies and profiles:

- [Authorization Profile, page 20-3](#)
- [Authorization Policy, page 20-3](#)
- [Access Control Lists, page 20-4](#)
- [Network Authorization, page 20-2](#)
- [Policy Elements, page 20-3](#)

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 RADIUS access to the Cisco ISE network and its resources.

Policy Elements

Policy elements are components that define an authorization policy and are as follows:

- Rule name
- Identity groups
- Conditions
- 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

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 conditions 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—Standard policies are policies created to remain in effect for long periods of time, to apply to a larger group of users, devices, or groups, and to 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 that you modify 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 user groups, devices, or network groups.

- **Exception**—By contrast, exception policies are appropriately named because this type of policy acts as an exception to the standard policies. Exception policies are intended for authorizing limited access that is based on a variety of factors, such as 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 access control list (ACL) in 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 (such as, Permit or Deny). Cisco ISE also uses downloadable ACL (DACLS).

Authorization Policies and Supported Dictionaries

For both simple and compound authorization policy types, the verification must comply with the authorization profiles to be returned.

Verifications typically include one or more conditions 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:

- System-defined dictionary:
 - RADIUS
- RADIUS-vendor dictionaries
 - Airespace
 - Cisco
 - Cisco-BBSM
 - Cisco-VPN3000
 - Microsoft

See the [“Dictionaries and Dictionary Attributes” section on page 10-1](#) for more information on Cisco ISE dictionaries.

Guidelines for Configuring Authorization Policies and Profiles

Observe the following guidelines when managing or administering authorization policies and profiles:

- Rule names you create must use only the following supported characters:
 - 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 characters:
 - 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).
- Make sure that you click **Save** to save the new or modified policy or profile in the Cisco ISE database.

Default Authorization Policy, Rule, and Profile Configuration

The Cisco ISE software comes installed with a number of preinstalled 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 20-1](#).

Table 20-1 Authorization Policy, Profile, and Rule Configuration Defaults

Name	Path in the User Interface	Description	Additional Information
Authorization Policy Configuration Defaults			
Default Compound Conditions for Authorization Policies	Policy > Policy Elements > Conditions > Authorization	These are preinstalled 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 20-1 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the User Interface	Description	Additional Information
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.
Authorization Profile Configuration Defaults			
Blacklist_Access	Policy > Policy Elements > Results > Authorization Profiles > Blacklist_Access	This authorization profile rejects access to devices that are blacklisted. All blacklisted devices are redirected to the following URL: url-redirect=https://ip:port/mydevices/blackhole.jsp	This default authorization profile is applied for all endpoints that are declared as “lost” in the My Devices Portal.
Cisco_IP_Phones	Policy > Policy Elements > Results > Authorization Profiles > Cisco_IP_Phones	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).

Table 20-1 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the User Interface	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.
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 must 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.
Black List Default Authorization Rule	Policy > Authorization Policy	This authorization policy uses a configuration default rule with the following values: • Rule Name: Black List Default • Endpoint Identity Group: Blacklist • Conditions: Any • Permissions/Authorization Profile: Blacklist_Access	This default rule is designed to appropriately provision “lost” user devices until they are either removed from the system or “reinstated.”

Table 20-1 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the User Interface	Description	Additional Information
Profiled Cisco IP Phones 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 • Permissions/Authorization Profile: Cisco_IP_Phones	This default rule uses Cisco IP Phones as its default endpoint identity group and the values listed in this table.
Authorization Rule Configuration Defaults			
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 default rule uses “any” as its default endpoint identity group and the values listed in this table.

Configuring Authorization Policies

The Authorization Policy page lets you display, create, duplicate, modify, or delete authorization policies. 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.

Before You Begin

Before you begin this procedure, you should have a basic understanding of simple and rule-based conditions, the basic building blocks of identity groups, conditions, and permissions, and how they are used in the Admin portal.

-
- Step 1** Choose **Policy > Authorization > Standard**.
- Step 2** Click the down arrow on the far-right and select either **Insert New Rule Above** or **Insert New Rule Below**.
- Step 3** Enter the rule name and select identity group, condition, attribute and permission for the authorization policy.
- Not all attributes you select will include the “Equals,” “Not Equals,” “Matches,” “Starts With,” or “Not Starts With” operator options.
- The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

Step 4 Click **Done**.

Step 5 Click **Save** to save your changes to the Cisco ISE system database and create this new authorization policy.

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 in which the authentication succeeded.
- When an identity source sequence is used 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 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”.

Related Topics

- [Authorization Policy Settings, page B-5](#)
- [Simple and Compound Conditions, page 18-1](#)
- [Creating Simple Conditions, page 18-2](#)
- [Creating Compound Conditions, page 18-3](#)

Time and Date Conditions

Use the Policy Elements Conditions page 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 directed by the attribute settings you make.

Related Topics

- [Creating Time and Date Conditions, page 18-8](#)
- [Time and Date Condition Settings, page B-17](#)

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 page
- Know the basic guidelines to follow when configuring policies and profiles
- Understand what comprises permissions in an authorization profile
- Are aware of configuration default values that are described in the following topics:
 - [Authorization Policies and Supported Dictionaries, page 20-4](#)
 - [Guidelines for Configuring Authorization Policies and Profiles, page 20-4](#)
 - [Default Authorization Policy, Rule, and Profile Configuration, page 20-5](#)

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 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 must enter the value for the Common Tasks attributes, which Cisco ISE translates to the underlying RADIUS values.

Related Topic

[Configuring Permissions for New Standard Authorization Profiles, page 20-10](#)

Configuring Permissions for New Standard Authorization Profiles

Use the Authorization profiles page to create a new standard authorization profile and configure its permissions.

-
Step 1	Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles .
Step 2	Click Add .

- Step 3** Enter values as required to configure a new authorization profile. Supported characters for the name field are: space, ! # \$ % & ' () * + , - . / ; = ? @ _ { .
- Step 4** Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.

Related Topics

[Authorization Profile Settings, page B-23](#)

Downloadable ACLs

You can define DACLs for the Access-Accept message to return. Use ACLs to prevent unwanted traffic from entering the network. ACLs can filter source and destination IP addresses, transport protocols, and more by using the RADIUS protocol.

After you create DACLs as named permission objects, you can add them to authorization profiles, which you can then specify as the result of an authorization policy.

You can duplicate a DACL if you want to create a new DACL that is the same, or similar to, an existing downloadable ACL.

After duplication is complete, you access each DACL (original and duplicated) separately to edit or delete them.



Note

While creating DACL, the keyword *Any* must be the source in all ACE in DACL. Once the DACL is pushed, the *Any* in the source is replaced with the IP address of the client that is connecting to the switch.

Related Topic

[Configuring Permissions for Downloadable ACLs, page 20-13](#)

[Supported DACL Format, page 20-11](#)

Supported DACL Format

The following is the supported format for DACL referenced by an inline posture authorization profile:

- **ACTION PROTOCOL SOURCE_SUBNET WILDCARD_MASK [OPERATOR [PORT]] DEST_SUBNET WILDCARD_MASK [OPERATOR [PORT]] [ICMP_TYPE_CODE]**

Table 20-2 describes the options in the DACL format.

Table 20-2 **DACL Format - Options**

Option	Description
ACTION	Specifies whether the policy element permissions should permit or deny access.
PROTOCOL	Specifies any one of the following protocols: • ICMP • UDP • TCP • IP
SOURCE_SUBNET	Specifies any one of the following source subnet formats: • any • host x.x.x.x • <subnet>
DEST_SUBNET	Specifies any one of the following destination subnet formats: • any • host x.x.x.x • <subnet>
WILDCARD_MASK	Specifies the inverse of the subnet mask. For example, 0.0.0.255.
OPERATOR	Specifies any one of the following operators: • eq • lt • gt • neq • range
<i>PORT</i>	Specifies the port. The valid range is from 1 to 65535.
<i>ICMP_TYPE_CODE</i>	Specifies any one of the following ICMP type codes: • 0—Echo reply • 8—Echo request • 3:[0-15]—Destination unreachable • 5:[0-3]—ICMP redirects

Examples of acceptable ACL Format:

permit tcp any host 192.168.1.100 eq 80—permits www traffic from anywhere to host 192.168.1.100

permit udp any eq 68 any eq 67—permits dhcp traffic

permit icmp any any 8, permit icmp any any 0—allows icmp echo-request and echo-reply

deny icmp any any 5:0—denies icmp network redirects

permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255—permits all traffic from 192.168.2.0 subnet to 192.168.1.0 subnet

permit udp any any range 16384 32767—permits voice traffic using range of udp ports

Examples of incorrect syntax:

permit ip 192.168.2.100 192.168.1.100—host/wildcard keyword missing

permit tcp host 192.168.2.100 host 192.168.1.100 eq 88 389 636 454 3268 3269 1025 1026 (You cannot club multiple ports using eq operator, and this ACL needs to be split into multiple lines one for each destination port)



Note

Ensure that there are no empty spaces or hidden characters in the DACL syntax. Any unknown characters, if exists in the DACL syntax, the Inline Posture node will not accept the DACL. For more information, refer to the Inline Posture logs.

Configuring Permissions for Downloadable ACLs

Use the Downloadable ACLs page to create a new DACL and configure its permissions.

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
 - Step 2** Click the **action** icon and select **Create DACL** or click **Add** in the DACL Management page.
 - Step 3** Enter the desired values for the DACL. Supported characters for the name field are: space, ! # \$ % & ' () * + , - . / ; = ? @ _ { .
 - Step 4** Click **Submit**.
-

Related Topic

[Downloadable ACLs, page 20-11](#)

Machine Access Restriction for Active Directory User Authorization

Cisco ISE 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 is 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 is assigned.

Related Topics

[User and Machine Authentication in Active Directory, page 14-9](#)



Cisco ISE Endpoint Profiling Policies

This chapter describes how Cisco ISE profiles endpoints that connect to a Cisco ISE network, and how you can create profiling policies to manage these endpoints and grant them access to the resources in your network.

This chapter covers the following topics:

- [Cisco ISE Profiling Service, page 21-1](#)
- [Configuring Profiling Service in Cisco ISE Nodes, page 21-3](#)
- [Network Probes Used by Profiling Service, page 21-4](#)
- [Configuring Probes per Cisco ISE Node, page 21-13](#)
- [Setting up COA, SNMP RO Community and Endpoint Attribute Filter, page 21-15](#)
- [Attribute Filters for ISE Database Persistence and Performance, page 21-18](#)
- [Attributes Collection from IOS Sensor Embedded Switches, page 21-20](#)
- [Endpoint Profiling Policy Rules, page 21-22](#)
- [Endpoint Profiling Policies Grouped into Logical Profiles, page 21-28](#)
- [Cisco ISE Integration with Cisco NAC Appliance, page 21-33](#)
- [Identified Endpoints, page 21-40](#)
- [Identified Endpoints Grouped in Endpoint Identity Groups, page 21-42](#)
- [Profiler Feed Service, page 21-44](#)
- [Profiler Reports, page 21-47](#)

Cisco ISE Profiling Service

The profiling service in Cisco Identity Services Engine (ISE) identifies the devices that connect to your network and their location. The endpoints are profiled based on the endpoint profiling policies configured in Cisco ISE. Cisco ISE then grants permission to the endpoints to access the resources in your network based on the result of the policy evaluation.

The profiling service:

- 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.

Related Topics

- [Endpoint Inventory Using Profiling Service, page 21-2](#)
- [Cisco ISE Profiler Queue Limit Configuration, page 21-2](#)

Endpoint Inventory Using Profiling Service

You can use the profiling service to discover, locate, and determine the capabilities of all the endpoints connected to your network. You can ensure and maintain appropriate access of endpoints to the enterprise network, regardless of their device types.

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. All the attributes that are handled by the profiling service need to be defined in the profiler dictionaries.

The profiling service identifies each endpoint on your network, and groups those endpoints according to their profiles to an existing endpoint identity group in the system, or to a new group that you can create in the system. By grouping endpoints, and applying endpoint profiling policies to the endpoint identity group, you can determine the mapping of endpoints to the corresponding endpoint profiling policies.

Cisco ISE Profiler Queue Limit Configuration

Cisco ISE profiler collects a significant amount of endpoint data from the network in a short period of time. It causes Java Virtual Machine (JVM) memory utilization to go up due to accumulated backlog when some of the slower Cisco ISE components process the data generated by the profiler, which results in performance degradation and stability issues.

To ensure that the profiler does not increase the JVM memory utilization and prevent JVM to go out of memory and restart, limits are applied to the following internal components of the profiler:

- **Endpoint Cache**—Internal cache is limited in size that has to be purged periodically (based on least recently used strategy) when the size exceeds the limit.
- **Forwarder**—The main ingress queue of endpoint information collected by the profiler.
- **Event Handler**—An internal queue that disconnects a fast component, which feeds data to a slower processing component (typically related to a database query).

Endpoint Cache

For example,

- `maxEndPointsInLocalDb = 100000` (endpoint objects in cache)
- `endPointsPurgeIntervalSec = 300` (endpoint cache purge thread interval in seconds)
- `numberOfProfilingThreads = 8` (number of threads)

The limit is applicable to all profiler internal event handlers. A monitoring alarm is triggered when queue size limit is reached.

Cisco ISE Profiler Queue Size Limits

For example,

- forwarderQueueSize = 5000 (endpoint collection events)
- eventHandlerQueueSize = 10000 (events)

Event Handlers

- NetworkDeviceEventHandler—For network device events, in addition to filtering duplicate Network Access Device (NAD) IP addresses, which are already cached.
- ARPCacheEventHandler—For ARP Cache events.

CoA Handler

- CoAHandler—For CoA events, in addition to filtering duplicate MAC addresses that are still in the queue for processing.

You can configure the profiler queue limits and others as listed below in the platform.properties file. This file is included during Cisco ISE installation, which can be located in the following location:
/opt/CSCOcpm/config/

For example,

```
# -----
# Profiler Settings
# -----

profiler.maxEndpointsInLocalDb=100000
profiler.endPointsPurgeIntervalSec=300
profiler.numberOfProfilingThreads=8
<ucsSmall>.profiler.forwarderQueueSize=5000
<ucsLarge>.profiler.forwarderQueueSize=5000
<ibmSmallMedium>.profiler.forwarderQueueSize=5000
<ibmLarge>.profiler.forwarderQueueSize=5000
<ucsSmall>.profiler.eventHandlerQueueSize=10000
<ucsLarge>.profiler.eventHandlerQueueSize=10000
<ibmSmallMedium>.profiler.eventHandlerQueueSize=10000
<ibmLarge>.profiler.eventHandlerQueueSize=10000
```

Configuring Profiling Service in Cisco ISE Nodes

You can configure the profiling service that provides you a contextual inventory of all the endpoints that are using your network resources in any Cisco ISE-enabled network.

You can configure the profiling service to run on a single Cisco ISE node that assumes all Administration, Monitoring, and Policy Service personas by default.

In a distributed deployment, the profiling service runs only on Cisco ISE nodes that assume the Policy Service persona and does not run on other Cisco ISE nodes that assume the Administration and Monitoring personas.

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Choose a Cisco ISE node that assumes the Policy Service persona.

- Step 3** Click **Edit** in the Deployment Nodes page.
- Step 4** On the **General Settings** tab, check the **Policy Service** check box. If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.
- Step 5** Perform the following tasks:
- Check the **Enable Session Services** check box to run the Network Access, Posture, Guest, and Client Provisioning session services.
 - Check the **Enable Profiling Services** check box to run the profiling service.
- Step 6** Click **Save** to save the node configuration.
-

Network Probes Used by Profiling Service

Network 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 Cisco ISE database.

Cisco ISE can profile devices using a number of network probes that analyze the behavior of devices on the network and determine the type of the device. Network probes help you to gain more network visibility.

The following probes are supported by Cisco ISE:

- [NetFlow Probe, page 21-4](#)
- [DHCP Probe, page 21-5](#)
- [DHCP SPAN Probe, page 21-6](#)
- [HTTP Probe, page 21-6](#)
- [HTTP SPAN Probe, page 21-7](#)
- [RADIUS Probe, page 21-7](#)
- [Network Scan Probe, page 21-7](#)
- [DNS Probe, page 21-10](#)
- [SNMP Query Probe, page 21-11](#)
- [SNMP Trap Probe, page 21-13](#)

NetFlow Probe

Cisco ISE profiler implements Cisco IOS NetFlow Version 9. We recommend using NetFlow Version 9, which has additional functionality needed to enhance the profiler to support the Cisco ISE profiling service.

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.

In addition, Cisco ISE supports NetFlow versions earlier than Version 5. If you use NetFlow Version 5 in your network, then you can use Version 5 only on the primary network access device (NAD) at the access layer because it will not work anywhere else.

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, which can be done by combining IP addresses of the network access devices and IP addresses obtained from the NetFlow Version 5 attributes. However, these endpoints must have been previously discovered with the RADIUS or SNMP probe.

The MAC address is not a part of IP flows in earlier versions of NetFlow Version 5, which requires you to profile endpoints with their IP addresses by correlating the attributes information collected from the network access devices in the endpoints cache.

Related Topics

- For more information, see Table 6, “NetFlow Version 9 Field Type Definitions” of The NetFlow Version 9 Flow Record Format:
http://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9_ps6601_Products_White_Paper.html
- For more information on the NetFlow Version 5 Record Format, see
http://www.cisco.com/en/US/docs/ios/solutions_docs/netflow/nfwhite.html#wp1030618
- [Profiling Node Settings, page A-5](#)

DHCP Probe

The Dynamic Host Configuration Protocol probe in your Cisco ISE deployment, when enabled, allows the Cisco ISE profiling service to reprofile endpoints based only on new requests of INIT-REBOOT, and SELECTING message types. Though other DHCP message types such as RENEWING and REBINDING are processed, they are not used for profiling endpoints. Any attribute parsed out of DHCP packets is mapped to endpoint attributes.

DHCPREQUEST Message 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. Instead it should fill in the Requested IP address (requested-ip) option with the previously assigned IP address, and fill in the Client IP Address (ciaddr) field with zero in its DHCPREQUEST message. The DHCP server will then send a DHCPNAK message to the client if the Requested IP address is incorrect or the client is located in the wrong network.

DHCPREQUEST Message Generated During SELECTING State

The DHCP client inserts the IP address of the selected DHCP server in the Server identifier (server-ip) option, fills in the Requested IP address (requested-ip) option with the value of the Your IP Address (yiaddr) field from the chosen DHCPOFFER by the client, and fills in the “ciaddr” field with zero.

[Table 21-1](#) describes the different states of DHCP client messages.

Table 21-1 DHCP Client Messages from Different States

	INIT-REBOOT	SELECTING	RENEWING	REBINDING
broadcast/unicast	broadcast	broadcast	unicast	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT

Table 21-1 *DHCP Client Messages from Different States (continued)*

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP address	IP address

Related Topics

- [Wireless LAN Controller Configuration in DHCP Bridging Mode, page 21-6](#)
- [Profiling Node Settings, page A-5](#)

Wireless LAN Controller Configuration in DHCP Bridging Mode

We recommend that you configure wireless LAN controllers (WLCs) in Dynamic Host Configuration Protocol (DHCP) bridging mode, where you can forward all the DHCP packets from the wireless clients to Cisco ISE.

You must uncheck the **Enable DHCP Proxy** check box available in the WLC web interface: **Controller > Advanced > DHCP Master Controller Mode > DHCP Parameters**.

You must also ensure that the DHCP IP helper command points to the Cisco ISE Policy Service node.

DHCP SPAN Probe

The DHCP Switched Port Analyzer (SPAN) probe, when initialized in 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.

For example,

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

Related Topics

[Profiling Node Settings, page A-5](#)

HTTP Probe

In HTTP probe, the identification string is transmitted in an HTTP request-header field User-Agent, which is an attribute that can be used to create a profiling condition of IP type, and to check the web browser information. The profiler captures the web browser information from the User-Agent attribute along with other HTTP attributes from the request messages, and adds them to the list of endpoint attributes.

Cisco ISE listens to communication from the web browsers on both port 80 and port 8080. Cisco ISE provides many default profiles, which are built in to the system to identify endpoints based on the User-Agent attribute.

Related Topics

[Profiling Node Settings, page A-5](#)

HTTP SPAN Probe

The HTTP probe in your Cisco ISE deployment, when enabled with the Switched Port Analyzer (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 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, and computers with different operating systems. Identifying different mobile and portable IP-enabled devices is made more reliable because the Cisco ISE server redirects captures during a guest login or client provisioning download. This allows the profiler to collect the User-Agent attribute and other HTTP attributes, from the request messages and then identify devices such as Apple devices.

Related Topics

[Unable to Collect HTTP Attributes in Cisco ISE Running on VMware, page 21-7](#)

Unable to Collect HTTP Attributes in Cisco ISE Running on VMware

If you deploy Cisco ISE on an ESX server (VMware), the Cisco ISE profiler collects the Dynamic Host Configuration Protocol traffic but does not collect the HTTP traffic due to configuration issues on the vSphere client.

To collect HTTP traffic on a VMware setup, 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 Switched Port Analyzer (SPAN) probe for DHCP and HTTP is enabled, Cisco ISE profiler collects both the DHCP and HTTP traffic.

RADIUS Probe

You can configure Cisco ISE for authentication with RADIUS, where you can define a shared secret that you can use in client-server transactions. With the RADIUS request and response messages that are received from the RADIUS servers, the profiler can collect RADIUS attributes, which can be used for profiling endpoints.

Cisco ISE can function as a RADIUS server, and 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.

Related Topics

[Profiling Node Settings, page A-5](#)

Network Scan Probe

Cisco ISE enables you to detect devices in the subnet by using the NMAP manual subnet scan. You must choose the Policy Service node from the Admin portal in your deployment, and run the manual subnet scan from the Policy Service node that is enabled to run the profiling service.

Each NMAP manual subnet scan has a unique numeric ID that is used to update an endpoint source information with that scan ID. Upon detection of endpoints, the endpoint source information can also be updated to indicate that it is discovered by the Network Scan probe.

The NMAP manual subnet scan is useful for detecting devices such as printers with a static IP address assigned to them that are connected constantly to the Cisco ISE network, and therefore these devices cannot be discovered by other probes.

Related Topics

- [Profiling Node Settings, page A-5](#)
- [IP Address and MAC Address Binding, page 21-9](#)

Limitations of NMAP Manual Subnet Scan

The following are the limitations of a NMAP manual subnet scan:

- Scanning a subnet is highly resource intensive.
- Scanning a subnet is lengthy process that depends on the size and density of the subnet.
- Number of active scans is always restricted to one scan, which means that you can scan only a single subnet at a time.

You can cancel a subnet scan at any time while the subnet scan is in progress. You can use the **Click to see latest scan results** link to view the most recent network scan results that are stored in **Administration > Identities > Latest Network Scan Results**.

Related Topics

[Configuring Call Station ID Type in the WLC Web Interface, page 21-11](#)

NMAP Manual Subnet Scan Command

The following NMAP command scans a subnet:

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log --append-output -oX - <subnet>
```

Table 21-2 *NMAP Commands for a Manual Subnet Scan*

-O	Enables OS detection
-sU	UDP scan
-p <port ranges>	Scans only specified ports. For example, U:161, 162
-oN	Normal output
-oX	XML output

Network Mapper Integration with Cisco ISE

Network Mapper (NMAP) is integrated with the Cisco ISE profiler to augment the profiling service capability to improve 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.

Related Topics

- For more information on NMAP, see [Network Mapper \(NMAP\)](#) and the NMAP documentation that is available at <http://nmap.org/docs.html>.
- For more information on the network scanning, see “[NMAP Manual Subnet Scan Command](#)” section on page 21-8.

SNMP Read Only Community Strings for NMAP Manual Subnet Scan

The NMAP manual subnet scan is augmented with an SNMP Query whenever the scan discovers that UDP port 161 is open on an endpoint that results in more attributes being collected. During the NMAP manual subnet scan, the Network Scan probe detects whether 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 Read Only community string is set to public, you can obtain the MAC address of the device from the MIB value “ifPhysAddress”.

In addition, you can configure additional SNMP Read Only community strings separated by a comma for the NMAP manual network scan in the Profiler Configuration page. You can also specify new Read Only community strings for an SNMP MIB walk with SNMP versions 1 and 2c in the following location: **Administration > System > Settings > Profiling**.

Related Topics

[Setting up COA, SNMP RO Community and Endpoint Attribute Filter, page 21-15](#)

IP Address and MAC Address Binding

You can create or update endpoints only 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 the IN_SRC_MAC of a NetFlow packet in Cisco ISE.

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, mapping may not be reliable.

Some of the known attributes of NetFlow packets that you collect include 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, you can create endpoints only by using the MAC addresses of HTTP packets, because the HTTP request messages do not carry IP addresses and MAC addresses of endpoints in the payload data.

Cisco ISE implements an ARP cache in the profiling service, so that you can reliably map the IP addresses and the 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 the IP addresses and the 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.

DNS Probe

The Domain Name Service (DNS) probe in your Cisco ISE deployment allows the profiler to lookup an endpoint and get the fully qualified domain name (FQDN). After an endpoint is detected in your Cisco ISE-enabled network, a list of endpoint attributes is collected from the NetFlow, DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP probes.

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. When you run the setup utility, you will configure the Domain Name System (DNS) domain and the primary nameserver (primary DNS server), where you can configure one or more nameservers during setup. You can also change or add DNS nameservers later after deploying Cisco ISE using the CLI commands.

Related Topics

- For more information on the CLI commands, see [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).
- [Configuring Call Station ID Type in the WLC Web Interface, page 21-11](#)
- [Profiling Node Settings, page A-5](#)

DNS FQDN Lookup

Before a DNS lookup can be performed, one of the following probes must be started along with the DNS probe: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. 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 that exists in the system IP dictionary. You can create an endpoint profiling condition to validate the FQDN attribute and its value for profiling.

The following are the specific endpoint attributes that are required for a DNS lookup and the probe that collects these attributes:

- 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

DNS Lookup with an Inline Posture Node Deployment in Bridged Mode

For the Domain Name Service probe to work with Inline Posture deployment in the Bridged mode, you must configure the callStationIdType information sent in RADIUS messages for the Wireless LAN Controllers (WLCs).

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.

The WLCs must be configured to send the calling station ID in the MAC address format instead of the current IP address format in RADIUS messages.

Once the callStationIdType is configured in the WLCs, the 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 does a reverse DNS lookup (FQDN lookup) against the specified name servers and update the FQDN of endpoints.

Related Topics

- WLC GUI configuration—Using the GUI to Configure RADIUS section (Chapter 6, “Configuring Security Solutions”) in the [Cisco Wireless LAN Controller Configuration Guide, Release 7.0](#).
- WLC CLI configuration—The config radius callStationIdType command (Chapter 2, “CLI Commands”) in the [Cisco Wireless LAN Controller Command Reference, Release 7.0](#).
- [Configuring Call Station ID Type in the WLC Web Interface, page 21-11](#)

Configuring Call Station ID Type in the WLC Web Interface

You can use the WLC web interface to configure Call Station ID Type information. You can go to the Security tab of the WLC web interface to configure the calling station ID in the RADIUS Authentication Servers page. The MAC Delimiter field is set to Colon by default in the WLC user interface.

-
Step 1	Log in to your Wireless LAN Controller user interface.
Step 2	Click Security .
Step 3	Expand AAA , and then choose RADIUS > Authentication .
Step 4	Choose System MAC Address from the Call Station ID Type drop-down list.
Step 5	Check the AES Key Wrap check box when you run Cisco ISE in FIPS mode.
Step 6	Choose Colon from the MAC Delimiter drop-down list.
-

Related Topics

- WLC GUI configuration—Using the GUI to Configure RADIUS section (Chapter 6, “Configuring Security Solutions”) in the [Cisco Wireless LAN Controller Configuration Guide, Release 7.2](#).
- WLC CLI configuration—The config radius callStationIdType command (Chapter 2, “Controller Commands”) in the [Cisco Wireless LAN Controller Command Reference Guide, Release 7.2](#).

SNMP Query Probe

In addition to configuring the SNMP Query probe in the Edit Node page, you must configure other Simple Management Protocol settings in the following location: **Administration > Network Resources > Network Devices**.

You can configure SNMP settings in the new network access devices (NADs) in the Network Devices list page. The polling interval that you specify in the SNMP query probe or in the SNMP settings in the network access devices query NADs at regular intervals.

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

- SNMP query on Link up and New MAC notification turned on or turned off for Cisco Discovery Protocol information
- SNMP query timer for once an hour for each switch by default

For an iDevice, and other mobile 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 by an SNMP Query probe.

Related Topics

[Profiling Node Settings, page A-5](#)

Cisco Discovery Protocol Support with SNMP Query

When you configure SNMP settings on the network devices, you must ensure that the Cisco Discovery Protocol is enabled (by default) on all the ports of the network devices. If you disable the Cisco Discovery Protocol on any of the ports on the network devices, then you may not be able to profile properly because you will miss the Cisco Discovery Protocol information of all the connected endpoints.

You can enable the Cisco Discovery Protocol globally by using the **cdp run** command on a network device, and enable the Cisco Discovery Protocol by using the **cdp enable** command on any interface of the network access device. To disable the Cisco Discovery Protocol on the network device and on the interface, use the **no** keyword at the beginning of the commands.

Link Layer Discovery Protocol Support with SNMP Query

The Cisco ISE profiler uses an SNMP Query to collect LLDP attributes. You can also collect LLDP attributes from a Cisco IOS sensor, which is embedded in the network device, by using the RADIUS probe.

[Table 21-3](#) shows the default LLDP configuration settings that you can use to configure LLDP global configuration and LLDP interface configuration commands on the network access devices.

Table 21-3 *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

CDP and LLDP Capability Codes Displayed in a Single Character

The Attribute List of an endpoint displays a single character value for the `lldpCacheCapabilities` and `lldpCapabilitiesMapSupported` attributes. The values are the Capability Codes that are displayed for the network access device that runs CDP and LLDP.

Example 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

Example 2

```
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#
```

SNMP Trap Probe

The SNMP Trap receives information from the specific network access devices that support MAC notification, linkup, linkdown, and informs. The SNMP Trap probe receives information from the specific network access devices when ports come up or go down and endpoints disconnect from or connect to your network, which results in the information received that is not sufficient to create endpoints in Cisco ISE.

For SNMP Trap to be fully functional and create endpoints, you must enable SNMP Query so that the SNMP Query probe triggers a poll event on the particular port of the network access device when a trap is received. To make this feature fully functional you should configure the network access device and SNMP Trap.

**Note**

Cisco ISE does not support SNMP Traps that are received from the Wireless LAN Controllers (WLCs) and Access Points (APs).

Related Topics

[Profiling Node Settings, page A-5](#)

Configuring Probes per Cisco ISE Node

You can configure one or more probes on the Profiling Configuration tab per Cisco ISE node in your deployment that assumes the Policy Service persona, which could be:

- A standalone node—If you have deployed Cisco ISE on a single node that assumes all Administration, Monitoring, and Policy Service personas by default.
- Multiple nodes—If you have registered more than one node in your deployment that assume Policy Service persona.

Before You Begin

You can configure the probes per Cisco ISE node only from the Administration node, which is unavailable on the secondary Administration node in a distributed deployment.

-
Step 1	Choose Administration > System > Deployment .
Step 2	Choose a Cisco ISE node that assumes the Policy Service persona.
Step 3	Click Edit in the Deployment Nodes page.
Step 4	On the General Settings tab, check the Policy Service check box. If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.
Step 5	Check the Enable Profiling Services check box.
Step 6	Click the Profiling Configuration tab.
Step 7	Configure the values for each probe.
Step 8	Click Save to save the probe configuration.
-

Related Topics

- [Profiling Node Settings, page A-5](#)

Setting up CoA, SNMP RO Community and Endpoint Attribute Filter

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.

In addition, you can configure additional SNMP Read Only community strings separated by a comma for the NMAP manual network scan in the Profiler Configuration page. The SNMP RO community strings are used in the same order as they appear in the Current custom SNMP community strings field.

You can also configure endpoint attribute filtering in the Profiler Configuration page.

-
- Step 1** Choose **Administration > System > Settings > Profiling**.
- Step 2** Choose one of the following settings to configure the CoA type:
- **No CoA** (default)—You can use this option to disable the global configuration of CoA. This setting overrides any configured CoA per endpoint profiling policy.
 - **Port Bounce**—You can use this option, if the switch port exists with only one session. If the port exists with multiple sessions, then use the Reauth option.
 - **Reauth**—You can use this option to enforce reauthentication of an already authenticated endpoint when it is 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 avoids disconnecting other sessions, a situation that might occur with the Port Bounce option.
- Step 3** Enter new SNMP community strings separated by a comma for the NMAP manual network scan in the **Change custom SNMP community strings** field, and re-enter the strings in the **Confirm custom SNMP community strings** field for confirmation.
- Step 4** Check the **Endpoint Attribute Filter** check box to enable endpoint attribute filtering.
- Step 5** Click **Save**.
-

Related Topics

- [SNMP Read Only Community Strings for NMAP Manual Subnet Scan, page 21-9](#)
- [Global Configuration of Change of Authorization for Authenticated Endpoints, page 21-15](#)
- [Change of Authorization Issued for Each Type of CoA Configuration, page 21-18](#)
- [Global Setting to Filter Endpoint Attributes with Whitelist, page 21-19](#)
- [Change of Authorization Configuration per Endpoint Profiling Policy, page 21-24](#)

Global Configuration of Change of Authorization for Authenticated Endpoints

You can use the global configuration option to disable change of authorization (CoA) by using the default No CoA option or enable CoA by using port bounce and reauthentication options. If you have configured Port Bounce for CoA in Cisco ISE, the profiling service may still issue other CoAs as described in the “CoA Exemptions” section.

You can use the RADIUS probe or the Monitoring persona REST API to authenticate the endpoints. You can enable the RADIUS probe, which allows faster performance. If you have enabled CoA, then we recommend that you enable the RADIUS probe in conjunction with your CoA configuration in the Cisco ISE application for faster performance. 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, then you can rely on the Monitoring persona REST API to issue CoAs. This allows the profiling service to support a wider range of endpoints. In a distributed deployment, your network must have at least one Cisco ISE node that assumes the Monitoring persona to rely on the Monitoring persona REST API to issue a CoA.

Cisco ISE arbitrarily will designate either the primary or secondary Monitoring node as the default destination for REST queries in your distributed deployment, because both the primary and secondary Monitoring nodes have identical session directory information.

Related Topics

- [Use Cases for Issuing Change of Authorization, page 21-16](#)

Use Cases for Issuing Change of Authorization

The profiling service issues the change of authorization in the following cases:

- Endpoint deleted—When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.
- An exception action is configured—If you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the corresponding static profile by issuing a CoA.
- An endpoint is profiled for the first time—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.
- An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.

The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:

- The endpoint identity group changes for endpoints when they are dynamically profiled
- The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint
- An endpoint profiling policy has changed and the policy is used in an authorization policy—When an endpoint profiling policy changes, and the policy is included in a logical profile that is used in an authorization policy. The endpoint profiling policy may change due to the profiling policy match or when an endpoint is statically assigned to an endpoint profiling policy, which is associated to a logical profile. In both the cases, the profiling service issues a CoA, only when the endpoint profiling policy is used in an authorization policy.

Related Topics

[Exemptions for Issuing a Change of Authorization, page 21-17.](#)

Exemptions for Issuing a Change of Authorization

The profiling service does not issue a CoA when there is a change in an endpoint identity group and the static assignment is already true.

Cisco ISE does not issue a CoA for the following reasons:

- An Endpoint disconnected from the network—When an endpoint disconnected from your network is discovered.
- Authenticated wired (Extensible Authentication Protocol) EAP-capable endpoint—When an authenticated wired EAP-capable endpoint is discovered.
- Multiple active sessions per port—When 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.
- Packet-of-Disconnect CoA (Terminate Session) when a wireless endpoint is detected—If an endpoint is discovered as wireless, then a Packet-of-Disconnect CoA (Terminate-Session) is issued instead of the Port Bounce CoA. The benefit of this change is to support the Wireless LAN Controller (WLC) CoA.
- An Endpoint Created through Guest Device Registration flow—When endpoints are created through device registration for the guests. Even though CoA is enabled globally in Cisco ISE, the profiling service does not issue a CoA so that the device registration flow is not affected. In particular, the PortBounce CoA global configuration breaks the flow of the connecting endpoint.
- Global No CoA Setting overrides Policy CoA—Global No CoA overrides all configuration settings in endpoint profiling policies as there is no CoA issued in Cisco ISE irrespective of CoA configured per endpoint profiling policy.



Note No CoA and Reauth CoA configurations are not affected, and the profiler service applies the same CoA configuration for wired and wireless endpoints.

Related Topics

[Table 21-4, Change of Authorization for Each CoA Configuration](#)

Change of Authorization Issued for Each Type of CoA Configuration

Table 21-4 summarizes CoA for different environments for each type of CoA configuration in Cisco ISE.

Table 21-4 *Change of Authorization for Each CoA Configuration*

Scenarios	No CoA Configuration	Port Bounce Configuration	Reauth Configuration	Additional Information
Global CoA configuration in Cisco ISE (typical configuration)	No CoA	Port Bounce	Reauthentication	—
An endpoint is disconnected on your network	No CoA	No CoA	No CoA	Change of authorization is determined by the RADIUS attribute Acct-Status-Type value Stop.
Wired with multiple active sessions on the same switch port	No CoA	Reauthentication	Reauthentication	Reauthentication avoids disconnecting other sessions.
Wireless endpoint	No CoA	Packet-of-Disconnect CoA (Terminate Session)	Reauthentication	Support to Wireless LAN Controller.
Incomplete CoA data	No CoA	No CoA	No CoA	Due to missing RADIUS attributes.

Attribute Filters for ISE Database Persistence and Performance

Cisco ISE implements filters for Dynamic Host Configuration Protocol (both DHCP Helper and DHCP SPAN), HTTP, RADIUS, and Simple Network Management Protocol probes except for the NetFlow probe to address performance degradation. 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 isebootstrap log (isebootstrap-yyyymmdd-xxxxxx.log) contains messages that handles the creation of dictionaries and with filtering of attributes from the dictionaries. You can also configure to log a debug message when endpoints go through the filtering phase to indicate that filtering has occurred.

The Cisco ISE profiler invokes the following endpoint attribute filters:

- 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.

- SNMP filter for SNMP Query includes separate CDP and LLDP filters, which are all used for SNMP-Query probe.

Global Setting to Filter Endpoint Attributes with Whitelist

You can reduce the number of persistence events and replication events by reducing the number of endpoint attributes that do not change frequently at the collection point. Enabling the EndPoint Attribute Filter will have the Cisco ISE profiler only to keep significant attributes and discard all other attributes. Significant attributes are those used by the Cisco ISE system or those used specifically in a endpoint profiling policy or rule.

A whitelist is a set of attributes that are used in custom endpoint profiling policies for profiling endpoints, and that are essential for Change of Authorization (CoA), Bring Your Own Device (BYOD), Device Registration WebAuth (DRW), and so on to function in Cisco ISE as expected. The whitelist is always used as a criteria when ownership changes for the endpoint (when attributes are collected by multiple Policy Service nodes) even when disabled.

By default, the whitelist is disabled and the attributes are dropped only when the attribute filter is enabled. The white list is dynamically updated when endpoint profiling policies change including from the feed to include new attributes in the profiling policies. Any attribute that is not present in the whitelist is dropped immediately at the time of collection, and the attribute cannot participate in profiling endpoints. When combined with the buffering, the number of persistence events can be reduced.

You must ensure that the whitelist contains a set of attributes determined from the following two sources:

- A set of attributes that are used in the default profiles so that you can match endpoints to the profiles.
- A set of attributes that are essential for Change of Authorization (CoA), Bring Your Own Device (BYOD), Device Registration WebAuth (DRW), and so on to function as expected.

Table 21-5 **Whitelist Attributes**

AAA-Server	BYODRegistration
Calling-Station-ID	Certificate Expiration Date
Certificate Issue Date	Certificate Issuer Name
Certificate Serial Number	Description
DestinationIPAddress	Device Identifier
Device Name	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
FQDN	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type

Table 21-5 Whitelist Attributes

NmapScanCount	NmapSubnetScanID
OS Version	OUI
PolicyVersion	PortalUser
PostureApplicable	Product
RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress
cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

Attributes Collection from IOS Sensor Embedded Switches

An IOS sensor integration allows Cisco ISE run time 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 the RADIUS protocol. The attributes that are collected for DHCP, CDP, and LLDP are then parsed and mapped to attributes in the profiler dictionaries in the following location: **Policy > Policy Elements > Dictionaries**.

Related Topics

[Cisco Identity Services Engine Network Component Compatibility, Release 1.2.](#)

IOS Sensor Embedded Network Access Devices

Integrating IOS sensor embedded network access devices with Cisco ISE involves the following components:

- An IOS sensor
- Data collector that is embedded in the network access device (switch) for gathering DHCP, CDP, and LLDP data
- Analyzers for processing the data and determining the device-type of endpoints

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

Configuration Checklist for IOS Sensor-Enabled Network Access Devices

This section summarizes a list of tasks that you must configure in the IOS sensor-enabled switches and Cisco ISE to collect DHCP, CDP, and LLDP attributes directly from the switch:

- 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 the network access devices to add IOS sensor protocol data to the RADIUS accounting messages and 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 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 generated only when an incoming packet includes a type, length, and value (TLV) 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.

Endpoint Profiling Policy Rules

You can define a rule that allows you to choose one or more profiling conditions from the library that are previously created and saved in the policy elements library, and to associate an integer value for the certainty factor for each condition, or associate either an exception action or a network scan action for that condition. The exception action or the network scan action is used to trigger the configurable action while Cisco ISE is evaluating the profiling policies with respect to the overall classification of endpoints.

When the rules in a given policy are evaluated separately with an OR operator, the certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. If the rules of an endpoint profiling policy match, then the profiling policy and the matched policy are the same for that endpoint when they are dynamically discovered on your network.

Logically Grouped Conditions in Rules

An endpoint profiling policy (profile) contains a single condition or a combination of multiple single conditions that are logically combined using an AND or OR operator, against which you can check, categorize, and group endpoints for a given rule in a policy.

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 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 or trigger an exception action that is associated to the condition or a network scan action that is associated to the condition.

When you import endpoint profiling policies in Cisco ISE 1.2 from Cisco ISE 1.1.x, you must modify the name of the conditions in the exported profiler_policies.xml before importing policies.

Certainty Factor

The minimum certainty metric in the profiling policy evaluates the matching profile for an endpoint. Each rule in an endpoint profiling policy has a minimum certainty metric (an integer value) associated to the profiling conditions. The certainty metric is a measure that is added for all the valid rules in an endpoint profiling policy, which measures how each condition in an endpoint profiling policy contributes to improve the overall classification of endpoints.

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. It must exceed the minimum certainty factor that is defined in an endpoint profiling policy. By default, the minimum certainty factor for all new profiling policy rules and predefined profiling policies is 10.

Creating Endpoint Profiling Policies

You can use the Profiling Policies page to manage endpoint profiling policies that you create as an administrator of Cisco ISE, and also endpoint profiling policies that are provided by Cisco ISE when deployed.

You can create new profiling policies to profile endpoints by using the following options in the New Profiler Policy page:

- Policy Enabled
- Create an Identity Group for the policy to create a matching endpoint identity group or use the endpoint identity group hierarchy
- Parent Policy
- Associated CoA Type

**Note**

When you choose to create an endpoint policy in the Profiling Policies page, do not use the Stop button on your web browsers. This action leads to the following: stops loading the New Profiler Policy page, loads other list pages and the menus within the list pages when you access them, and prevents you from performing operations on all the menus within the list pages except the Filter menus. You might need to log out of Cisco ISE, and then log in again to perform operations on all the menus within the list pages.

You can create a similar characteristic profiling policy by duplicating an endpoint profiling policy through which you can modify an existing profiling policy instead of creating a new profiling policy by redefining all conditions.

-
- Step 1** Choose **Policy > Profiling > Profiling Policies**.
- Step 2** Click **Add**.
- Step 3** Enter a name and description for the new endpoint policy that you want to create. The **Policy Enabled** check box is checked by default to include the endpoint profiling policy for validation when you profile an endpoint.
- Step 4** Enter a value for the minimum certainty factor within the valid range 1 to 65535.
- Step 5** Click the arrow next to the **Exception Action** drop-down list to associate an exception action or click the arrow next to the **Network Scan (NMAP) Action** drop-down list to associate a network scan action.
- Step 6** Choose one of the following options for **Create an Identity Group for the policy**:
- **Yes, create matching Identity Group**
 - **No, use existing Identity Group hierarchy**
- Step 7** Click the arrow next to the **Parent Policy** drop-down list to associate a parent policy to the new endpoint policy.
- Step 8** Choose a CoA type to be associated in the **Associated CoA Type** drop-down list.
- Step 9** Click in the rule to add conditions and associate an integer value for the certainty factor for each condition or associate either an exception action or a network scan action for that condition for the overall classification of an endpoint.
- Step 10** Click **Submit to add an endpoint policy** or click the **Profiler Policy List** link from the New Profiler Policy page to return to the Profiling Policies page.
-

Related Topics

- [Endpoint Profiling Policies Settings, page B-5](#)
- [Predefined Endpoint Profiling Policies, page 21-25](#)
- [Creating Exception Actions, page 21-30](#)

- [Creating Network Scan Actions, page 21-31](#)

Change of Authorization Configuration per Endpoint Profiling Policy

In addition to the global configuration of change of authorization (CoA) types in Cisco ISE, you can also configure to issue a specific type of CoA associated for each endpoint profiling policy.

The global No CoA type configuration overrides each CoA type configured in an endpoint profiling policy. If the global CoA type is set other than the No CoA type, then each endpoint profiling policy is allowed to override the global CoA configuration.

When a CoA is triggered, each endpoint profiling policy can determine the actual CoA type, as follows:

- **General Setting**—This is the default setting for all the endpoint profiling policies that issues a CoA per global configuration.
- **No CoA**—This setting overrides any global configuration and disables CoA for the profile.
- **Port Bounce**—This setting overrides the global Port Bounce and Reauth configuration types, and issues port bounce CoA.
- **Reauth**—This setting overrides the global Port Bounce and Reauth configuration types, and issues reauthentication CoA.



Note

If the profiler global CoA configuration is set to Port Bounce (or Reauth), ensure that you configure corresponding endpoint profiling policies with No CoA, the per-policy CoA option so that the BYOD flow does not break for your mobile devices.

[Table 21-6](#) describes configuration combined for all the CoA types and the actual CoA type issued in each case based on the global and endpoint profiling policy settings.

Table 21-6 CoA Type Issued for Various Combination of Configuration

Global CoA Type	Default CoA Type set per Policy	No CoA Type per Policy	Port Bounce Type per Policy	Reauth Type per Policy
No CoA	No CoA	No CoA	No CoA	No CoA
Port Bounce	Port Bounce	No CoA	Port Bounce	Re-Auth
Reauth	Reauth	No CoA	Port Bounce	Re-Auth

Importing Endpoint Profiling Policies

You can import endpoint profiling policies from a file in XML by using the same format that you can create in the export function. If you import newly created profiling policies that have parent policies associated, then you must have defined parent policies before you define child policies.

The imported file contains the hierarchy of endpoint profiling policies that contain the parent policy first, then the profile that you imported next along with the rules and checks that are defined in the policy.

-
- Step 1** Choose **Policy > Profiling > Profiling > Profiling Policies**.
- Step 2** Click **Import**.
- Step 3** Click **Browse** to locate the file that you previously exported and want to import.

- Step 4** Click **Submit**.
- Step 5** Click the **Profiler Policy List** link to return to the Profiling Policies page.
-

Related Topics

[Predefined Endpoint Profiling Policies, page 21-25](#)

Exporting Endpoint Profiling Policies

You can export endpoint profiling policies to other Cisco ISE deployments. Or, you can use the XML file as a template for creating your own policies to import. You can also download the file to your system in the default location, which can be used for importing later.

A dialog appears when you want to export endpoint profiling policies, which 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.

-
- Step 1** Choose **Policy > Profiling > Profiling > Profiling Policies**.
- Step 2** Choose **Export**, and choose one of the following:
- **Export Selected**—You can export only the selected endpoint profiling policies in the Profiling Policies page.
 - **Export Selected with Endpoints**—You can export the selected endpoint profiling policies, and the endpoints that are profiled with the selected endpoint profiling policies.
 - **Export All**—By default, you can export all the profiling policies in the Profiling Policies page.
- Step 3** Click **OK to export the endpoint profiling policies in the profiler_policies.xml file**.
-

Related Topics

[Predefined Endpoint Profiling Policies, page 21-25](#)

Predefined Endpoint Profiling Policies

Cisco ISE includes predefined default profiling policies when Cisco ISE is deployed, and their hierarchical construction allows you to categorize identified endpoints on your network, and assign them to a matching endpoint identity groups. Because endpoint profiling policies are hierarchical, you can find that the Profiling Policies page displays the list of generic (parent) policies for devices and child policies to which their parent policies are associated in the Profiling Policies list page.

The Profiling Policies page displays endpoint profiling policies with their names, type, description and the status, if enabled or not for validation.

The endpoint profiling policy types are classified as follows:

- **Cisco Provided**—Endpoint profiling policies that are predefined in Cisco ISE are identified as the Cisco Provided type.

- **Administrator Modified**—Endpoint profiling policies are identified as the Administrator Modified type when you modify predefined endpoint profiling policies. Cisco ISE overwrites changes that you have made in the predefined endpoint profiling policies during upgrade.

You can delete administrator-modified policies but Cisco ISE replaces them with up-to-date versions of Cisco-provided policies.

- **Administrator Created**—Endpoint profiling policies that you create or when you duplicate Cisco-provided endpoint profiling policies are identified as the Administrator Created type.

We recommend that you create a generic policy (a parent) for a set of endpoints from which its children can inherit the rules and conditions. If an endpoint has to be classified, then the endpoint profile has to first match the parent, and then its descendant (child) policies when you are profiling an endpoint.

For example, Cisco-Device is a generic endpoint profiling policy for all Cisco devices, and other policies for Cisco devices are children of Cisco-Device. 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 the Cisco-IP-Phone 7960 profiling policy for better classification.

Predefined Endpoint Profiling Policies Overwritten During Upgrade

You can edit existing endpoint profiling policies in the Profiling Policies page. You must also save all your configurations in a copy of the predefined endpoint profiles when you want to modify the predefined endpoint profiling policies.

During an upgrade, Cisco ISE overwrites any configuration that you have saved in the predefined endpoint profiles.

Unable to Delete Endpoint Profiling Policies

You can delete selected or all the endpoint profiling policies in the Profiling Policies page. By default, you can delete all the endpoint profiling policies from the Profiling Policies page. When you select all the endpoint profiling policies and try to delete them in the Profiling Policies page, some of them may not be deleted when the endpoint profiling policies are a parent policy mapped to other endpoint profiling policies or mapped to an authorization policy and a parent policy to other endpoint profiling policies.

For example,

1. You cannot delete Cisco Provided endpoint profiling policies,
1. You cannot delete a parent profile in the Profiling 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 profiling policies for Cisco devices.
2. 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 profiling policies for Cisco IP Phones.

Predefined Profiling Policies for Draeger Medical Devices

Cisco ISE contains default endpoint profiling policies that include a generic policy for Draeger medical devices, a policy for Draeger-Delta medical device, and a policy for Draeger-M300 medical device. Both the medical devices share ports 2050 and 2150, and therefore you cannot classify the Draeger-Delta and Draeger-M300 medical devices when you are using the default Draeger endpoint profiling policies.

If these Draeger devices share ports 2050 and 2150 in your environment, you must add a rule in addition to checking for the device destination IP address in the default Draeger-Delta and Draeger-M300 endpoint profiling policies so that you can distinguish these medical devices.

Cisco ISE includes the following profiling conditions that are used in the endpoint profiling policies for the Draeger medical devices:

- Draeger-Delta-PortCheck1 that contains port 2000
- Draeger-Delta-PortCheck2 that contains port 2050
- Draeger-Delta-PortCheck3 that contains port 2100
- Draeger-Delta-PortCheck4 that contains port 2150
- Draeger-M300PortCheck1 that contains port 1950
- Draeger-M300PortCheck2 that contains port 2050
- Draeger-M300PortCheck3 that contains port 2150

Endpoint Profiling Policy for Unknown Endpoints

An endpoint that does not match existing profiles and cannot be profiled in Cisco ISE is an unknown endpoint. An unknown profile is the default system profiling policy 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.

An Unknown profile is assigned in the following scenarios:

- 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.
- When an endpoint is statically added in Cisco ISE, and there is no matching endpoint profiling policy for a statically added endpoint, it is assigned to the unknown profile.

If you have statically added an endpoint to your network, the statically added endpoint is not profiled by the profiling service in Cisco ISE. You can change the unknown profile later to an appropriate profile and Cisco ISE will not reassign the profiling policy that you have assigned.

Endpoint Profiling Policy for Statically Added Endpoints

For the endpoint that is statically added 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 if that endpoint is dynamically profiled. This allows you to find the mismatch between the computed profile for statically added endpoints and the matching profile for dynamically profiled endpoints.

Endpoint Profiling Policy for Static IP Devices

If you have an endpoint with a statically assigned IP address, you can create a profile for such static IP devices.

You must enable the RADIUS probe or SNMP Query and SNMP Trap probes to profile an endpoint that has a static IP address.

Endpoint Profiling Policy Matching

Cisco ISE always considers a chosen policy for an endpoint that is the matched policy rather than an evaluated policy when the profiling conditions that are defined in one or more rules are met in a 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.

The following apply to the matched policies of endpoints:

- For statically assigned endpoint, the profiling service computes the MATCHEDPROFILE.
- For dynamically assigned endpoints, the MATCHEDPROFILES are identical to the matching endpoint profiles.

You can determine a matching profiling policy for dynamic endpoints using one or more rules that are defined in a profiling policy and assign appropriately an endpoint identity group for categorization.

When an endpoint is mapped to an existing policy, the profiling service searches the hierarchy of profiling policies for the closest parent profile that has a matching group of policies and assigns the endpoint to the appropriate endpoint policy.

Endpoint Profiling Policies Used for Authorization

You can use an endpoint profiling policy in authorization rules, where you can create a new condition to include a check for an endpoint profiling policy as an attribute, and the attribute value assumes the name of the endpoint profiling policy. You can select an endpoint profiling policy from the EndPoints dictionary, which includes the following attributes: PostureApplicable, EndPointPolicy, LogicalProfile, and BYODRegistration.

You can define an authorization rule that includes a combination of EndPointPolicy, BYODRegistration, and identity groups.

Endpoint Profiling Policies Grouped into Logical Profiles

A logical profile is a container for a category of profiles or associated profiles, irrespective of Cisco-provided or administrator-created endpoint profiling policies. An endpoint profiling policy can be associated to multiple logical profiles.

You can use the logical profile in an authorization policy condition to help create an overall network access policy for a category of profiles. You can create a simple condition for authorization, which can be included in the authorization rule. The attribute-value pair that you can use in the authorization condition is the logical profile (attribute) and the name of the logical profile (value), which can be found in the EndPoints systems dictionary.

For example, you can create a logical profile for all mobile devices like Android, Apple iPhone, or Blackberry by assigning matching endpoint profiling policies for that category to the logical profile. Cisco ISE contains IP-Phone, a default logical profile for all the IP phones, which includes IP-Phone, Cisco-IP-Phone, Nortel-IP-Phone-2000-Series, and Avaya-IP-Phone profiles.

Related Topics

[Creating Logical Profiles, page 21-29](#)

Creating Logical Profiles

You can create a logical profile that you can use to group a category of endpoint profiling policies, which allows you to create an overall category of profiles or associated profiles. You can also remove the endpoint profiling policies from the assigned set moving them back to the available set.

-
Step 1	Choose Policy > Profiling > Profiling > Logical Profiles .
Step 2	Click Add .
Step 3	Enter a name and description for the new logical profile in the text boxes for Name and Description .
Step 4	Choose endpoint profiling policies from the Available Policies to assign them in a logical profile.
Step 5	Click the right arrow to move the selected endpoint profiling policies to the Assigned Policies .
Step 6	Click Submit .
-

Related Topics

[Creating Exception Actions, page 21-30](#)

Profiling Exception Actions

An exception action is a single 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.

Exception Actions can be any one of the following types:

- Cisco-provided—You can not delete Cisco-provided exception actions. Cisco ISE triggers the following noneditable profiling exception actions from the system when you want to profile endpoints in Cisco ISE:
 - Authorization Change—The profiling service issues a change of authorization when an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.
 - Endpoint Delete—An exception action is triggered in Cisco ISE and a CoA is issued when an endpoint is deleted from the system in the Endpoints page, or reassigned to the unknown profile from the edit page on a Cisco ISE network.
 - 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.
- Administrator-created—Cisco ISE triggers profiling exception actions that you create.

Related Topics:

- [Predefined Endpoint Profiling Policies, page 21-25](#)
- [Creating Exception Actions, page 21-30](#)

Creating Exception Actions

You can define and associate one or more exception rules to a single profiling policy. This association triggers an exception action (a single configurable action) when the profiling policy matches and at least one of the exception rules matches in the profiling endpoints in Cisco ISE.

-
Step 1	Choose Policy > Policy Elements > Results > Profiling > Exception Actions .
Step 2	Click Add .
Step 3	Enter a name and description for the exception action in the text boxes for Name and Description .
Step 4	Check the CoA Action check box.
Step 5	Click the Policy Assignment drop-down list to choose an endpoint policy.
Step 6	Click Submit .
-

Related Topics

[Profiling Exception Action Settings, page B-25](#)

Profiling Network Scan Actions

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.

An endpoint scan is used to scan endpoints in order to limit resources usage in the Cisco ISE system. A network scan action scans a single endpoint, unlike 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 cannot edit or delete OS-scan, SNMPPortsAndOS-scan, and CommonPortsAndOS-scans, which are predefined network scan actions in Cisco ISE. 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.

Related Topics

- [Predefined Endpoint Profiling Policies, page 21-25](#)
- [Creating Network Scan Actions, page 21-31](#)

Creating Network Scan Actions

A network scan action that is associated with an endpoint profiling policy scans an endpoint for an operating system, Simple Network Management Protocol (SNMP) ports, and common ports.

You can define and associate one or more network scan rules in a 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.

Before You Begin

You must ensure that the Network Scan (NMAP) probe is enabled to trigger a network scan action that you define in the rule.

-
Step 1	Choose Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions .
Step 2	Click Add .
Step 3	Enter a name and description for the network scan action that you want to create.
Step 4	Check one or more check boxes when you want to scan an endpoint for the following: • Scan OS—To scan an operating system • Scan SNMP Port—To scan SNMP ports (161, 162) • Scan Common Port—To scan common ports.
Step 5	Click Submit .
-

Related Topics

- [Operating System Scan, page 21-31](#)
- [SNMP Port Scan, page 21-32](#)
- [Common Ports Scan, page 21-32](#)
- [Common Ports, page 21-33](#)

Operating System Scan

The operating system scan (OS-scan) type scans an operating system (and OS version) that an endpoint is running. This is a resource intensive scan.

Limitations of the NMAP tool that you use for an OS-scan may cause a scan of the operating system of endpoints to give unreliable results. 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. Cisco ISE displays the operating-system attribute, if the accuracy is not 100%.

For these devices, you can configure endpoint profiling policies that use the NMAP:operating-system attribute in their rules to have low certainty value conditions (Certainty Factor values). We recommend that whenever you create an endpoint profiling policy based on the NMAP:operating-system attribute, the profiling policy should contain an AND condition. For example, NMAP:operating-system contains 100.

**Note**

Do not create an endpoint profiling policy based on the NMAP:operating-system attribute unless the accuracy is 100%.

The following NMAP command scans the operating system when you associate Scan OS with an endpoint profiling policy:

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

Table 21-7 *NMAP Commands for an Endpoint OS Scan*

-sS	TCP SYN scan. SYN scan is the default.
-O	Enables OS detection.
-F	(Fast (limited port) scan). Specifies that you want to scan fewer ports than the default. Normally Nmap scans the most common 1000 ports for each scanned protocol. With -F, this is reduced to 100.
-oN	Normal output.
-oX	XML output.
IP-address	IP-address of an endpoint that is scanned.

SNMP Port Scan

The SNMPPortsAndOS-scan type scans an operating system (and OS version) that an endpoint is running and 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.

The following NMAP command scans SNMP ports (UDP 161 and 162) when you associate the Scan SNMP Port with an endpoint profiling policy:

```
nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>
```

Table 21-8 *NMAP Commands for an Endpoint SNMP Port Scan*

-sU	UDP scan.
-p <port-ranges>	Scans only specified ports. For example, scans UDP ports 161 and 162.
-oN	Normal output.
-oX	XML output.
IP-address	IP-address of an endpoint that is scanned.

Common Ports Scan

The CommonPortsAndOS-scan type scans an operating system (and OS version) that an endpoint is running and common ports (TCP and UDP), but not SNMP ports.

The following NMAP command scans common ports when you associate Scan Common Port with an endpoint profiling policy:

```
nmap -sTU -p
T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,
445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>
```

Table 21-9 NMAP Commands for an Endpoint Common Ports Scan

-sTU	Both TCP connect scan and UDP scan.
-p <port ranges>	Scans TCP ports: 21,22,23,25,53,80,110,135,139,143, 443,445,3306,3389,8080 and UDP ports: 53,67,68,123,135,137, 138,139,161,445,500,520,631,1434,1900
oN	Normal output.
oX	XML output.
IP address	IP address of an endpoint that is scanned.

Common Ports

The following table lists 30 common ports (15 TCP and 15 UDP ports) that NMAP uses for scanning.

Table 21-10 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
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

Cisco ISE Integration with Cisco NAC Appliance

Cisco ISE supports integration only with the Cisco Network Admission Control (NAC) Appliance Release 4.9 and is available when you have installed an Advanced or Wireless license in Cisco ISE.

The Cisco ISE profiler is similar to the Cisco Network Admission Control (NAC) Profiler that manages endpoints in a Cisco NAC deployment. 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 and the result of endpoint classification in to the Cisco Clean Access Manager (CAM).

Related Topics

- [Cisco NAC Appliance Hardware Installation Guide, Release 4.9](#)
- [Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9](#)
- [Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9 to install, configure and administer the Cisco NAC Appliance, Release 4.9](#)
- [Release Notes for Cisco NAC Appliance, Release 4.9](#)

Cisco Clean Access Manager Configuration in Administration Nodes

Cisco ISE allows you to register multiple Clean Access Managers (CAMs) on a primary Administration 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. The primary Administration node is responsible for all the communication between Cisco ISE and the Cisco NAC Appliance. You can configure CAMs only in the primary Administration node in Cisco ISE. The credentials that are used at the time of registering one or more CAMs in the primary Administration 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, because Cisco ISE pushes the profiler configuration changes to CAMs, and CAMs periodically pull the list of MAC addresses of endpoints and their corresponding profiles and the list of all the profile names, from Cisco ISE.

You must export the contents of the X509 Certificate from the Clean Access Manager in Administration > Clean Access Manager > SSL, and import it into the primary Administration node under Administration > System > Certificates > Certificate Trust Store in Cisco ISE for a proper secure communication between Cisco ISE and CAM.

Related Topics

[NAC Manager Settings, page A-45](#)

Cisco ISE Profiler and Cisco Clean Access Manager Communication

The Cisco ISE profiler notifies the profiler configuration changes to all the registered Clean Access Managers (CAMs) from the primary Administration node. It avoids duplicating notification in a Cisco ISE distributed deployment. It uses the REST APIs to notify the profiler configuration changes when endpoints are added or removed, and endpoint profiling 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 flow is 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 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 and 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)

Adding Cisco Clean Access Managers

Integrating Cisco ISE with the Cisco NAC Appliance, Release 4.9 allows you to utilize the Cisco ISE profiling service in a Cisco NAC deployment. to utilize the Cisco ISE profiling service in a Cisco NAC deployment.

The NAC Managers page allows you to configure multiple Cisco Access Managers (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.

-
Step 1	Choose Administration > Network Resources > NAC Managers .
Step 2	Click Add .
Step 3	Enter the name for the Cisco Access Manager.
Step 4	Click the Status check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.
Step 5	Enter the IP address for the CAM except the following IP addresses: 0.0.0.0 and 255.255.255.255.
Step 6	Enter the username and password of the CAM administrator that you use to log in to the user interface of the CAM.
Step 7	Click Submit .
-

Related Topics

[NAC Manager Settings, page A-45](#)

Creating Endpoints with Static Assignments of Policies and Identity Groups

You can create a new endpoint statically by using the MAC address of an endpoint in the Endpoints page. You can also choose an endpoint profiling policy and an identity group in the Endpoints page for static assignment.

-
- Step 1** Choose **Administration > Identity Management > Identities > Endpoints**.
 - Step 2** Click **Add**.
 - Step 3** Enter the MAC address of an endpoint in hexadecimal format and separated by a colon.
 - Step 4** Choose a matching endpoint policy from the **Policy Assignment** drop-down list to change the static assignment status from dynamic to static.
 - Step 5** Check the **Static Assignment** check box to change the status of static assignment that is assigned to the endpoint from dynamic to static.
 - Step 6** Choose an endpoint identity group to which you want to assign the newly created endpoint from the **Identity Group Assignment** drop-down list.
 - Step 7** Check the **Static Group Assignment** check box to change the dynamic assignment of an endpoint identity group to static.
 - Step 8** Click **Submit**.
-

Related Topics

- [Endpoint Settings, page A-25](#)
- [Adding Static Endpoints in Endpoint Identity Groups, page 21-44](#)
- [Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page G-5](#)
- [Cannot Authenticate on Profiled Endpoint, page G-21](#)

Importing Endpoints from CSV Files

You can import endpoints from a CSV file for which you have already exported endpoints from a Cisco ISE server, or a CSV file that you have created from Cisco ISE and updated with endpoint details.

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

Both endpoint policy and endpoint identity group are optional for importing endpoints in a CSV file. If you want to import the endpoint identity group without the endpoint policy for endpoints, the values are still separated by the comma.

For example,

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, , Endpoint Identity Group4

-
- Step 1** Choose **Administration > Identity Management > Identities > Endpoints > Import**.
- Step 2** Click **Import From File**.
- Step 3** Click Browse to locate the CSV file that you have already exported from the Cisco ISE server or the CSV file that you have created and updated with endpoints in the file format as specified.
- Step 4** Click **Submit**.
-

Related Topics

- [Default Import Template Available for Endpoints, page 21-37](#)
- [Unknown Endpoints Reprofiled During Import, page 21-37](#)
- [Static Assignments of Policies and Identity Groups for Endpoints Retained During Import, page 21-38](#)
- [Importing Endpoints from LDAP Server, page 21-39](#)

Default Import Template Available for Endpoints

You can generate a template in which you can update endpoints that can be used to import endpoints. 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. The file can be found in Administration > Identity Management > Identities > Endpoints > Import > Import From File.

You can use the Generate a Template link to create a template, and the Cisco ISE server will display the Opening template.csv dialog. This dialog allows you to open the default 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 default template.csv file contains a header row that displays the MAC address, Endpoint Policy, and Endpoint Identity Group columns. You must update the MAC addresses of endpoints, endpoint profiling policies, and endpoint identity groups and save the file with a different file name that you can use to import endpoints.

[Table 21-11](#) displays the header row in the template.csv file that is created when you use the Generate a Template link.

Table 21-11 CSV Template File

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

Unknown Endpoints Reprofiled During Import

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

[Table 21-12](#) 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 21-12 *Unknown Profiles: Import from a File*

MAC Address	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 no profile is assigned to an endpoint, then it is assigned to the Unknown profile, and also reprofiled to the matching profile.	Xerox-Device

Static Assignments of Policies and Identity Groups for Endpoints Retained During Import

If the file used for import contains endpoints that have their MAC addresses, and their assigned endpoint profiling policy is the static assignment, then they are not reprofiled during import.

[Table 21-13](#) shows how Cisco ISE retains the Cisco-Device profile, the static assignment of an endpoint during import.

Table 21-13 *Static Assignment: Import From a File*

MAC Address	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 (static assignment)	Cisco-Device

Endpoints with Invalid Profiles Not Imported

If endpoints are assigned to invalid profiles in the file used for import, then they are not imported because there are no matching profiles in Cisco ISE.

[Table 21-14](#) also shows that endpoints are not imported when they are assigned to invalid profiles in the CSV file.

Table 21-14 *Invalid Profiles: Import from a File*

MAC Address	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
00:00:00:00:01:05	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.

Related Topics

[Importing Endpoints from CSV Files, page 21-36](#)

Importing Endpoints from LDAP Server

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

Before You Begin

Before you begin to import endpoints, ensure that you have installed the LDAP server.

You have to configure the connection settings and query settings before you can 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.

-
Step 1	Choose Administration > Identity Management > Identities > Endpoints > Import > Import From LDAP .
Step 2	Enter the values for the connection settings.
Step 3	Enter the values for the query settings.
Step 4	Click Submit .
-

Related Topics

[Endpoint Import from LDAP Settings, page A-27](#)

Exporting Endpoints with Comma-Separated Values File

You can export selected or all endpoints from a Cisco ISE server to different Cisco ISE servers in a comma-separated values (CSV) file in which endpoints are listed with their MAC addresses, endpoint profiling policies, and endpoint identity groups to which they are assigned.

Export All is the default option. If endpoints are filtered in the Endpoints page, only those filtered endpoints are exported when you are using the Export All option. By default, the profiler_endpoints.csv is the CSV file and the Microsoft Office Excel is the default application to open the CSV file from the Opening profiler_endpoints.csv dialog box or to save the CSV file. For example, you can export selected endpoints or all endpoints in the profiler_endpoints.csv file, which you can use to import those endpoints.

-
Step 1	Choose Administration > Identity Management > Identities > Endpoints .
Step 2	Click Export , and choose one of the following: • Export Selected—You can export only the selected endpoints in the Endpoints page. • Export All—By default, you can export all the endpoints in the Endpoints page.
Step 3	Click OK to save the profiler_endpoints.csv file.
-

Identified Endpoints

Cisco ISE displays identified endpoints that connect to your network and use resources on your network in the Endpoints page. An endpoint is typically a network-capable device that connect to your network through wired and wireless network access devices and VPN. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, and so on.

The MAC address of an endpoint, expressed in hexadecimal form, 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 and the methods (probes) that you use to collect these attributes.

Dynamically Profiled Endpoints

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

Statically Profiled Endpoints

An endpoint can be profiled statically when you create an endpoint with its MAC address and associate a profile to it along with an endpoint identity group in Cisco ISE. Cisco ISE does not reassign the profiling policy and the identity group for statically assigned endpoints.

Unknown Endpoints

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

Related Topics

- [Identified Endpoints Locally Stored in Policy Service Nodes Database, page 21-40](#)
- [Policy Service Node, page 3-3](#)
- [Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page G-5](#)
- [Cannot Authenticate on Profiled Endpoint, page G-21](#)

Identified Endpoints Locally Stored in Policy Service Nodes Database

Cisco ISE writes identified endpoints locally in the Policy Service node database. After storing endpoints locally in the database, these endpoints are then made available (remote write) in the Administration node database only when significant attributes change in the endpoints, and replicated to the other Policy Service nodes database.

The following are the significant attributes:

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment

- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

When you change endpoint profile definitions in Cisco ISE, all endpoints have to be reprofiled. A Policy Service node that collects the attributes of endpoints is responsible for reprofiling of those endpoints.

When a Policy Service node starts collecting attributes about an endpoint for which attributes were initially collected by a different Policy Service node, then the endpoint ownership changes to the current Policy Service node. The new Policy Service node will retrieve the latest attributes from the previous Policy Service node and reconcile the collected attributes with those attributes that were already collected.

When a significant attribute changes in the endpoint, attributes of the endpoint are automatically saved in the Administration node database so that you have the latest significant change in the endpoint. If the Policy Service node that owns an endpoint is not available for some reasons, then the Administrator ISE node will reprofile an endpoint that lost the owner and you have to configure a new Policy Service node for such endpoints.

Policy Service Nodes in Cluster

Cisco ISE uses Policy Service node group as a cluster that allows to exchange endpoint attributes when two or more nodes in the cluster collect attributes for the same endpoint. We recommend to create clusters for all Policy Service nodes that reside behind a load balancer.

If a different node other than the current owner receives attributes for the same endpoint, it sends a message across the cluster requesting the latest attributes from the current owner to merge attributes and determine if a change of ownership is needed. If you have not defined a node group in Cisco ISE, it is assumed that all nodes are within one cluster.

There are no changes made to endpoint creation and replication in Cisco ISE. Only the change of ownership for endpoints is decided based on a list of attributes (white list) used for profiling that are built from static attributes and dynamic attributes. See [Table 21-5 on page 21-19](#).

Upon subsequent attributes collection, the endpoint is updated on the Administration node, if any of the following attributes changes:

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

When an endpoint is edited and saved in the Administration node, the attributes are retrieved from the current owner of the endpoint.

Related Topics

- [Identified Endpoints Locally Stored in Policy Service Nodes Database, page 21-40](#)
- [Policy Service Node, page 3-3](#)

Creating Endpoint Identity Groups

You can create, edit, or delete an endpoint identity group on the Endpoint Identity Groups page. You can only edit the name and description of the identity groups, and delete identity groups that you have created in the system. You cannot edit the name of the endpoint identity groups although their description are editable, and delete endpoint identity groups that are created by Cisco ISE in the system.

-
Step 1	Choose Administration > Identity Management > Groups > Endpoint Identity Groups .
Step 2	Click Add .
Step 3	Enter the name for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).
Step 4	Enter the description for the endpoint identity group that you want to create.
Step 5	Click the Parent Group drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.
Step 6	Click Submit .
-

Related Topics

- [Endpoint Identity Group Settings, page A-28](#)
- [Adding Static Endpoints in Endpoint Identity Groups, page 21-44](#)

Identified Endpoints Grouped in Endpoint Identity Groups

Cisco ISE groups discovered endpoints into their corresponding endpoint identity groups based on the endpoint profiling policies. Profiling policies are hierarchical, and they are applied at the endpoint identity groups level in Cisco ISE. By grouping endpoints to endpoint identity groups, and applying profiling policies to endpoint identity groups, Cisco ISE enables you to determine the mapping of endpoints to the endpoint profiles by checking corresponding endpoint profiling policies.

Cisco ISE creates a set of endpoint identity groups by default, and allows you to create your own identity groups to which endpoints can be assigned dynamically or statically. You can create an endpoint identity group and associate the identity group to one of the system-created identity groups. You can also assign an endpoint that you create statically to any one of the identity groups that exists in the system, and the profiling service cannot reassign the identity group.

Related Topics

- [Creating Endpoint Identity Groups, page 21-42](#)
- [Default Endpoint Identity Groups Created for Endpoints, page 21-43](#)

- [Endpoint Identity Groups Created for Matched Endpoint Profiling Policies, page 21-43](#)

Default Endpoint Identity Groups Created for Endpoints

Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, 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. A parent group is the default identity group that exists in the system.

Cisco ISE creates the following endpoint identity groups:

- **Blacklist**—This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are blacklisted in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.
- **GuestEndpoints**—This endpoint identity group includes endpoints that are used by guest users.
- **Profiled**—This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.
- **RegisteredDevices**—This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and blacklist these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blacklisted in the device registration portal are assigned to the Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blacklisted devices to an URL, which displays “Unauthorised Network Access”, a default portal page to the blacklisted devices.
- **Unknown**—This endpoint identity group includes endpoints that do not match any profile in Cisco ISE.

In addition to the above system created endpoint identity groups, Cisco ISE creates 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.
- **Workstation**—An identity group that contains all the profiled workstations on your network.

Related Topics

[Endpoint Identity Groups Created for Matched Endpoint Profiling Policies, page 21-43](#)

Endpoint Identity Groups Created for Matched Endpoint Profiling Policies

If you have an endpoint policy that matches an existing policy, then the profiling service can create a matching endpoint identity group. This identity group becomes the child of the Profiled endpoint identity group. When you create an endpoint policy, you can check the Create Matching Identity Group check box in the Profiling Policies page to create a matching endpoint identity group. You cannot delete the matching identity group unless the mapping of the profile is removed.

Related Topics

[Endpoint Profiling Policy for Statically Added Endpoints, page 21-27](#)

Adding Static Endpoints in Endpoint Identity Groups

You can add or remove statically added endpoints in any endpoint identity group.

You can add endpoints from the Endpoints widget only 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. You do not delete endpoints from the system but only remove them from the endpoint identity group.

-
Step 1	Choose Administration > Identity Management > Groups > Endpoint Identity Groups .
Step 2	Choose an endpoint identity group, and click Edit .
Step 3	Click Add .
Step 4	Choose an endpoint in the Endpoints widget to add the selected endpoint in the endpoint identity group.
Step 5	Click the Endpoint Group List link to return to the Endpoint Identity Groups page.
-

Related Topics

[Dynamic Endpoints Reprofiled After Adding or Removing in Identity Groups, page 21-44](#)

Dynamic Endpoints Reprofiled After Adding or Removing in Identity Groups

If an endpoint identity group assignment is not static, then endpoints are reprofiled after you add or remove them from an endpoint identity group. Endpoints that are identified dynamically by the ISE 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.

Endpoint Identity Groups Used in Authorization Rules

You can effectively use endpoint identity groups in the authorization policies to provide appropriate network access privileges to the discovered endpoints. For example, an authorization rule for all types of Cisco IP Phones is available by default in Cisco ISE in the following location: **Policy > Authorization > Standard**.

You must ensure that the endpoint profiling policies are either standalone policies (not a parent to other endpoint profiling policies), or their parent policies of the endpoint profiling policies are not disabled.

Profiler Feed Service

With the introduction of the profiler feed service, the profiler conditions, exception actions, and NMAP scan actions are classified as Cisco-provided or administrator-created (see the System Type attribute) in Cisco ISE. Also, the endpoint profiling policies are classified as Cisco provided, administrator created, or administrator modified (see the System Type attribute).

You can perform different operations on the profiler conditions, exception actions, NMAP scan actions, and endpoint profiling policies depending on the System Type attribute. You cannot edit or delete Cisco-provided conditions, exception actions, and nmap scan actions. Endpoint policies that are provided by Cisco cannot be deleted. When policies are edited, they are considered as administrator-modified. When administrator-modified policies are deleted, they are replaced by the up-to-date version of the Cisco-provided policy that it was based on.

You can retrieve new and updated endpoint profiling policies and the updated OUI database as a feed from a designated Cisco feed server through a subscription into Cisco ISE. You can also receive e-mail notifications to the e-mail address as an administrator of Cisco ISE that you have configured for applied, success, and failure messages. You can also provide additional subscriber information to receive notifications. You can send the subscriber information back to Cisco for maintaining the records and they are treated as privileged and confidential.

By default, the profiler feed service is disabled, and it requires an Advanced license to enable the service. When you enable the profiler feed service, Cisco ISE downloads the feed service policies and OUI database updates every day at 1:00 A.M of the local Cisco ISE server time zone. Cisco ISE automatically applies these downloaded feed server policies, which also stores the set of changes so that you can revert these changes back to the previous state. When you revert from the set of changes that you last applied, endpoint profiling policies that are newly added are removed and endpoint profiling policies that are updated are reverted to the previous state. In addition, the profiler feed service is automatically disabled.

When the updates occur, only the Cisco Provided profiling policies are updated and the endpoint profiling policies which were modified by the previous update. Cisco Provided disabled profiling policies are also updated but they remain disabled. Administrator Created or Administrator Modified profiling policies are not overwritten. If you want to revert any Administrator Modified endpoint profiling policy to any Cisco Provided endpoint profiling policy, then you must delete the Administrator Modified endpoint profiling policy or revert the Administrator Modified endpoint profiling policy to the previous Cisco Provided endpoint profiling policy.

Related Topics

- [OUI Feed Service, page 21-45](#)
- [Configuring Profiler Feed Service, page 21-46](#)
- [Removing Updates to Endpoint Profiling Policies, page 21-47](#)

OUI Feed Service

The designated Cisco feed server downloads the updated OUI database from the following location: <http://standards.ieee.org/develop/regauth/oui/oui.txt>, which is the list of vendors associated to the MAC OUI. The updated OUI database is available for any ISE deployment as a feed that Cisco ISE downloads to its own database. Cisco ISE updates endpoints and then starts reprofiling endpoints.

The designated Cisco feed server is located at <https://ise.cisco.com:8443/feedserver/>. If you have any issues accessing the service, ensure that your network security components (like a firewall or proxy server, for example) allow direct access to this URL.

Configuring Profiler Feed Service

You can configure Cisco ISE to receive updates for new, updated endpoint profiling policies, and MAC OUI as a feed from a designated Cisco feed server. Enabling the profiler feed service allows Cisco ISE to check for new and updated profiles that are created since the last feed service update, and MAC OUI. If feed service is unavailable or other errors have occurred, then they are reported in the Operations Audit report.

You can configure Cisco ISE to send the feed service usage report back to Cisco as an administrator of Cisco ISE and provide an alternate Cisco ISE administrator details (optional attributes) in the Feed Service Subscriber Information section.

You can send the following data back to Cisco:

- Hostname - Cisco ISE hostname
- MaxCount - Total number of endpoints
- ProfiledCount - Profiled endpoints count
- UnknownCount - Unknown endpoints count
- MatchSystemProfilesCount - Cisco Provided profiles count
- UserCreatedProfiles - User created profiles count

The CoA type in a profiling policy downloaded from the feed server is locally configured and not downloaded. If you change the CoA type in the downloaded policy, the state will not be updated. It remains as a system policy and you need to update the policy via the feed server.

Before You Begin

You can configure the profiler feed service only from the Cisco ISE Admin portal in a distributed deployment or in a standalone ISE node.

Cisco ISE requires the feed server certificate in order to communicate as the feed service client interacts with the feed service platform through HTTPS. You can download the certificate from the Certificate Store by navigating to Administration > System > Certificates.

You must set up a Simple Mail Transfer Protocol (SMTP) server to send e-mail notifications from the Admin portal (Administration > System > Settings).

-
Step 1	Choose Administration > FeedService > Profiler .
Step 2	Check the Enable Profiler Feed Service check box.
Step 3	Enter time in HH:MM format (local time zone of the Cisco ISE server) in the Feed Service Scheduler section. By default, Cisco ISE profiler feed service is scheduled at 1.00 AM every day.
Step 4	Check the Notify administrator when download occurs check box in the Administrator Notification Options section and enter your e-mail address as an administrator of Cisco ISE in the Administrator email address text box.
Step 5	Check the Provide subscriber information to Cisco check box in the Feed Service Subscriber Information section to send the feed server usage report back to Cisco.
Step 6	Click Accept . See for more information, http://www.cisco.com/web/siteassets/legal/privacy.html
Step 7	Click Save .
Step 8	Click Update Now .

Instructs Cisco ISE to contact Cisco feed server for new and updated profiles created since the last feed service update. This reprofiles all endpoints in the system, which may cause an increase in the system load. Due to updated endpoint profiling policies, there may be changes in the authorization policy for some endpoints that are currently connected to Cisco ISE.

The Update Now button is disabled when you update new and updated profiles created since the last feed service and enabled only after the download is completed. You must navigate away from the Profiler Feed Service Configuration page and return to this page.

Step 9 Click **Yes**.

Related Topics

- [Removing Updates to Endpoint Profiling Policies, page 21-47](#)
- [Profiler Feed Service, page 21-44](#)
- [OUI Feed Service, page 21-45](#)
- [Configuring the SMTP Server to Support Notifications, page 5-5](#)

Removing Updates to Endpoint Profiling Policies

You can revert endpoint profiling policies that were updated in the previous update and remove endpoint profiling policies that are newly added through the previous update of the profiler feed service but OUI updates are not changed.

An endpoint profiling policy, if modified after an update from the feed server is not changed in the system.

-
- Step 1** Choose **Administration > FeedService > Profiler**.
- Step 2** Check the **Enable Profiler Feed Service** check box.
- Step 3** Click **Go to Update Report Page** to view the configuration changes made in the Change Configuration Audit report.
- Step 4** Click **Undo Latest**.
- Step 5** Click **Save**.
-

Related Topics

- [Configuring Profiler Feed Service, page 21-46](#)
- [Profiler Feed Service, page 21-44](#)

Profiler Reports

Cisco ISE provides you with various reports on endpoint profiling, and troubleshooting tools that you can use to 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 view more details. For large reports, you can also schedule reports and download them in various formats.

You can run the following reports for endpoints from **Operations > Reports > Endpoints and Users**:

- Endpoint Session History
- Profiled Endpoint Summary
- Endpoint Profile Changes
- Top Authorizations by Endpoint
- Registered Endpoints

Related Topics

[Chapter 26, “Reporting”](#)



Configuring Client Provisioning

This chapter describes client-provisioning functions in Cisco ISE that allows you to download client-provisioning resources and configure agent profiles for Windows and MAC OS X clients, and native supplicant profiles for your own personal devices.

- [Client Provisioning Resource Types, page 22-1](#)
- [Enabling and Disabling Client Provisioning, page 22-2](#)
- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)
- [Adding Client Provisioning Resources from a Local Machine, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)
- [Client Login Session Criteria, page 22-5](#)
- [Cisco ISE Agents, page 22-5](#)
- [Creating an Agent Customization File, page 22-13](#)
- [Agent Profile Configuration Guidelines, page 22-14](#)
- [Agent Profile Parameters and Applicable Values, page 22-15](#)
- [Creating Windows Agent Profiles, page 22-23](#)
- [Creating Mac OS X Agent Profiles, page 22-24](#)
- [Creating Native Supplicant Profiles, page 22-25](#)
- [Configuring Personal Device Registration Behavior, page 22-26](#)
- [Provisioning Client Machines with the Cisco NAC Agent MSI Installer, page 22-27](#)
- [Configuring Client Provisioning Resource Policies, page 22-28](#)
- [Viewing Client Provisioning Reports, page 22-30](#)
- [Collecting Cisco NAC Agent Logs, page 22-31](#)

Client Provisioning Resource Types

Client-provisioning resource policies enable users to download and install resources on client devices. These resources must be installed on Cisco ISE before users can access them and include:

- Persistent and temporal agents:
 - Windows and Mac OS X Cisco Network Admission Control (NAC) Agents
 - Cisco NAC Web Agent

- Native supplicant profiles
- Agent profiles
- Native supplicant provisioning/installation wizards
- Agent compliance modules
- Agent customization packages

Related Topics

- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)
- [Adding Client Provisioning Resources from a Local Machine, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)
- [Configuring Client Provisioning Resource Policies, page 22-28](#)
- [*Posture Services on the Cisco ISE Configuration Guide*](#)

Enabling and Disabling Client Provisioning

Before You Begin

To ensure that 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.

-
- Step 1** Choose **Administration > System > Settings > Client Provisioning**.
- Step 2** From the Enable Provisioning drop-down list, choose **Enable** or **Disable**.
- Step 3** Click **Save**.

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.

What To Do Next

Set up system-wide client-provisioning functions according to the guidelines in the following topics:

- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)
- [Adding Client Provisioning Resources from a Local Machine, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)
- [Configuring Client Provisioning Resource Policies, page 22-28](#)

Related Topics

- [Specifying Proxy Settings in Cisco ISE, page 5-2](#)
- [Cannot Download Remote Client Provisioning Resources, page G-13](#)

Adding Client Provisioning Resources from Remote Sources

You can add client-provisioning resources from a remote source like Cisco.com. Depending on the resources that you select and available network bandwidth, Cisco ISE can take a few seconds or even a few minutes to download the new items and display them in the list of available client-provisioning resources.

Before You Begin

Ensure that you are able to access the appropriate remote location to download client-provisioning resources to Cisco ISE, by verifying that the proxy settings for your network are correctly configured.

-
Step 1	Choose Policy > Policy Elements > Results > Client Provisioning > Resources.
Step 2	Choose Add > Agent resources from Cisco site.
Step 3	Select one or more required resources from the list available in the Downloaded Remote Resources dialog box.
Step 4	Click Save.
-

What To Do Next

After you have successfully added client-provisioning resources to Cisco ISE, you can begin to configure client-provisioning resource policies.

Related Topics

- [Specifying Proxy Settings in Cisco ISE, page 5-2](#)
- [Client Provisioning Resource Types, page 22-1](#)
- [Adding Client Provisioning Resources from a Local Machine, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)
- [Creating an Agent Customization File, page 22-13](#)
- [Configuring Client Provisioning Resource Policies, page 22-28](#)
- [Cannot Download Remote Client Provisioning Resources, page G-13](#)

Adding Client Provisioning Resources from a Local Machine

You can add existing client-provisioning resources from a local machine (for example, files that you may have already downloaded from Cisco.com to your laptop).

Before You Begin

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 1.2](#).

If you are downloading the resource files manually from the Cisco.com, refer to “Cisco ISE Offline Updates” section in the [Release Notes for the Cisco Identity Services Engine, Release 1.2](#).

-
Step 1	Choose Policy > Policy Elements > Results > Client Provisioning > Resources.

- Step 2** Choose **Add > Add resource 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**.
-

What To Do Next

After you have successfully added client-provisioning resources to Cisco ISE, you can begin to configure client-provisioning resource policies.

Related Topics

- [Specifying Proxy Settings in Cisco ISE, page 5-2](#)
- [Client Provisioning Resource Types, page 22-1](#)
- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)
- [Creating an Agent Customization File, page 22-13](#)
- [Agent Profile Configuration Guidelines, page 22-14](#)
- [Configuring Client Provisioning Resource Policies, page 22-28](#)

Downloading Client Provisioning Resources Automatically

This function automatically uploads *all* available software from Cisco, many items of which may not be pertinent to your deployment.

Before You Begin

To ensure that 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. If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the default URL, try also pointing your Cisco ISE to <https://www.perfigo.com/ise/provisioning-update.xml>.

The default URL for downloading client-provisioning resources is <https://www.cisco.com/web/secure/pmbu/provisioning-update.xml>.

Cisco recommends manually uploading resources whenever possible rather than opting to upload them automatically.

-
- Step 1** Choose **Administration > System > Settings > Client Provisioning**.
- Step 2** From the **Enable Automatic Download** drop-down list, choose **Enable**.
- Step 3** Specify the URL where Cisco ISE searches for system updates in the Update Feed URL text box.
- Step 4** Click **Save**.
-

What To Do Next

Set up system-wide client-provisioning functions according to the guidelines in the following topics:

- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)
- [Adding Client Provisioning Resources from a Local Machine, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)
- [Configuring Client Provisioning Resource Policies, page 22-28](#)

Related Topics

- [Specifying Proxy Settings in Cisco ISE, page 5-2](#)
- [Cannot Download Remote Client Provisioning Resources, page G-13](#)

Client Login Session Criteria

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 antispysware vendor support, and correct agent customization packages and profiles, if necessary.

Cisco ISE Agents

Agents are applications that reside on client machines logging into the Cisco ISE network. Agents can be persistent (like the Cisco NAC Agent or Mac OS X Agent) and remain on the client machine after installation, even when the client is not logged into the network, or Agents can be temporal (like the Cisco NAC Web Agent), removing themselves from the client machine after the login session has terminated. In either case, the Agent helps the user log in to the network, receive the appropriate access profile, and even perform posture assessment on the client machine to ensure it complies with network security guidelines before accessing the core of the network.

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 antispysware definition updates, launch qualified remediation programs, distribute files uploaded to the Cisco ISE server, distribute website links to websites for users to download files to fix their system, or simply distribute information and instructions.

Cisco strongly recommends that you ensure that the latest Windows hotfixes and patches are installed on Windows XP clients so that the Cisco NAC Agent can establish a secure and encrypted communication with Cisco ISE (via SSL over TCP).

Uninstalling Cisco NAC Agent for Windows Clients

The NAC 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**.
-

Related Topics

- [Cisco Identity Services Engine Network Component Compatibility, Release 1.2.](#)

Windows 8 Metro and Metro App Support—Toast Notifications

The **Enable Toast Notification** option is available on the Cisco NAC Agent Tray Icon, only for clients using Windows 8 as Operating System. You can enable this option to send relevant notifications to the user.

In Cisco NAC Agent scenarios where the user does not get network access, like “Remediation Failed” or “Network Access expired”, the Agent displays the following toast notification:

Network not available, Click “OK” to continue

To get more details, you can select the toast and you will be redirected to Desktop mode and the NAC agent dialog is displayed.

Toast Notification is displayed for all positive recommended actions that the user needs to perform to gain network access. The following are some examples:

- For Network Acceptance policy, toast will be displayed as: “Click Accept to gain network access”
- For Agent/Compliance Module Upgrade, toast will be displayed as: “Click OK to Upgrade/Update”
- In the “user logged out” event, when “Auto Close” option for Logoff is not enabled in CAM, toast notification is provided. This toast enables the users to know that they have been logged out and that they need to login again to get network access.

Cisco NAC Agent for Macintosh Clients

The Mac OS X Agent provides the posture assessment and remediation for Macintosh client machines. Users can download and install the Mac OS X Agent (read-only client software), which can check antivirus and antispware definition updates.

After users log in to the Mac OS X 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 restricted network access while the user tries to remediate the client system.

Related Topics

- [Cisco Identity Services Engine Network Component Compatibility, Release 1.2.](#)

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 <i><local drive ID></i> > 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.
-

Cisco 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. The Web Agent is available only for Windows clients and not for Mac OSX clients.

After users log in to 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 machine, 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.



Note

ActiveX is supported only on the 32-bit versions of Internet Explorer. You cannot install ActiveX on a Firefox web browser or on a 64-bit version of Internet Explorer.

Related Topics

- [Cisco Identity Services Engine Network Component Compatibility, Release 1.2.](#)

Agent Login Screen Customization

You can customize the elements that appear on the Cisco NAC Agent login screen. Once you have customized these elements, you then combine them with an “updateFeed.xml” XML descriptor file in a final .zip file (Agent login customization package) package to upload to Cisco ISE.

Windows client users see when they access your network via the Cisco NAC Agent by modifying the nac_login.xml file, replacing the default Cisco logo with your own corporate/company logo in the form of a .gif file named “nac_logo.gif file,” and creating one or more “nacStrings_xx.xml” files.

Figure 22-1 Cisco NAC Agent Login—Default Screen

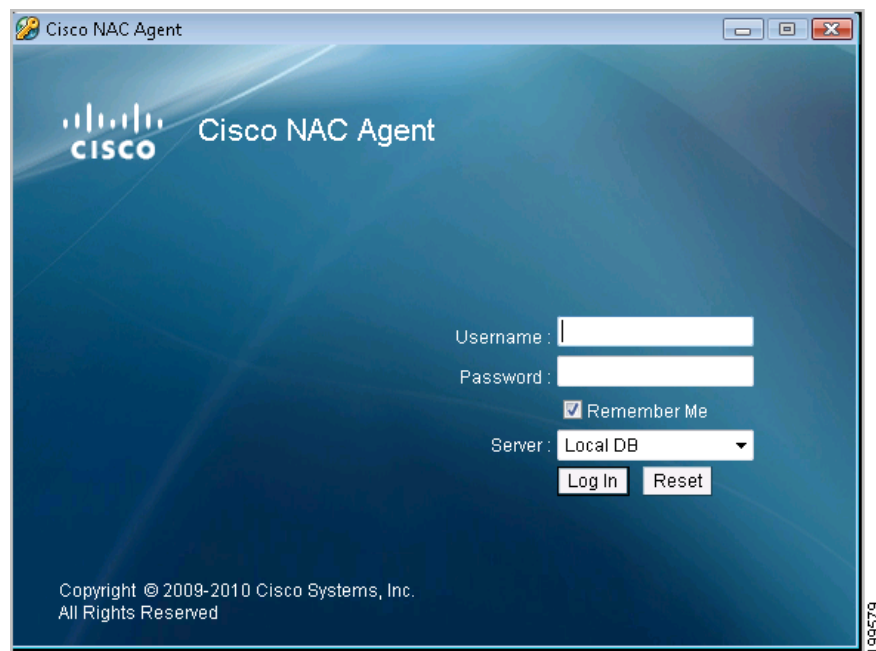
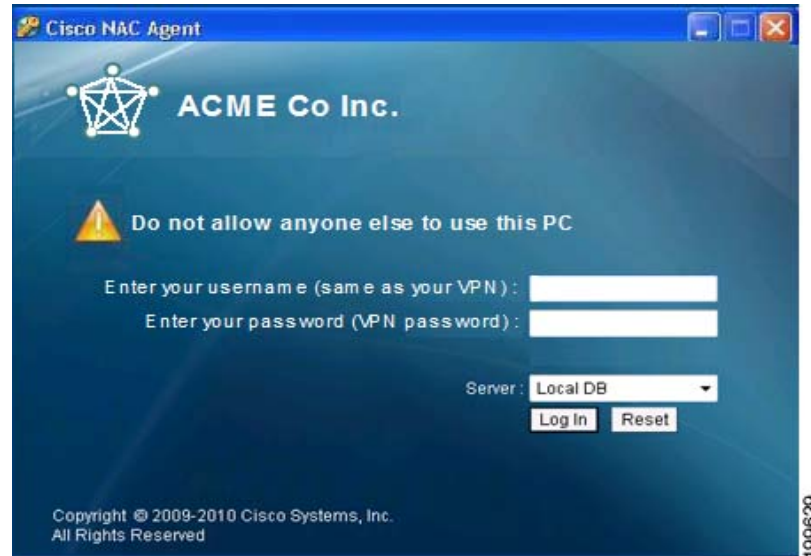


Figure 22-2 Cisco NAC Agent Login—Sample Customized Screen**Related Topics**

- [Custom nac_login.xml File Template, page 22-9](#)
- [Using a Custom Corporate/Company Logo, page 22-10](#)
- [Custom nacStrings_xx.xml File Template, page 22-11](#)
- [UpdateFeed.xml Descriptor File Template, page 22-12](#)
- [Creating an Agent Customization File, page 22-13](#)
- [Agent XML File Installation Directories, page 22-14](#)

Custom nac_login.xml File Template

This is one of the files that is required in your Agent login customization package, which allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent login dialog to suit your specific Windows client network access requirements.

Use the following template to construct an appropriate “nac_login.xml” file.

The following example shows customized text 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>
          </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>
```

Related Topics

- [Agent Login Screen Customization, page 22-8](#)
- [Using a Custom Corporate/Company Logo, page 22-10](#)
- [Custom nacStrings_xx.xml File Template, page 22-11](#)
- [Sample Extended nacStrings_xx.xml File, page 22-11](#)
- [UpdateFeed.xml Descriptor File Template, page 22-12](#)
- [Creating an Agent Customization File, page 22-13](#)
- [Agent XML File Installation Directories, page 22-14](#)

Using a Custom Corporate/Company Logo

You can replace the Cisco logo that appears in all the Cisco NAC Agent screens with your corporate/company logo.

Before You Begin

This is one of the files that is required in your Agent login customization package, which allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent login dialog to suit your specific Windows client network access requirements.

Be sure the image is a .gif file, not exceeding 67 x 40 pixels. Be sure to name the image “nac_logo.gif.”

Related Topics

- [Agent Login Screen Customization, page 22-8](#)
- [Custom nac_login.xml File Template, page 22-9](#)
- [Custom nacStrings_xx.xml File Template, page 22-11](#)
- [Sample Extended nacStrings_xx.xml File, page 22-11](#)
- [UpdateFeed.xml Descriptor File Template, page 22-12](#)
- [Creating an Agent Customization File, page 22-13](#)
- [Agent XML File Installation Directories, page 22-14](#)

Custom nacStrings_xx.xml File Template

This is one of the files that is required in your Agent login customization package, allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent login dialog to suit your specific Windows client network access requirements.

Use the following template to construct a one or more nacStrings_xx.xml files, where the xx is a two-character identifier for the specific language.

The following example shows customized text in boldface.

```
<cueslookup:name key="login.productname"> XYZ 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>
```



Note

There is no limit to the number of characters you can use for the customized text. However, Cisco recommends restricting the length so that these fields do not take up too much space in the resulting customized login screen as it appears on the client.

Related Topics

- [Agent Login Screen Customization, page 22-8](#)
- [Custom nac_login.xml File Template, page 22-9](#)
- [Using a Custom Corporate/Company Logo, page 22-10](#)
- [Sample Extended nacStrings_xx.xml File, page 22-11](#)
- [UpdateFeed.xml Descriptor File Template, page 22-12](#)
- [Creating an Agent Customization File, page 22-13](#)
- [Agent XML File Installation Directories, page 22-14](#)

Sample Extended 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>

```

UpdateFeed.xml Descriptor File Template

This is one of the files that is required in your Agent login customization package, allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent login dialog to suit your specific Windows client network access requirements.

Before you can complete your Agent login customization package, you must construct a suitable **updateFeed.xml** XML descriptor file. Use the following example as a template to set up the updateFeed.xml file required for your customization package.

```

<?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" />
  </entry>

```



```
<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>
```

Related Topics

- [Agent Login Screen Customization, page 22-8](#)
- [Custom nac_login.xml File Template, page 22-9](#)
- [Using a Custom Corporate/Company Logo, page 22-10](#)
- [Custom nacStrings_xx.xml File Template, page 22-11](#)
- [Sample Extended nacStrings_xx.xml File, page 22-11](#)
- [Creating an Agent Customization File, page 22-13](#)
- [Agent XML File Installation Directories, page 22-14](#)

Creating an Agent Customization File

An agent customization file allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent login dialog to suit your specific Windows client network access requirements.

You can create a customization package as a .zip file that contains an XML descriptor file and another .zip file with the contents comprising the customized options.

-
- Step 1** Assemble the files required to comprise your Agent login customization package:
- Customized nac_login.xml file
 - Customized corporate/company logo as a .gif file
 - One or more customized nacStrings_xx.xml files
 - Customized updateFeed.xml descriptor file
- Step 2** Create a zip file called “brand-win.zip” that contains the assembled files. For example, in a Linux or Unix environment, execute the following:
- ```
zip -r brand-win.zip nac_login.xml nac_logo.gif nacStrings_en.xml nacStrings_cy.xml
 nacStrings_el.xml
```
- Step 3** Create a “custom.zip” file that contains an appropriate updateFeed.xml descriptor file and the .zip file created above. For example, in a Linux or Unix environment, execute the following:
- ```
zip -r custom.zip updateFeed.xml brand-win.zip
```
- Step 4** Save the resulting “custom.zip” file to a location on a local machine that you can access when uploading the file to Cisco ISE.
-

Related Topics

- [Agent Login Screen Customization, page 22-8](#)
- [Custom nac_login.xml File Template, page 22-9](#)
- [Using a Custom Corporate/Company Logo, page 22-10](#)

- [Custom nacStrings_xx.xml File Template, page 22-11](#)
- [Sample Extended nacStrings_xx.xml File, page 22-11](#)
- [UpdateFeed.xml Descriptor File Template, page 22-12](#)
- [Agent XML File Installation Directories, page 22-14](#)

Agent XML File Installation Directories

In a system where the Cisco NAC Agent installed at the default location, you can find these .xml 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.

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”.

Related Topics

- [Agent Login Screen Customization, page 22-8](#)
- [Custom nac_login.xml File Template, page 22-9](#)
- [Using a Custom Corporate/Company Logo, page 22-10](#)
- [Custom nacStrings_xx.xml File Template, page 22-11](#)
- [Sample Extended nacStrings_xx.xml File, page 22-11](#)
- [UpdateFeed.xml Descriptor File Template, page 22-12](#)
- [Creating an Agent Customization File, page 22-13](#)

Agent Profile Configuration Guidelines

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.

Once you configure and upload an agent profile to a client device via policy enforcement or another method, that agent profile remains on the client and affects 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 clients. 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 and upload it via policy enforcement.

If Cisco ISE has a different agent profile than what is present on the client (which is determined using MD5 checksum), then Cisco ISE downloads the new agent profile to the client. If the agent customization file originating from Cisco ISE is different, Cisco ISE also downloads the new agent customization file to the client. See for more details.

Related Topics

- [Posture Administration Settings, page 23-5](#)
- [Creating an Agent Customization File, page 22-13](#)

Agent Profile Parameters and Applicable Values

Agent configuration parameters are grouped by function.

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.

Table 22-1 *Access to Authentication VLAN Change Detection on Clients with Multiple Active NICs*

Parameter	Default Value	Valid Range	Usage Guidelines
VLAN detect interval	0 ¹ , 5 ²	0, 5-900	• 0—Access to Authentication VLAN change feature is disabled • 1-5—Agent sends ICMP or ARP queries every 5 seconds • 6-900—An ICMP or ARP query is sent every x seconds
Enable VLAN detect without UI?	no	yes or no	• no—VLAN detect feature is disabled • yes—VLAN detect feature is enabled Note This setting does not apply to Mac OS X clients.

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 22-2 *Customize Agent Login/Logout Dialog Behavior*

Parameter	Default Value	Valid Range	Usage Guidelines
Disable Agent Exit?	no	yes or no	yes—Users cannot exit the Agent via the system tray icon Note This setting does not apply to Mac OS X clients.
Allow CRL Checks?	yes	yes or no	no—Turns off certificate revocation list (CRL) checking during discovery and negotiation Note This setting does not apply to Mac OS X clients.

Table 22-2 *Customize Agent Login/Logout Dialog Behavior (continued)*

Parameter	Default Value	Valid Range	Usage Guidelines
Accessibility mode?	no	yes or no	1—Agent is compatible with the Job Access with Speech (JAWS) screen reader 0—Agent does not interact with the JAWS screen reader 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 clients.
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 a Launch Program Remediation, page 23-16. Note This setting does not apply to Mac OS X clients.
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. Avoiding this step reduces or eliminates user interaction during the Agent login and remediation session. Note This setting does not apply to Mac OS X clients.

Table 22-3 *Manage Client-side MAC Address and Agent Discovery Host*

Parameter	Default Value	Valid Range	Usage Guidelines
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 clients.
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.

Table 22-3 Manage Client-side MAC Address and Agent Discovery Host (continued)

Parameter	Default Value	Valid Range	Usage Guidelines
Discovery host editable?	yes	yes or no	yes—(default value) User can specify a custom value in the Discovery Host field in the Agent Properties dialog box no—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 clients.
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 authorization is not performed. If any of the names are not found, then an error is reported. The server names should be FQDN names. You can use wildcard characters (asterisks [*]) to specify Cisco ISE node names with similar characters. For example, *.cisco.com matches all servers in the Cisco.com domain. Note This setting does not apply to Mac OS X clients.
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 clients.

Table 22-4 Specify Agent Localization Settings

Parameter	Default Value	Valid Range	Usage Guidelines
Language Info	OS setting (“default”)	—	default—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. See Table 22-5. “Supported Languages”. Note This setting does not apply to Mac OS X clients.

Table 22-5 Supported Languages

Language	ID	Abbreviated Name	Full Name
English US	1033	en	English
Catalan	1027	ca	Catalan (Spain)
ChineseSimplified	2052	zh_cn	Chinese (Simplified)

Table 22-5 **Supported Languages**

Language	ID	Abbreviated Name	Full Name
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
Polish	1045	pl	Polish
Portuguese	2070	pt	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 22-6 Report and Log Display Settings

Parameter	Default Value	Valid Range	Usage Guidelines
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. displayAll—Client posture assessment report appears, displaying all results when the user clicks Show Details in the Agent dialog displayFailed—(default value) 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 clients.
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. 0—Agent does not record any login or operation information for the user session on the client machine - any other integer—Agent records login and session information up to the number of megabytes that is specified¹

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 22-7 Recurring Client Machine Connection Verification

Parameter	Default Value	Valid Range	Usage Guidelines
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 <i>x</i> times before refreshing the client IP address.
Ping ARP	0	0-2	0—Poll using ICMP 1—Poll using ARP 2—Poll using ICMP first, then (if ICMP fails) ARP
Max Timeout for Ping	1	1-10	Poll using ICMP, and if there is no response in <i>x</i> seconds, then declare an ICMP polling failure.

Table 22-8 **Additional SWISS Discovery Customization**

Parameter	Default Value	Valid Range	Usage Guidelines
Swiss timeout	1	1 and above	1—Agent performs SWISS discovery as designed and no additional UDP response packet delay timeout value is introduced - an integer greater than 1—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. (SwissTimeout works only for UDP SWISS timeouts.) Note This setting does not apply to Mac OS X clients.
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 seconds, just like Layer 2 packets. The default setting is no. Note This setting does not apply to Mac OS X clients.

Table 22-9 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 seconds, 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.
Http timeout	120	0, 3 and above	Set by default at 120 seconds, 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, and the discovery process times out. The valid range is 3 seconds 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 22-10 Remediation Timeout Customization

Parameter	Default Value	Valid Range	Usage Guidelines
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 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 <i>both</i>.

Table 22-11 Agent Dialog Behavior on User Logout or Shutdown

Parameter	Default Value	Valid Range	Usage Guidelines
Enable auto close login screen?	no	yes or no	Allows you to determine whether or not the Agent login dialog in to 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.

Table 22-12 IP Address Behavior Settings for Client Machines

Parameter	Default Value	Valid Range	Usage Guidelines
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 the 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 <i>both</i>.

Table 22-12 IP Address Behavior Settings for Client Machines (continued)

Parameter	Default Value	Valid Range	Usage Guidelines
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.

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.

Creating Windows Agent Profiles

You can configure Agent profiles in Cisco ISE that specify how Windows clients behave when logging into your protected network. 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.

Before You Begin

Before you create a Windows agent profile, Cisco recommends uploading agent software to Cisco ISE:

- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)

- [Adding Client Provisioning Resources from a Local Machine, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)

-
- Step 1** Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.
- Step 2** Choose **Add > 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.
- Step 5** Click **Submit**.
-

What To Do Next

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.

Related Topics

- [Agent Profile Configuration Guidelines, page 22-14](#)
- [Agent Profile Parameters and Applicable Values, page 22-15](#)
- [Example XML File Generated Using the Create Profile Function, page 22-23](#)
- [Configuring Client Provisioning Resource Policies, page 22-28](#)

Creating Mac OS X Agent Profiles

You can configure Agent profiles in Cisco ISE that specify how Mac OS X clients behave when logging into your protected network. 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.

The parameters available to configure for Mac OS X client machines are only a subset of those available for Windows client machines. Cisco recommends that 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 clients.

Before You Begin

Before you create a Mac OS X agent profile, Cisco recommends uploading agent software to Cisco ISE:

- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)
- [Adding Client Provisioning Resources from a Local Machine, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)

-
- Step 1** Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.
- Step 2** Choose **Add > ISE Posture Agent 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.
- Step 5** Click **Submit**.
-

What To Do Next

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.

Related Topics

- [Configuring Client Provisioning Resource Policies, page 22-28](#)
- [Agent Profile Configuration Guidelines, page 22-14](#)
- [Agent Profile Parameters and Applicable Values, page 22-15](#)
- [Example XML File Generated Using the Create Profile Function, page 22-23](#)

Creating Native Supplicant Profiles

You can create native supplicant profiles to enable users to bring their own devices into the Cisco ISE network. When the user logs in, based on the profile that you associate with that user's authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard needed to set up the user's personal device to access the network.

Before You Begin

- If you intend to use a TLS device protocol for remote device registration, be sure you set up at least one Simple Certificate Enrollment Protocol (SCEP) profile, as described in [Simple Certificate Enrollment Protocol Profiles, page 8-30](#).
- Be sure to open up TCP port 8909 and UDP port 8909 to enable Cisco NAC Agent, Cisco NAC Web Agent, and supplicant provisioning wizard installation. For more information on port usage, see the "Cisco ISE Appliance Ports Reference" appendix in the [Cisco Identity Services Engine Hardware Installation Guide, Release 1.2](#).

-
- Step 1** Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.
- Step 2** Choose **Add > Native Supplicant Profile**.
- Step 3** Specify a Name for the agent profile.
- Step 4** Enter an optional Description for the Native Supplicant Profile.
- Step 5** Select an Operating System for this profile.
- Step 6** Enable the appropriate options for Wired or Wireless Connection Type (or both) for this profile. If you enable the Wireless connection option, be sure to also specify the device SSID and the wireless Security type (either WPA2 Enterprise or WPA Enterprise).
- Step 7** Choose the Allowed Protocol for the device profile.
- Step 8** Enable or disable other **Optional Settings** as appropriate for this profile.

Step 9 Click **Submit**.

What To Do Next

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network, as described in the Support for multiple Guest Portals section.

Related Topics

- [Agent Profile Configuration Guidelines, page 22-14](#)
- [Support for Multiple Guest Portals, page 16-2](#)

Allowed Protocol Settings

Table 22-13 *Allowed Protocol Settings*

Parameter	Description
TLS	Use the TLS protocol to provide the highest level of device registration security. When you specify the TLS method, Cisco ISE generates a Certificate Signing Request for the device certificate and forwards an SCEP request to the applicable certificate registration authority. For more information on configuring a connection to an SCEP certificate authority, see Simple Certificate Enrollment Protocol Profiles, page 8-30 .
PEAP	In general, PEAP allows users to enter their access credentials when logging into the network, and accepts standard registration certificates in return.
EAP-FAST	Use EAP-FAST to connect Apple iOS and Mac OS X devices. Connection typically takes place independent of certificate type and presence. Note Due to Apple iOS default behavior on iPhones and iPads, Cisco ISE does not support using the EAP-FAST protocol in the native supplicant profile when connecting via a <i>single</i> Service Set Identifier (SSID). When logging into the Cisco ISE network, iOS-based devices automatically negotiate using the PEAP-MSCHAPv2 protocol by default, even if the supplicant provisioning profile that is installed on the device specifies the EAP-FAST protocol. In a dual SSID environment, iOS-based devices should not face this restriction.

Configuring Personal Device Registration Behavior

Use this function to specify how Cisco ISE should handle user login sessions via personal devices on which Cisco ISE cannot install a native supplicant provisioning wizard (like Research In Motion Blackberry devices).

Step 1 Choose **Administration > System > Settings > Client Provisioning**.

Step 2 From the Native Supplicant Provisioning Policy Unavailable drop-down list, choose one of the following two options:

- **Allow Network Access**—Users are allowed to register their device on the network without having to install and launch the native supplicant wizard.

- **Apply Defined Authorization Policy**—Users must try to access the Cisco ISE network via standard authentication and authorization policy application (outside of the native supplicant provisioning process). If you enable this option, the user device goes through standard registration according to any client-provisioning policy applied to the user's ID. If the user's device requires a certificate to access the Cisco ISE network, you must also provide detailed instructions to the user describing how to obtain and apply a valid certificate using the customizable user-facing text fields, as described in the “Adding a Custom Language Template” section in the Chapter 15, Setting up and Customizing End_User Web Portals.

Step 3 Click **Save**.

What To Do Next

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network, as described in the Support for multiple Guest Portals section.

Related Topics

- [Support for Multiple Guest Portals, page 16-2](#)
- [Adding a Custom Language Template, page 15-4](#)

Provisioning Client Machines with the Cisco NAC Agent MSI Installer

You can place the MSI installer in a directory or a zip version of the same installer 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://software.cisco.com/download/navigator.html>.

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. If you are not connected to Cisco 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.

Step 4 Open a Command prompt on the client machine and enter the following to execute the installation:

```
msiexec.exe /i NACAgentSetup-win-<version>.msi /qn /l*v c:\temp\agent-install.log
```

(The `/qn` qualifier installs the Cisco NAC Agent completely silently. The `/1*v` logs the installation session in verbose mode.)

To uninstall the NAC Agent, you can execute the following command:

```
msiexec /x NACAgentSetup-win-<version>.msi /qn
```

**Note**

Installing a new version of the Agent using MSI will uninstall the old version and install the new version using the above commands.

- Step 5** If you are using Altiris/SMS to distribute the MSI installer, 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.

Related Topics

- [Example XML File Generated Using the Create Profile Function, page 22-23](#)
- [Creating Windows Agent Profiles, page 22-23](#)

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 existing one, if any, available in the system.

Before You Begin

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 5-2.](#)
- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)
- [Adding Client Provisioning Resources from a Local Machine, page 22-3](#)
- [Downloading Client Provisioning Resources Automatically, page 22-4](#)

- Step 1** Choose **Policy > Client Provisioning**.

- Step 2** Choose **Enable**, **Disable**, or **Monitor** from the behavior drop-down list:

- **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.

- Step 3** Enter a name for the new resource policy in the Rule Name text box.

- 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 that you have configured.
- Step 5** Use the Operating Systems field to specify one or more operating systems that might be running on the client machine or device through which the user is logging into Cisco ISE.
- You can choose to specify a single operating system like “Android,” “Mac iOS,” and “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).”
- Step 6** In the Other Conditions field, specify a new expression that you want to create for this particular resource policy.
- Step 7** For client machines, specify which agent type, compliance module, agent customization package, and/or profile to make available and provision on the client machine based on the categorization defined in the preceding topic.
- Choose an available agent from the **Agent** drop-down list and 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 Agent customization package updates are always mandatory.

- Choose an existing agent profile from the **Profile** drop-down list.
- Choose an available 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 these three resource types by clicking the Action icon and choosing **Download Resource** or **Upload Resource** from the drop-down list. This opens the Downloaded Remote Resources or Manual Resource Upload dialog box, where you can download one or more resources to Cisco ISE, as described in the “Adding Client_Provisioning Resources from Remote Sources” and “Adding Client_Provisioning Resources from a Local Machine” sections.

- Choose an available agent customization package for the client machine from the **Agent Customization Package** drop-down list.

Starting from Cisco ISE Release 1.2, it is mandatory to include the client provisioning URL in authorization policy, to enable the NAC Agent to popup in the client machines. This prevents request from any random clients and ensures that only clients with proper redirect URL can request for posture assessment.

- Step 8** For personal devices, specify which Native Supplicant Configuration to make available and provision on the registered personal device based on the categorization defined above:
- Choose the specific **Configuration Wizard** to distribute to these personal devices.
 - Specify the applicable **Wizard Profile** for the given personal device type.
- Step 9** Click **Save**.

What To Do Next

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.

Related Topics

- [Chapter 23, “Configuring Client Posture Policies.”](#)

Viewing Client Provisioning Reports

You can 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.

Related Topics

- [Viewing Client Provisioning Requests, page 22-30](#)
- [Viewing Client Access Sessions, page 22-30](#)
- [Viewing Client Provisioning Resource Configuration Changes, page 22-30](#)
- [Viewing Supplicant Provisioning Requests, page 22-31](#)
- [Viewing Client Provisioning Event Logs, page 22-31](#)

Viewing Client Provisioning Requests

The **Operations > Reports > ISE Reports > Endpoints and Users > Client Provisioning** page displays statistics about successful and unsuccessful client-provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client-provisioning data.

Viewing Client Access Sessions

The **Operations > Reports > Catalog > User > Unique Users** page displays statistics about known specific client access sessions initiated during the specified time period. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client-provisioning data.

Viewing Client Provisioning Resource Configuration Changes

The **Operations > Reports > Catalog > Server Instance > Server Configuration Audit** page displays information about recent client-provisioning resource configuration changes. 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.

Viewing Supplicant Provisioning Requests

The **Operations > Reports > Catalog > User > Supplicant Provisioning** window displays information about recent successful and unsuccessful user device registration and supplicant provisioning requests. When you choose **Run** and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting supplicant provisioning data.

The Supplicant Provisioning report provides information about a list of endpoints that are registered through the device registration portal for a specific period of time, including data like the Logged In Date and Time, User ID, IP Address, MAC Address, Server, Operating System, SPW Version, Failure Reason (if any), and the Status of the registration.

Viewing Client Provisioning Event Logs

You can search event log entries 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.

Related Topics

- [Chapter 11, “Logging”](#)

Collecting Cisco NAC Agent Logs

In Cisco NAC Agent for Windows, right-click the Agent Tray Icon and then click **Log Packager** to run the support package and collect the logs.

In Cisco NAC Agent for Mac OS X, in the Tools menu, right-click the Agent icon and click the **Collect Support Logs** option to collect the Agent logs and support information. The collected information is available as a zip file. The user can save the file by choosing the file location and filename. By default the file is saved on the desktop with the filename as *CiscoSupportReport.zip*.

If the Agent crashes or hangs, you can run the **CCAAgentLogPackager.app** to collect the logs. This file is available at **/Applications/CCAAgent.app**. You can right-click **CCAAgent.app**, select **Show Package Contents** and double-click **CCAAgentLogPackager** to collect the support information.



Configuring Client Posture Policies

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients to access protected areas of a network.

This chapter describes the posture service in Cisco ISE in the following topics:

- [Posture Service, page 23-1](#)
- [Posture Administration Settings, page 23-5](#)
- [Configuring Posture Policies, page 23-11](#)
- [Posture Assessment Options, page 23-12](#)
- [Custom Conditions for Posture, page 23-13](#)
- [Custom Posture Remediation Actions, page 23-13](#)
- [Custom Permissions for Posture, page 23-20](#)
- [Configuring Standard Authorization Policies, page 23-21](#)

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. The NAC Agents assist you in evaluating the clients against the posture policies and enforcing the security policies on clients to meet the compliance.

The NAC Agent for Cisco 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.

Client Provisioning is a service to ensure that the clients are setup with appropriate Agents that provide posture assessment and remediation for the clients.

Related Topics

- [Components of Posture Services, page 23-2](#)
- [Running Posture Reports, page 23-5](#)

Components of Posture Services

Cisco ISE posture service primarily includes the posture administration services and the posture run-time services.

Posture Administration Services

If you have not installed the advanced license in Cisco ISE, then the posture administration services option is not available from the Admin portal.

Administration services provide the back-end support for posture-specific custom conditions and remediation actions that are associated with the requirements and authorization policies that are configured for posture service.

Posture Run-time Services

The posture run-time services encapsulate 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.

The SWISS protocol is a stateless request response protocol that allows NAC Agents 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.

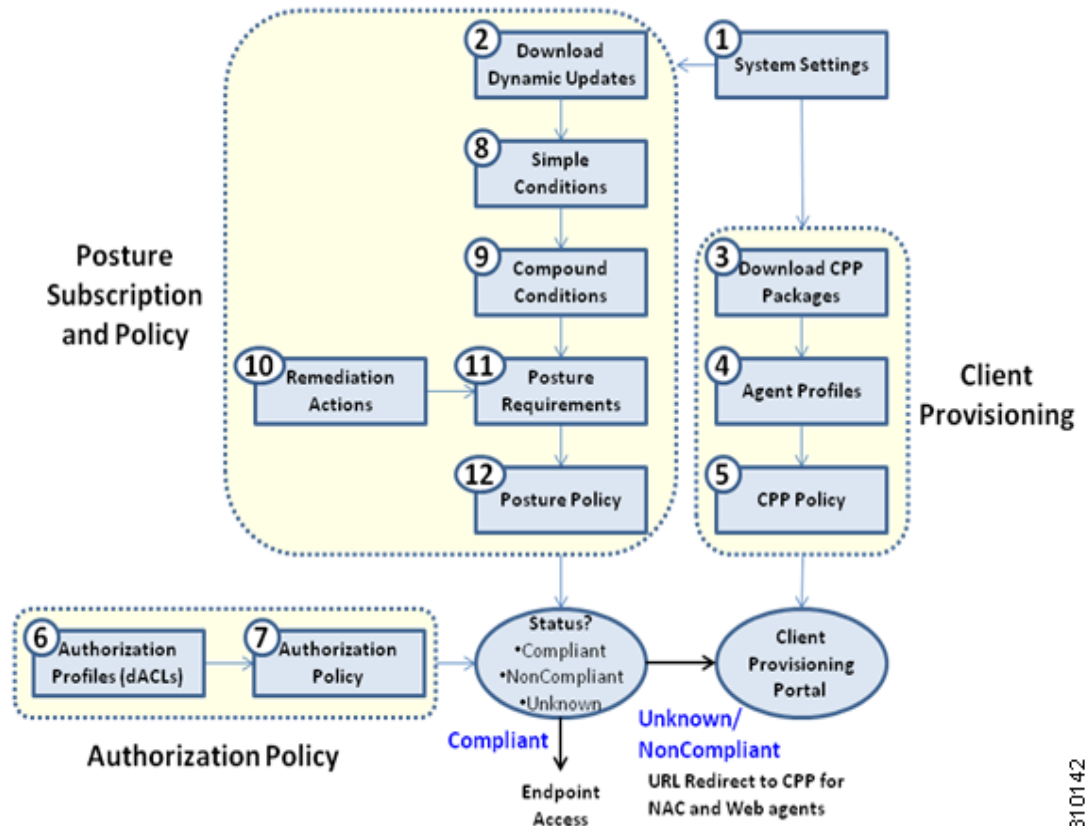
The SWISS request message that comes from the client machine includes information pertaining to resource types for the following items:

- Agent profiles
- Agent compliance modules
- Agent customization package

In addition to answering these request items, the SWISS response from the Cisco ISE server can also contain prompts to update the current Agent and URLs that are required to perform posture assessment and remediation on the client machine.

Posture and Client-Provisioning Policies Workflow

Figure 23-1 Posture and Client Provisioning Policies Workflow in Cisco ISE



Related Topics

- [Configuring Client Provisioning Resource Policies](#), page 22-28
- [Chapter 22, “Configuring Client Provisioning.”](#)
- [Cisco Identity Services Engine Network Component Compatibility, Release 1.2](#)

Posture Service Licenses

Cisco ISE provides you with two types of licenses, the base license and advanced license. You must install the base license for the basic services or the advanced license for all the services of Cisco ISE. Depending on the type of deployment and the license you have installed, the posture service of Cisco ISE can run on a single node or on multiple nodes. You also have an evaluation license which can be upgraded to the appropriate base or advanced license once the evaluation license period is over.

If you have not installed the advanced license on the 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. The posture run-time services takes appropriate action when

you add or remove any advanced license file to the 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.

Posture Service Deployment

You can deploy Cisco ISE in a standalone environment (on a single node) or in a distributed environment (on multiple nodes).

In a standalone Cisco ISE deployment, you can configure a single node for all the administration services, the monitoring and troubleshooting services, and the policy run-time services.

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.

Deploying Posture Session Service

You must enable session services in Cisco ISE and install the advanced licence package to initialize the SWISS server and serve all the posture requests received from the clients.

Before You Begin

- If you have more than one node that is registered in a distributed deployment, all the nodes that you have registered appear in the Deployment Nodes page, apart from the primary node. You can configure each node as a Cisco ISE node (Administration, Policy Service, and Monitoring personas) or an Inline Posture node.
- 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 1	Choose Administration > System > Deployment > Deployment .
Step 2	Choose a Cisco ISE node from the Deployment Nodes page.
Step 3	Click Edit .
Step 4	On the General settings tab, check the Policy Service check box, If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.
Step 5	Check the Enable Session Services check box, for the Policy Service persona to run the Network Access, Posture, Guest, and Client Provisioning session services. To stop the session services, uncheck the check box.
Step 6	Click Save .
-

Running Posture Reports

You can run the Posture Detail Assessment report to generate a detailed status of compliance of the clients against the posture policies that are used during posture assessment.

-
Step 1	Choose Operations > Reports > ISE Reports > Endpoints and Users > Posture Detail Assessment .
Step 2	Click the Time Range drop-down arrow and select the specific time period.
Step 3	Click Run to view the summary of all the endpoints that logged on for a selected period of time.
-

Related Topics

- [Chapter 26, “Reporting.”](#)

Posture Administration Settings

You can globally configure the Admin portal for posture services. You can download updates automatically to the Cisco ISE server through the web from Cisco. You can also update Cisco ISE manually offline later. In addition, the NAC Agents and Web Agents 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.

Related Topics

- [Timer Settings for Clients, page 23-5](#)
- [Setting Posture Status for Non-Agent Devices, page 23-7](#)
- [Periodic Reassessments, page 23-7](#)
- [Downloading Posture Updates, page 23-9](#)
- [Downloading Posture Updates Automatically, page 23-9](#)
- [Configuring Acceptable Use Policies for Posture Assessment, page 23-10](#)

Timer Settings for Clients

You can set up timers for users to remediate, to transition from one state to another, and to control the login success screen.

We recommend configuring agent profiles with remediation timers and network transition delay timers as well as the timer used to control the login success screen on client machines so that these settings are policy based. You can configure all these timers for agents in client provisioning resources in **Policy > Policy Elements > Results > Client Provisioning > Resources > Add > New Profile**.

However, when there are no agent profiles configured to match the client provisioning policies, you can use the settings in the **Administration > System > Settings > Posture > General Settings** configuration page.

Related Topics

- [Agent Profile Parameters and Applicable Values, page 22-15](#)
- [Setting Timer for Users to Remediate, page 23-6](#)
- [Setting Timer for Users to Transition, page 23-6](#)
- [Setting Timer to Automatically Close the Login Window, page 23-7](#)

Setting Timer for Users to Remediate

You can configure the timer for clients to remediate themselves within specified time. 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 send a report to the posture run-time services after which the clients are moved to the noncompliance state.

-
- Step 1** Choose **Administration > System > Settings > Posture > General Settings**.
- Step 2** Enter a time value in minutes, in the **Remediation Timer** field.
The default value is 4 minutes. The valid range is 1 to 300 minutes.
- Step 3** Click **Save**.
-

Related Topics

[Posture General Settings, page A-19](#)

Setting Timer for Users to Transition

You can configure the timer for clients to transition from one state to the other state within a specified time using the network transition delay timer, which is required for Change of Authorization (CoA) to complete. It may require a longer delay time when clients need time to get a new VLAN IP address during success and failure of posture. When successfully postured, Cisco ISE allows clients to transition from unknown to compliant mode within the time specified in the network transition delay timer. Upon failure of posture, Cisco ISE allows clients to transition from unknown to noncompliant mode within the time specified in the timer.

-
- Step 1** Choose **Administration > System > Settings > Posture > General Settings**.
- Step 2** Enter a time value in seconds, in the **Network Transition Delay** field.
The default value is 3 seconds. The valid range is 2 to 30 seconds.
- Step 3** Click **Save**.
-

Related Topics

- [Posture General Settings, page A-19](#)

Setting Timer to Automatically Close the Login Window

After successful posture assessment, the NAC Agents and Web Agents display a temporary network access screen. The user needs to click the OK button in the login screen to close it. You can set up a timer to close this login screen automatically after specified time.

-
Step 1	Choose Administration > System > Settings > Posture > General Settings .
Step 2	Check the Automatically Close Login Success Screen After check box.
Step 3	Enter a time value in seconds, in the field next to Automatically Close Login Success Screen After check box. The valid range is 0 to 300 seconds. If the time is set to zero, then the NAC Agents and Web Agents do not display the login success screen.
Step 4	Click Save .
-

Related Topics

- [Posture General Settings, page A-19](#)

Setting Posture Status for Non-Agent Devices

You can configure the posture status of endpoints that run on non-agent devices like Linux or iDevices. When Android devices and Apple iDevices such as an iPod, iPhone, or iPad connect to a Cisco ISE enabled network, these devices assume the Default Posture Status settings.

These settings can also be applied to endpoints that run on Windows and Macintosh operating systems when a matching policy is not found during posture runtime.

Before You Begin

In order to enforce policy on an endpoint with a matching Posture policy, you must configure a corresponding Client Provisioning policy (Agent installation package). Otherwise, the posture status of the endpoint automatically reflects the default setting. For details, see [Configuring Client Provisioning Resource Policies, page 22-28](#).

-
Step 1	Choose Administration > System > Settings > Posture > General Settings .
Step 2	From the Default Posture Status , choose the option as Compliant or Noncompliant .
Step 3	Click Save .
-

Related Topics

- [Posture General Settings, page A-19](#)

Periodic Reassessments

Periodic reassessment (PRA) configurations can be done only for clients that are already successfully postured for compliance. PRA cannot occur if clients are not compliant on your network.

The NAC Agent sends a compliance report to the policy service node once the client is postured successfully and is compliant on your network. A PRA is valid and applicable only if the endpoints are in a compliant state. 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 a 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 CoA request. The NAC Agent periodically sends the PRA requests based on the interval specified in the configuration. 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.

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 PostureStatus is updated in the Monitoring reports as well. The posture status is unknown when the PostureStatus attribute of any client before reassessment of new requirements and posture policies retrieved from the server in a PRA request assuming that the client is being postured after successful authentication.

Related Topics

- [Configuring Periodic Reassessments, page 23-8](#)

Configuring Periodic Reassessments

You can configure periodic reassessments only for clients that are already successfully postured for compliance. You can configure each PRA to a user identity group that is defined in the system. If you configure a PRA with the *Any* role then only the configuration with this role exists, and no other configurations can exist in the system.

Before You Begin

- Ensure that each PRA configuration has a unique group or a unique combination of user identity groups assigned to the configuration.
- You can assign a `role_test_1` and a `role_test_2`, which are 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`.
- Ensure that two PRA configurations do not have a user identity group in common.
- If a PRA configuration already exists with a user identity group “Any”, you cannot create other PRA configurations unless you perform the following:
 - Update the existing PRA configuration with the Any user identity group to reflect a user identity group other than *Any*.
 - or
 - Delete the existing PRA configuration with a user identity group “Any”.

-
- Step 1** Choose **Administration > System > Settings > Posture > Reassessments**.
 - Step 2** Click **Add**.
 - Step 3** Modify the values in the **New Reassessment Configuration** page to create a new PRA.
 - Step 4** Click **Submit** to create a PRA configuration.
-

Related Topics

- [Posture Reassessment Configuration Settings, page A-19](#)

Downloading Posture Updates

Posture updates include a set of predefined checks, rules, and support charts for antivirus and antispyware for both Windows and Macintosh operating systems, and operating systems information that are supported by Cisco. 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 posture updates from the web. This process usually takes approximately 20 minutes. After the initial download, you can configure Cisco ISE to verify and download incremental updates to occur automatically.

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 manual or scheduled updates.

Before You Begin

To ensure that you are able to access the appropriate remote location from which you can download posture 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 5-2](#).

You can use the Posture Update page to download updates dynamically from the web.

-
- Step 1** Choose **Administration > System > Settings > Posture > Updates**.
 - Step 2** Choose the **Web** option to download updates dynamically.
 - Step 3** Click **Set to Default** to set the Cisco default value for the Update Feed URL field. The default Update Feed URL is <https://www.cisco.com/web/secure/pmbu/posture-update.xml>.
If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the above URL, try also pointing your Cisco ISE to <https://www.perfigo.com/ise/posture-update.xml>.
 - Step 4** Modify the values on the **Posture Updates** page.
 - Step 5** Click **Update Now** to download updates from Cisco.
 - Step 6** 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 section in the Posture Updates page.

Downloading Posture Updates Automatically

After an initial update, you can configure Cisco ISE to check for the updates and download them automatically.

Before You Begin

- You should have initially downloaded the posture updates to configure Cisco ISE to check for the updates and download them automatically. See [“Downloading Posture Updates” section on page 23-9](#).

-
- Step 1** Choose **Administration > System > Settings > Posture > Updates**.
- Step 2** In the **Posture Updates** page, check the **Automatically check for updates starting from initial delay** check box.
- Step 3** Enter the initial delay time in hh:mm:ss format.
Cisco ISE starts checking for updates after the initial delay time is over.
- Step 4** Enter the time interval in hours.
Cisco ISE downloads the updates to your deployment at specified intervals from the initial delay time.
- Step 5** Click **Yes** to continue.
- Step 6** Click **Save**.
-

**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.

Related Topics

- For details on performing offline posture package updates in Cisco ISE, refer to the “Cisco ISE Offline Updates” section of the [Release Notes for the Cisco Identity Services Engine, Release 1.2](#).
- [Adding Client Provisioning Resources from Remote Sources, page 22-3](#)
- [Configuring Client Provisioning Resource Policies, page 22-28](#)
- [Custom Conditions for Posture, page 23-13](#)

Configuring Acceptable Use Policies for Posture Assessment

After login and successful posture assessment of clients, the NAC Agents and Web Agents display a temporary network access screen. This screen contains a link to an acceptable use policy (AUP). When users click the link, they are redirected to a page that displays the network-usage terms and conditions, which they must read and accept.

Each Acceptable Use Policy configuration must have a unique user identity group, or a unique combination of 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 that displays the AUP.

-
- Step 1** Choose **Administration > System > Settings > Posture > Acceptable Use Policy**.
- Step 2** Click **Add**.
- Step 3** Modify the values in the **New Acceptable Use Policy Configuration** page.

Step 4 Click **Submit**.

Related Topics

- [Posture Acceptable Use Policy Configuration Settings, page A-20](#)

Configuring Posture 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.

Before You Begin

- You must have an understanding of acceptable use policy (AUP). See “[Configuring Acceptable Use Policies for Posture Assessment](#)” section on page 23-10
- You must have an understanding of periodic reassessments (PRA). See “[Configuring Periodic Reassessments](#)” section on page 23-8.

Step 1 Choose **Policy > Posture**.

Step 2 Choose the **Status** type.

Step 3 In the **Rule Name** text box, enter the policy name.

Step 4 From **identity Groups**, choose the role.

Step 5 From **Operating Systems**, choose the operating system.

Step 6 In **Other Conditions**, you can add one or more dictionary attributes and save them as simple or compound conditions to a dictionary.



Note Dictionary simple conditions and dictionary compound conditions that you create in the Posture Policy page are not visible while configuring an authorization policy.

Step 7 From **Requirements**, choose a requirement. You can also create a new Requirement.

Step 8 Click **Done**.

Step 9 Click **Save**.

Related Topics

- [Posture Assessment Options, page 23-12](#)
- [Creating Client Posture Requirements, page 23-19](#)
- [Creating Simple Posture Conditions, page 18-6](#)
- [Creating Compound Posture Conditions, page 18-7](#)
- [Time and Date Conditions, page 20-10](#)
- [Agent Fails to Initiate Posture Assessment, page G-32](#)
- [Posture Services on the Cisco ISE Configuration Guide](#)

Posture Assessment Options

The following table provides a list of posture assessment (posture conditions) options that are supported by the NAC Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 23-1 *Posture Assessment Options*

NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Operating System/Service Packs/Hotfixes	Operating System/Service Packs/Hotfixes	—
Process Check	Process Check	—
Registry Check	Registry Check	—
File Check	File Check	—
Application Check	Application Check	—
Antivirus Installation	Antivirus Installation	Antivirus Installation
Antivirus Version/ Antivirus Definition Date	Antivirus Version/ Antivirus Definition Date	Antivirus Version/ Antivirus Definition Date
Antispyware Installation	Antispyware Installation	Antispyware Installation
Antispyware Version/ Antispyware Definition Date	Antispyware Version/ Antispyware Definition Date	Antispyware Version/ Antispyware Definition Date
Windows Update Running	Windows Update Running	—
Windows Update Configuration	Windows Update Configuration	—
WSUS Compliance Settings	WSUS Compliance Settings	—

Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the NAC Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 23-2 *Posture Remediation Options*

NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	File Distribution	—
Launch Program	—	—

Table 23-2 *Posture Remediation Options (continued)*

NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh OS X
Antivirus Definition Update	—	Antivirus Live Update
Antispyware Definition Update	—	Antispyware Live Update
Windows Update	—	—
WSUS	—	—

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 with a posture requirement.

After an initial posture update, Cisco ISE also creates Cisco-defined simple and compound conditions. Cisco-defined simple conditions use the `pc_` as and compound conditions use `pr_` as.

A user-defined condition or a Cisco-defined condition includes both simple and compound conditions.

Posture service makes use of internal checks based on antivirus and antispyware (AV/AS) compound conditions. Hence, posture reports do not reflect the exact AV/AS compound-condition names that you have created. The reports display only the internal check names of AV/AS compound conditions.

For example, if you have created an AV compound condition named "MyCondition_AV_Check" to check any Vendor and any Product, the posture reports will display the internal check, that is "av_def_ANY", as the condition name, instead of "MyCondition_AV_Check".

Related Topics

- [Simple and Compound Conditions, page 18-1](#)
- [Posture Conditions, page 18-5](#)
- [Simple Posture Conditions, page 18-5](#)
- [Creating Simple Posture Conditions, page 18-6](#)
- [Compound Posture Conditions, page 18-6](#)
- [Creating Compound Posture Conditions, page 18-7](#)

Custom Posture Remediation Actions

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

Table 23-3 shows remediation types that are supported by NAC Web Agent and NAC Agents for Windows and Macintosh clients.

Table 23-3 Remediation Types Supported by Agents

Remediation Types	NAC Agent for Windows	Web Agent for Windows	NAC Agent for Macintosh
File Remediation	Supported	Supported	—
Link remediation (manual)	Supported	Supported	Supported
Link remediation (automatic)	Supported	Not supported	Not supported
Antivirus remediation (manual)	Supported	Not supported	Supported
Antivirus remediation (automatic)	Supported	Not supported	Not supported
Antispyware remediation (manual)	Supported	Not supported	Not supported
Antispyware remediation (automatic)	Supported	Not supported	Not supported
Launch Program remediation (manual)	Supported	Not supported	—
Launch Program remediation (automatic)	Supported	Not supported	—
Windows Update remediation (manual)	Supported	Not supported	—
Windows Update remediation (automatic)	Supported	Not supported	—
Windows Server Update Services remediation (manual)	Supported	Not supported	—
Windows Server Update Services remediation (automatic)	Supported	Not supported	—

Related Topics

- [Adding a File Remediation, page 23-15](#)
- [Adding a Link Remediation, page 23-15](#)
- [Adding an Antivirus Remediation, page 23-15](#)
- [Adding an Antispyware Remediation, page 23-16](#)
- [Adding a Launch Program Remediation, page 23-16](#)
- [Adding a Windows Update Remediation, page 23-17](#)
- [Adding a Windows Server Update Services Remediation, page 23-18](#)
- [Agent Fails to Initiate Posture Assessment, page G-32](#)

Adding a File Remediation

A file remediation allows clients to download the required file version for compliance. The NAC Agents and Web Agents remediate an endpoint with a file that is required by the client for compliance.

You can filter, view, add, or delete file remediations in the File Remediations page, but you cannot edit file remediations. The File Remediations page displays all the file remediations along with their name and description and the files that are required for remediation.

-
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
- Step 2** Click **Remediation Actions**.
- Step 3** Click **File Remediation**.
- Step 4** Click **Add**.
- Step 5** Modify the values in the **New File Remediation** page.
- Step 6** Click **Submit**.
-

Related Topics

- [File Remediation, page B-26](#)

Adding a Link Remediation

A link remediation allows clients to click a URL to access a remediation page or resource. The NAC Agents and Web Agents open a browser with the link and allow the clients to remediate themselves for compliance.

The Link Remediation page displays all the link remediations along with their name and description and their modes of remediation.

-
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
- Step 2** Click **Remediation Actions**.
- Step 3** Click **Link Remediation**.
- Step 4** Click **Add**.
- Step 5** Modify the values in the **New Link Remediation** page.
- Step 6** Click **Submit**.
-

Related Topics

- [Link Remediation, page B-26](#)

Adding an Antivirus Remediation

You can create an antivirus remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AV Remediations page displays all the antivirus remediations along with their name and description and their modes of remediation.

-
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
 - Step 2** Click **Remediation Actions**.
 - Step 3** Click **AV Remediation**.
 - Step 4** Click **Add**.
 - Step 5** Modify the values in the **New AV Remediation** page.
 - Step 6** Click **Submit**.
-

Related Topics

- [Antivirus Remediation, page B-26](#)

Adding an Antispyware Remediation

You can create an antispyware remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AS Remediations page displays all the antivirus remediations along with their name and description and their modes of remediation.

-
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
 - Step 2** Click **Remediation Actions**.
 - Step 3** Click **AS Remediation**.
 - Step 4** Click **Add**.
 - Step 5** Modify the values in the **New AS Remediations** page.
 - Step 6** Click **Submit**.
-

Related Topics

- [Antispyware Remediation, page B-27](#)

Adding a Launch Program Remediation

You can create a launch program remediation, where the NAC Agents and Web Agents remediate clients by launching one or more applications for compliance.

The Launch Program Remediations page displays all the launch program remediations along with their name and description and their modes of remediation.

-
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
 - Step 2** Click **Remediation Actions**.

- Step 3** Click **Launch Program Remediation**.
- Step 4** Click **Add**.
- Step 5** Modify the values in the **New Launch Program Remediation** page.
- Step 6** Click **Submit**.
-

Related Topics

- [Launch Program Remediation, page B-27](#)

Windows Update Remediation

Windows update remediation ensures that Automatic Updates configuration is turned on Windows clients per your security policy. Windows administrators have an option to turn on or turn off Automatic Updates on Windows clients. Microsoft Windows uses this feature to check for updates regularly. If the Automatic Updates feature is turned on, then Windows automatically updates Windows-recommended updates before any other updates.

The Windows Automatic Updates setting will differ for different Windows operating systems.

For example, Windows XP provides the following settings for configuring Automatic Updates:

- Automatic (recommended)—Windows allows clients to download recommended Windows updates and install them automatically
- 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 updates
- Notify me but don't automatically download or install them—Windows only notifies clients, but does not automatically download, or install updates
- Turn off Automatic Updates—Windows allows clients to turn off the Windows Automatic Updates feature. Here, clients are vulnerable unless clients install updates regularly, which can be done from the Windows Update Web site link.

You can check whether or not the Windows updates service (wuaserv) is started or stopped in any Windows client by using the **pr_AutoUpdateCheck_Rule**. This is a predefined Cisco rule, which can be used to create a posture requirement. If the posture requirement fails, the Windows update remediation that you associate to the requirement enforces the Windows client to remediate by using one of the options in Automatic Updates.

Related Topics

- [Adding a Windows Update Remediation](#)

Adding a Windows Update Remediation

The Windows Update Remediations page displays all the Windows update remediations along with their name and description and their modes of remediation.

-
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
- Step 2** Click **Remediation Actions**.
- Step 3** Click **Windows Update Remediation**.

- Step 4** Click **Add**.
 - Step 5** Modify the values in the **New Windows Update Remediation** page.
 - Step 6** Click **Submit**.
-

Related Topics

- [Windows Update Remediation, page B-28](#)

Adding a Windows Server Update Services Remediation

You can configure Windows clients to receive the latest WSUS updates from a locally administered or a Microsoft-managed WSUS server for compliance. A Windows Server Update Services (WSUS) remediation installs latest Windows service packs, hotfixes, and patches from a locally managed WSUS server or a Microsoft-managed WSUS server.

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.

-
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
 - Step 2** Click **Remediation Actions**.
 - Step 3** Click **Windows Server Update Services Remediation**.
 - Step 4** Click **Add**.
 - Step 5** Modify the values in the **New Windows Server Update Services Remediation** page.
 - Step 6** Click **Submit**.
-

Related Topics

- [Windows Server Update Services Remediation, page B-29](#)

Posture Assessment Requirements

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network.

Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue further during posture evaluation of endpoints.

Mandatory Requirements

If clients fail to meet mandatory requirements as defined in the posture policies, then they are provided with remediation options during policy evaluation. End users should remediate to meet the requirements within the time specified in the remediation timer settings.

If a client is unable to remediate a mandatory requirement, the posture status changes to “non-compliant” and the agent session is quarantined. To get the client out of a non-compliant state, refer to [“Client System Stuck in Noncompliant State” section on page 23-19](#).

Optional Requirements

If clients fail to meet optional requirements during policy evaluation, then the agent prompts end users with an option to continue further so that they can skip optional requirements.

Audit Requirements

Audit requirements are not shown to end users even though they pass or fail during policy evaluation.

Related Topics

- [Client System Stuck in Noncompliant State, page 23-19](#)
- [Custom Posture Remediation Actions, page 23-13](#)
- [Agent Fails to Initiate Posture Assessment, page G-32](#)

Client System Stuck in Noncompliant State

If a client machine is unable to remediate a mandatory requirement, the posture status changes to “noncompliant” and the agent session is quarantined. To get the client machine past this “noncompliant” state, you need to restart the posture session so that the agent starts posture assessment on the client machine again. You can restart the posture session as follows:

- In wired and wireless Change of Authorization (CoA) in an 802.1X environment:
 - You can configure the Reauthentication timer for a specific authorization policy when you create a new authorization profile in the New Authorization Profiles page. See the [“Configuring Permissions for Downloadable ACLs” section on page 20-13](#) for more information. This method is not supported in Inline Posture deployments.
 - 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 wireless lan controller (WLC) and wait until the user idle timeout period has expired before attempting to reconnect to the network.
- In a VPN environment—Disconnect and reconnect the VPN tunnel.

Related Topics

- [Configuring Posture Policies, page 23-11](#)
- [Custom Posture Remediation Actions, page 23-13](#)
- [Creating Client Posture Requirements, page 23-19](#)

Creating Client Posture Requirements

You can create a requirement in the Requirements page where you can associate user-defined conditions and Cisco defined conditions, and remediation actions. Once created and saved in the Requirements page, user-defined conditions and remediation actions can be viewed from their respective list pages.

Before You Begin

- You must have an understanding of acceptable use policies (AUPs) for a posture. See the [“Configuring Acceptable Use Policies for Posture Assessment” section on page 23-10.](#)

-
- Step 1** Choose **Policy > Policy Elements > Results > Posture > Requirements.**
- Step 2** Enter the values in the **Requirements** page.
- Step 3** Click **Done** to save the posture requirement in read-only mode.
- Step 4** Click **Save.**
-

Related Topics

- [Configuring Standard Authorization Policies, page 23-21](#)
- [Client Posture Requirements, page B-30](#)

Custom Permissions for Posture

A custom permission is a standard authorization profile that you define in Cisco ISE. 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. These profiles can be associated with three different authorization policies. To differentiate these authorization policies, you can use the Session:PostureStatus attribute along with other conditions.

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 by the NAC Agent.

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 it fails to meet all the mandatory requirements 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.

Related Topics

- [Configuring Standard Authorization Policies, page 23-21](#)

Configuring Standard Authorization Policies

You can define two types of authorization policies in the Authorization Policy page, standard exceptions authorization policies. The standard authorization policies that are specific to posture are used to make policy decisions based on the compliance status of endpoints.

-
- Step 1** Choose **Policy > Authorization**.
- Step 2** Choose one of the matching rule type to apply from the drop-down list shown at the top of the Authorization Policy page.
- **First Matched Rule Applies** — This option sets access privileges with a single authorization policy that is first matched during evaluation from the list of standard authorization policies. Once the first matching authorization policy is found, the rest of the standard authorization policies are not evaluated.
 - **Multiple Matched Rule Applies** — This option sets access privileges with multiple authorization policies that are matched during evaluation from the list of all the standard authorization policies.
- Step 3** Click the down arrow next to **Edit** in the default standard authorization policy row.
- Step 4** Click **Insert New Rule Above**.
- Step 5** Enter a rule name, choose identity groups and other conditions, and associate an authorization profile in the new authorization policy row that appears above the default standard authorization policy row.
- Step 6** Click **Done** to create a new standard authorization policy in read-only mode.
- Step 7** Click **Save**.
-

Related Topics

- [Custom Permissions for Posture, page 23-20](#)
- [Authorization Policy Settings, page B-5](#)
- [Chapter 20, “Managing Authorization Policies and Profiles.”](#)



Configuring Cisco Security Group Access Policies

This chapter describes how to configure a Cisco Identity Services Engine (Cisco ISE) node as an authentication server, using Security Group Access (SGA) policies. This requires a Cisco SGA solution-enabled network.

This chapter contains the following topics:

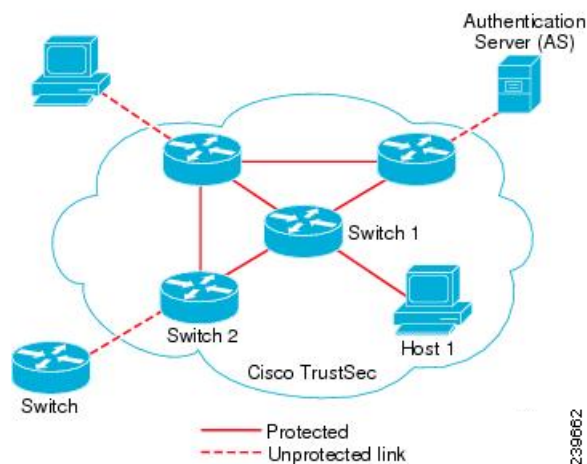
- [Security Group Access Architecture, page 24-1](#)
- [Enable SGA Solution, page 24-5](#)
- [Assigning Security Groups to Users and Endpoints, page 24-13](#)
- [Egress Policy, page 24-13](#)
- [OOB SGA PAC, page 24-18](#)
- [SGA CoA, page 24-21](#)

Security Group Access 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 Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

You need an Advanced License Package for Cisco ISE to enable SGA services.

Figure 24-1 SGA Architecture



- <http://www.cisco.com/en/US/netsol/ns1051/index.html>
- SGA Features, page 24-2
- SGA Terminology, page 24-3
- Supported Switches for SGA, page 24-4
- Components Required for SGA, page 24-5

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 Cisco ISE to reserve a range of SGTs to enable IP to SGT mapping.
- **IP-to-SGT Mapping**—An enhancement in Cisco ISE to bind an endpoint IP to an SGT and provision it to an SGA-capable device. Cisco ISE, Release 1.2 supports entering 1000 IP-to-SGT Mappings.
- **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.

SGA Terminology

Table 24-1 lists some of the common terms that are used in the SGA solution and their meaning in an SGA environment.

Table 24-1 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.

Table 24-1 SGA Terminology (continued)

Term	Meaning
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.
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 Cisco 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.

Supported Switches for SGA

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 24-2](#) lists the supported Cisco switch platforms.

Table 24-2 Supported Switches

Supported Cisco Switch Platforms		
Platform	Operating System Version	Requirement
Cisco Nexus 7000 Series	Cisco Nexus operating system, Release 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, Release 12.2(33) SXI3 or later	Optional as an access switch
Cisco Catalyst 4900 Series Switch	Cisco IOS Software, Release 2.2(50) SG7 or later	Optional as an access switch
Cisco Catalyst 4500E Switch with Supervisor 6L-E or 6-E	Cisco IOS Software, Release 12.2(50) SG7 or later	Optional as an access switch
Cisco Catalyst 3750-X or 3560-X Series Switches	Cisco IOS Software, Release 12.2(53) SE1 or later	Optional as an access switch

Table 24-2 **Supported Switches**

Supported Cisco Switch Platforms		
Cisco Catalyst 3750 or 3560 Series Switches	Cisco IOS Software, Release 12.2(53) SE1 or later	Optional as an access switch
Cisco Catalyst Blade Switch 3000 or 3100 Series	Cisco IOS Software, Release 12.2(53) SE1 or later	Optional as an access switch

Components Required for SGA

Apart from the switches listed in [Table 24-2](#), 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 24-3](#) lists other components that may be required for your Cisco SGA environment.

Table 24-3 **Components**

Component	Description
User Identity Repository	Although you can use the Cisco ISE internal user database, we recommend that you use an external database for identity authentication. Cisco 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.

Related Topics

[“Enable Cisco Security Group Access Switch Ports” section on page F-6](#)

Enable SGA Solution

This section describes the tasks that you must perform to enable the SGA solution in your Cisco ISE network.

This section contains the following:

- [Configure SGA Settings on the Switches, page 24-6](#)
- [Configuring SGA Devices, page 24-6](#)
- [Configuring Security Group Access Settings, page 24-7](#)
- [Configuring Security Group Access AAA Servers, page 24-8](#)
- [Configure Security Groups, page 24-8](#)
- [Configure Security Group Access Control Lists, page 24-10](#)
- [Map Security Groups to Devices, page 24-11](#)
- [Configuring SGA Policy by Assigning SGTs to Devices, page 24-12](#)

Configure 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 F-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 the following URLs:

- 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.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > Network Resources > Network Devices > Network Devices .
Step 2	Add a network device to the deployment.
Step 3	Click Submit to save the SGA device definition.
-

What To Do Next

- [Configuring Security Group Access Settings, page 24-7](#)

Related Topics

- [Network Device Definition Settings, page A-36](#)
- [SGA Device Attribute Settings, page A-39](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Configuring Security Group Access Settings

For Cisco ISE to function as an SGA server and provide SGA services, you must define some global SGA settings.

Before You Begin

- 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 Cisco 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 Cisco ISE PAC information can be uniquely identified on network devices upon NDAC authentication.

- To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Administration > System > Settings > Security Group Access .
Step 2	Enter the values in the fields.
Step 3	Click Save .
-

What To Do Next

- [Configuring Security Group Access AAA Servers, page 24-8](#)

Related Topics

- [Map Security Groups to Devices, page 24-11](#)
- [Security Group Access Settings, page A-24](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

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 Cisco ISE servers to this list, all these server details are downloaded to the SGA device. When an SGA device tries to authenticate, it chooses any Cisco 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 Cisco ISE server is an SGA AAA server. We recommend that you configure additional Cisco ISE servers in this AAA server list so that if one server is busy, another server from this list can handle the SGA request.

This page lists the Cisco 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.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Administration > Network Resources > SGA AAA Servers**.
- Step 2** Click **Add**.
- Step 3** Enter the values as described:
- **Name**—Name that you want to assign to the Cisco ISE server in this AAA Server list. This name can be different from the hostname of the Cisco ISE server.
 - **Description**—An optional description.
 - **IP**—IP address of the Cisco ISE server that you are adding to the AAA Server list.
 - **Port**—Port over which communication between the SGA device and server should take place. The default is 1812.
- Step 4** Click **Submit**.
-

What To Do Next

[Configure Security Groups, page 24-8](#)

Related Topics

[Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Configure 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. Cisco 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.

You can configure security groups from the following pages in the Admin portal:

- **Policy > Policy Elements > Results > Security Group Access > Security Groups.** See [“Adding Security Groups”](#) section on page 24-9.
- Directly from egress policy page. See [“Configuring SGT from Egress Policy”](#) section on page 24-16.
- Clicking the **Generate SGTs** button on the **Policy > Policy Elements > Results > Security Group Access > Security Groups** page. See [“Adding Security Groups”](#) section on page 24-9.

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 Security Groups, page 24-9](#)
- [Configuring SGA Policy by Assigning SGTs to Devices, page 24-12](#)

Adding Security Groups

Each security group in your SGA solution should be assigned a unique SGT. Even though Cisco 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.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Policy > Policy Elements > Results > Security Group Access > Security Groups .
Step 2	Click Add to add a new security group.
Step 3	Enter the values in the fields.
Step 4	Click Save to save the security group.
-

What To Do Next

- [Configure Security Group Access Control Lists, page 24-10](#)
- [Assigning Security Groups to Users and Endpoints, page 24-13](#)

Related Topics

[Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Configure 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 Admin portal.

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.

Related Topics

- [Adding Security Group Access Control Lists, page 24-10](#)
- [Configuring SGT from Egress Policy, page 24-16](#)

Adding Security Group Access Control Lists

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Policy > Policy Elements > Results > Security Group Access > Security Group ACLs**.
- Step 2** Enter 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
 - Security Group ACL Content—Access control list (ACL) commands. For example:


```
permit icmp
deny all
```
- Step 3** Click **Submit**.
-

Access Control List Entries for Nexus 7000 Series

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}]
```

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.

What To Do Next

[Configuring SGA Policy by Assigning SGTs to Devices, page 24-12](#)

Related Topics

- http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/security/command/reference/sec_cmds_d.html#wp1057446
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [Update RBACL Named List CoA, page 24-24](#)

Map 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, Cisco 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. You can map the security groups to devices from the Admin portal.

Related Topics

- [Adding Security Group Mappings, page 24-11](#)
- [Configuring Security Group Access Settings, page 24-7](#)

Adding Security Group Mappings

You can add security group mappings from the Admin portal.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
Step 1	Choose Policy > Policy Elements > Results > Security Group Mappings .
Step 2	Click Add to add a new security group mapping.
Step 3	Enter the values in the fields.
Step 4	Check the check box next to an existing security group mapping that you want to reassign, and then click Reassign Groups .
Step 5	Check the check box next to an existing security group mapping that you want to deploy, and then click Deploy .

- Step 6** Check the check box next to an existing security group mapping whose status you want to check, then choose >> and click **Check Status**.
- Step 7** Click **Submit**.
-

Related Topics

[Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Configuring SGA Policy by Assigning SGTs to Devices

You can configure the SGA policy by assigning SGTs to devices. You can assign security groups to devices by using the SGA device ID.

Before You Begin

- Ensure that you create the security groups for use in the policy. See [“Configure Security Groups” section on page 24-8](#) for more information.
 - To perform the following task, you must be a Super Admin or System Admin.
-

- Step 1** Choose **Policy > Security Group Access > Network Device Authorization**.
- Step 2** Click the Action icon in the Default Rule row, and click **Insert New Row Above**.
- Step 3** Enter the name for this rule.
- Step 4** Click the plus sign (+) next to **Conditions** to add a policy condition.
- Step 5** You can click **Create New Condition (Advance Option)** and create a new condition.
- Step 6** From the **Security Group** drop-down list, select the SGT that you want to assign if this condition evaluates to true.
- Step 7** 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 8** 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.

Related Topics

[Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Assigning Security Groups to Users and Endpoints

Cisco 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.

Before You Begin

- Read the [“Cisco ISE Authorization Policies” section on page 20-1](#) for information on authorization policies.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Policy > Authorization > Standard**.

Step 2 Create a new authorization policy.

Step 3 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.

Related Topics

- [Configuring Authorization Policies, page 20-8](#)
- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

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. Cisco 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.

This section contains the following:

- [View the Egress Policy, page 24-14](#)
- [Matrix Operations, page 24-15](#)
- [Configure Egress Policy Table Cells, page 24-15](#)
- [Configuring SGT from Egress Policy, page 24-16](#)
- [The Unknown Security Group, page 24-18](#)

Related Topics

- [Configure Security Groups, page 24-8](#)
- [Configure Security Group Access Control Lists, page 24-10](#)

View the Egress Policy

You can view the Egress Policy in the **Policy > Security Group Access > Egress Policy** page.

You can view the Egress policy in three different ways:

- [Source Tree, page 24-14](#)
- [Destination Tree, page 24-14](#)
- [Matrix View, page 24-14](#)

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.

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.

Related Topics

[Matrix Operations, page 24-15](#)

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.

Configure Egress Policy Table Cells

Cisco ISE allows you to configure cells using various options that are available in the tool bar. Cisco ISE does not allow a cell configuration if the selected source and destination SGTs are identical to a mapped cell.

This section contains:

- [Adding the Mapping of Egress Policy Cells, page 24-15](#)
- [Configuring SGT from Egress Policy, page 24-16](#)

Adding the Mapping of Egress Policy Cells

You can add the mapping cell for Egress Policy from the Policy page.

-
Step 1	Choose Policy > Security Group Access > Egress Policy
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 **Add** to add a new mapping cell

Step 5 Select appropriate values for:

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule

Step 6 Click **Submit** to save the configuration.

Configuring SGT from Egress Policy

You can create Security Groups directly from the Egress Policy page.

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

Step 2 Choose **Create Security Group** from the Configure option drop-down list.

Step 3 Create a Security Group.

Related Topics

[Configure Security Groups, page 24-8](#)

Configuring SGACL from Egress Policy

You can create Security Group ACLs directly from the Egress Policy page.

Step 1 Choose **Policy > Security Group Access > Egress Policy**.

Step 2 Choose **Create Security Group ACLs** from the Configure option drop-down list.

Step 3 Create a Security Group ACLs.

Related Topics

[Configure Security Group Access Control Lists, page 24-10](#)

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.

Related Topics

[Update SGT Matrix CoA, page 24-25](#)

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.

Features of 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

Related Topics

- [Running Top N RBACL Drops by User](#)
- [Chapter 26, “Reporting.”](#)

Running Top N RBACL Drops by User

You can run Top N RBACL Drops by User report as follows:

-
Step 1	From the Cisco ISE Admin dashboard, select Operations > Reports > ISE Reports > Security Group Access .
Step 2	Click Top N RBACL Drops by User .
Step 3	From the Filters drop-down menu, add the required monitor modes. The following options are available: • Destination Name/Destination Address • SGA SGT • SGA DGT • Enforcement Mode

- Step 4** Enter the values for the selected parameters accordingly. You can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.
- Step 5** From the **Time Range** drop-down menu, choose a time period over which the report data will be collected.
- Step 6** Click **Run** to run the report for a specific period, along with the selected parameters.
-

The Unknown Security Group

The Unknown security group is a pre-configured security group that cannot be modified and represents the 0x000 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 Cisco 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, Cisco ISE cannot provision these devices with SGA PAC over EAP-FAST. Instead, the SGA PAC is generated on Cisco 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 24-19](#)
- [Monitoring SGA PAC, page 24-20](#)

SGA PAC Provisioning

This section describes the following:

- [Generating an SGA PAC from the Settings Screen, page 24-19](#)
- [Generating an SGA PAC from the Network Devices Screen, page 24-19](#)
- [Generating an SGA PAC from the Network Devices List Screen, page 24-20](#)

Generating an SGA PAC from the Settings Screen

You can generate an SGA PAC from the Settings screen.

-
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 .
Step 4	Generate SGA PAC.
-

Related Topics

[Generating the PAC for EAP-FAST, page 19-12](#)

Generating an SGA PAC from the Network Devices Screen

You can generate an SGA PAC from the Network Devices screen.

-
Step 1	Choose Administration > Network Resources > Network Devices .
Step 2	Click Add . You can also click Add new device from the action icon on the Network Devices navigation pane.
Step 3	If you are adding a new device, provide a device name.
Step 4	Check the Security Group Access (SGA) check box to configure an SGA device.
Step 5	Under the Out of Band (OOB) SGA PAC sub section, click Generate PAC .
Step 6	Provide the following details: • PAC Time to Live—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**—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 7 Click **Generate PAC**.

Generating an SGA PAC from the Network Devices List Screen

You can generate an SGA PAC from the Network Devices list screen.

- Step 1** Choose **Administration > Network Resources > Network Devices**.
- Step 2** Click **Network Devices**.
- Step 3** Check the check box next to a device for which you want to generate the SGA PAC and click **Generate PAC**.
- Step 4** Provide the details in the fields.
- Step 5** Click **Generate PAC**.
-

Related Topics

[Generating an SGA PAC from the Network Devices Screen, page 24-19](#)

Monitoring SGA PAC

You can view SGA PAC provisioning data in the form of a PAC Provisioning Report.

- Step 1** From the Cisco ISE Admin dashboard, select **Operations > Reports > ISE Reports > Security Group Access**.
- Step 2** Click **PAC Provisioning**.
- Step 3** From the **Time Range** drop-down menu, choose a time period over which the report data will be collected.
- Step 4** Click the **Run** button to run the report for a specific period.
-

Related Topics

[Chapter 26, “Reporting.”](#)

SGA CoA

Cisco ISE supports SGA Change of Authorization (CoA) which allows Cisco 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 24-21](#)
- [Environment CoA, page 24-22](#)
- [Per Policy CoA, page 24-24](#)
- [SGA CoA Summary, page 24-27](#)
- [Monitor SGA CoA, page 24-27](#)

CoA Supported Network Devices

Cisco 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

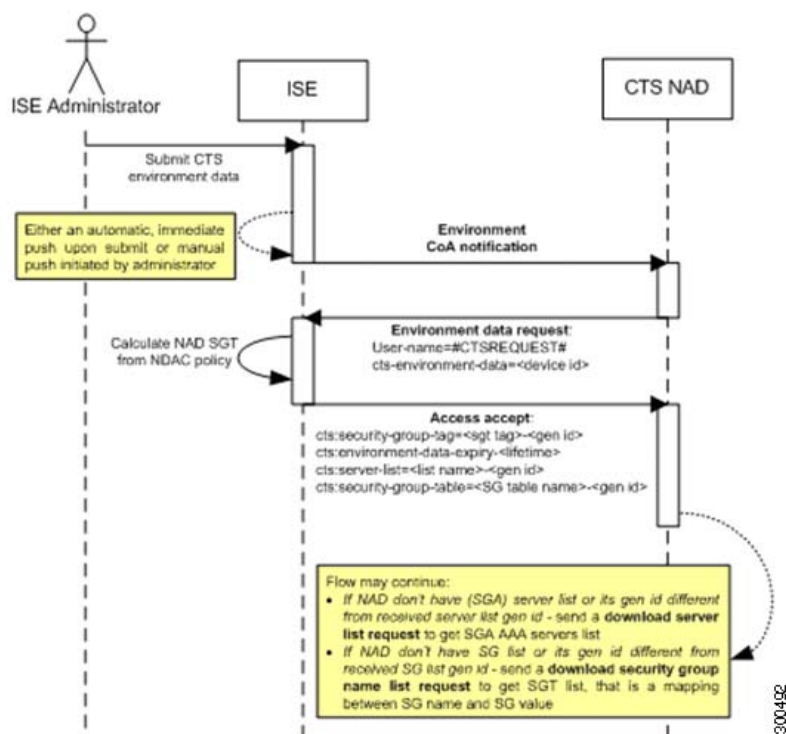
When Cisco ISE is deployed in a distributed environment where there are several secondaries that interoperate with different sets of devices, CoA requests are sent from Cisco ISE primary node to all the network devices. Therefore, SGA network devices need to be configured with the Cisco ISE primary node 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 24-2 depicts the Environment CoA notification flow.

Figure 24-2 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.

Initiate Environment CoA

An Environment CoA can be triggered for:

- [Triggering Environment CoA for Network Devices, page 24-23](#)
- [Triggering Environment CoA for Security Groups, page 24-23](#)
- [Triggering Environment CoA for SGA AAA Servers, page 24-23](#)
- [Triggering Environment CoA for NDAC Policy, page 24-24](#)

Triggering Environment CoA for 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.

Because 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.

Triggering Environment CoA for Security Groups

To trigger an Environment CoA for the security groups, complete the following steps.

Step 1 Choose **Policy > Policy Elements > Results > Security Group Access > Security Groups**.

Step 2 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 3 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.

Triggering Environment CoA for 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.

Triggering Environment CoA for 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 24-22](#).

Per Policy CoA

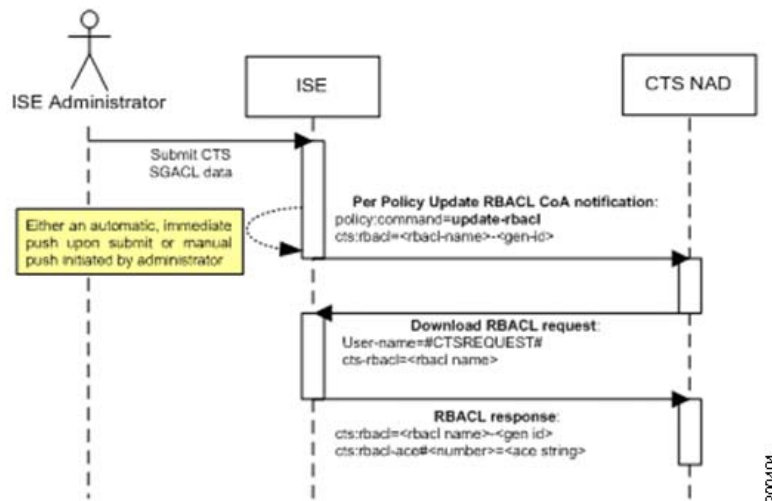
There are three types of Per Policy CoA notification:

- [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 24-3 depicts the Update RBACL Named List CoA flow.

Figure 24-3 Update RBACL Named List CoA Notification Flow



1. Cisco 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, Cisco 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 [Configure Security Group Access Control Lists, page 24-10](#).
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.
-

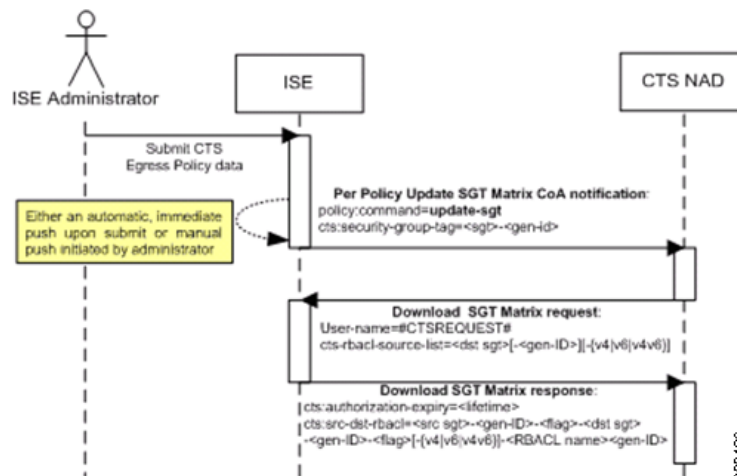
Changing the name or the IP version of an SGACL does not change its generation ID; hence it does not require sending an update RBACL named list CoA notification.

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 24-26](#) that deals with changes in the egress policy.

Update SGT Matrix CoA

Figure 24-4 depicts the Update SGT Matrix CoA flow.

Figure 24-4 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, Cisco 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.

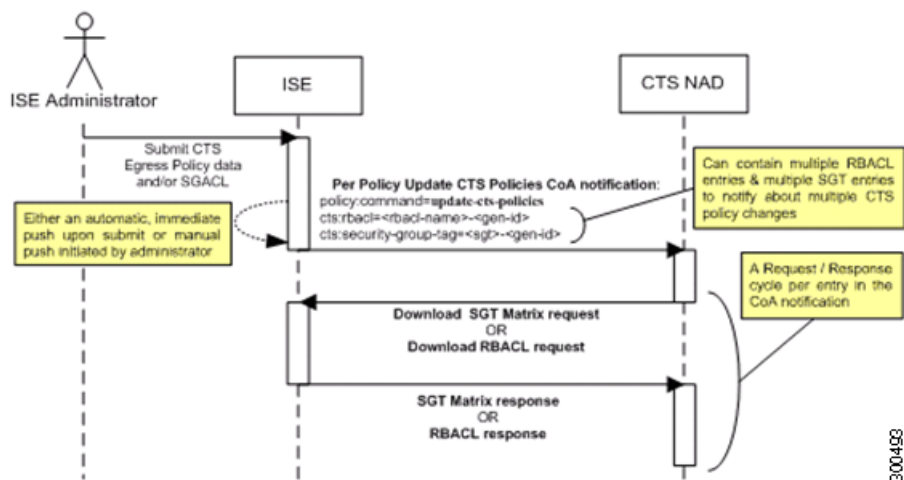
Initiating Update SGT matrix CoA from Egress Policy

-
- 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 24-5 depicts the Policies Update CoA flow.

Figure 24-5 Policies Update CoA flow



1. Cisco 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, Cisco ISE returns the relevant data.

SGA CoA Summary

Table 24-4 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 24-4 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

Monitor 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 24-28](#)
- [Running SGA CoA Report, page 24-28](#)

SGA CoA Alarms

When CoA returns CoA-NAK, an alarm is generated.

To view SGA CoA alarms, go to **Operations > Alarms > Rules**.

You can also view the SGA CoA alarms under Live Logs. To view live logs, go to **Operations > Alarms > Inbox**.

Running SGA CoA Report

You can run the SGA CoA Report as follows:

-
Step 1	From the Cisco ISE Admin dashboard, select Operations > Reports > ISE Reports > Security Group Access .
Step 2	From the Run drop-down menu, choose a time period over which the report data will be collected. 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.
-



PART 6

Monitoring and Troubleshooting Cisco ISE



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 describes monitoring and troubleshooting functions and tasks and contains the following sections:

- [Monitoring and Troubleshooting Service in Cisco ISE, page 25-1](#)
- [Device Configuration for Monitoring, page 25-3](#)
- [Cisco ISE Alarms, page 25-5](#)
- [Troubleshooting Network Access Issues, page 25-17](#)
- [Obtaining Additional Troubleshooting Information, page 25-25](#)
- [Monitoring Database, page 25-29](#)



Note

For a list of inherent known issues and workarounds associated with monitoring and troubleshooting, refer to the [Release Notes for the Cisco Identity Services Engine, Release 1.2](#).

Monitoring and Troubleshooting Service in Cisco ISE

The Monitoring and troubleshooting service is a comprehensive identity solution for all Cisco ISE run-time services and uses 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 affect operational conditions.
- **Troubleshooting**—Provides contextual guidance for resolving access issues on networks. You can then address user concerns and provide a 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 them for future use.

Cisco ISE Dashboard

The Cisco ISE dashboard, or home page, is the landing page that appears after you log in to 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.

Dashboard's real-time data provides an at-a-glance status of the devices and users that are accessing your network as well as the system health overview.

**Note**

You must have Adobe Flash Player installed on the Administration node to be able to view the dashlets and metric meters on the dashboard.

The dashboard shows the activity on the Network Privilege Framework (NPF), and provides detailed information on the various components.

The NPF is composed of the three tiers outlined in [Table 25-1](#).

Table 25-1 **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 26, "Reporting."](#)

The NPF authentication and authorization event flow uses the following process:

1. NAD performs an authorization or flex authorization.
2. An unknown agentless identity is profiled with web authorization.
3. RADIUS server authenticates and authorizes the identity.
4. Authorization is provisioned for the identity at the port.
5. Unauthorized endpoint traffic is dropped.

User Roles and Permissions for Monitoring and Troubleshooting Capabilities

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 [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#).

Data Stored in Monitoring 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 nodes or network devices, a Cisco ISE node dedicated to monitoring is recommended.

To manage the information stored in the Monitoring database, you are required to perform full and incremental backups of the database. This includes purging unwanted data, and then restoring the database.

Related Topic

[Monitoring Database, page 25-29](#)

Device Configuration for Monitoring

The Monitoring node receives and uses data from devices on the network to populate the dashboard display. To enable communication between the Monitoring node and the network devices, switches and Network Access Devices (NADs) must be configured properly.

For information on how to configure these devices, see [Configure NADs for ISE Monitoring, page G-39](#)

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.

-
Step 1	Go to the Cisco ISE Dashboard .
Step 2	Expand the System Summary dashlet. A detailed real-time report appears.
Step 3	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
-

The color of the system status icon indicates the health of your system:

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

Related Topics

- [Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8, page G-14](#)

Monitoring Network Authentications

You can view the passed and failed network authentications from the Authentications dashlet. It provides 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.

-
- Step 1** Go to the Cisco ISE **Dashboard**.
 - Step 2** Expand the **Authentications** dashlet. A detailed real-time report appears.
 - Step 3** Review the information for the users or devices that are authenticated on the network:
 - Step 4** Expand the data categories for more information.
-

Determining Profiler Activity and 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 the peak endpoint activity over the last 24 hours or 60 minutes.

-
- Step 1** Go to the Cisco ISE **Dashboard**.
 - Step 2** In the **Profiler Activity** dashlet, hover your cursor over a stack bar or sparkline.
A tooltip provides detailed information.
 - Step 3** Expand the data categories for more information.
 - Step 4** Expand the **Profiler Activity** dashlet. A detailed real-time report appears.
-

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.

Checking Posture Compliance

The Posture Compliance dashlet provides 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.

-
- Step 1** Go to the Cisco ISE **Dashboard**.
 - Step 2** In the **Posture Compliance** dashlet, hover your cursor over a stack bar or sparkline.
A tooltip provides detailed information.

- Step 3** Expand the data categories for more information.
- Step 4** Expand the **Posture Compliance** dashlet. A detailed real-time report appears.

Cisco ISE Alarms

Alarms notify you of critical conditions on a network and are displayed in the Alarms dashlet. They also provide information on system activities, such as data purge events. You can configure how you want to be notified about system activities, or disable them entirely. You can also configure the threshold for certain alarms.

Alarms do not have an associated schedule and are sent immediately after an event occurs. At any given point in time, only the latest 15,000 alarms are retained.

If the event re-occurs, then the same alarms are suppressed for a minimum duration of two hours. During the time that the event re-occurs, depending up on the trigger, it may take up to three hours for the alarms to re-appear.

Table 25-2 lists all the Cisco ISE alarms, descriptions and their resolution.

Table 25-2 Cisco ISE Alarms

Alarm Name	Alarm Description	Alarm Resolution
Administrative and Operational Audit Management		
Administrator account Locked/Disabled	Administrator account is locked or disabled due to password expiration or incorrect login attempts. For more details, refer to the administrator password policy.	Administrator password can be reset by another administrator using the GUI or CLI.
Backup Failed	The ISE backup operation failed.	Check the network connectivity between Cisco ISE and the repository. Ensure that: • The credentials used for the repository is correct. • There is sufficient disk space in the repository. • The repository user has write privileges.
CA Server is down	CA server is down.	Check to make sure that the CA services are up and running on the CA server.
CA Server is Up	CA server is up.	A notification to inform the administrator that the CA server is up.

Table 25-2 Cisco ISE Alarms (continued)

Alarm Name	Alarm Description	Alarm Resolution
Certificate Expiration	This certificate will expire soon. When it expires, Cisco ISE may fail to establish secure communication with clients.	Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE to extend the expiration date. You can delete the certificate if it is no longer used.
Certificate Expired	This certificate has expired. Cisco ISE may fail to establish secure communication with clients. Node-to-node communication may also be affected.	Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE to extend the expiration date. You can delete the certificate if it is no longer used.
Certificate Request Forwarding Failed	Certificate request forwarding failed.	Make sure that the certification request coming in matches with attributes from the sender.
Configuration Changed	Cisco ISE configuration is updated. This alarm is not triggered for any configuration change in users and endpoints.	Check if the configuration change is expected.
CRL Retrieval Failed	Unable to retrieve CRL from the server. This could occur if the specified CRL is unavailable.	Ensure that the download URL is correct and is available for the service.
DNS Resolution Failure	DNS resolution failed on the node.	Check if the DNS server configured by the command ip name-server is reachable. If you get the alarm as 'DNS Resolution failed for CNAME <hostname of the node>', then ensure that you create CNAME RR along with the A record for each Cisco ISE node.
External MDM Server API Version Mismatch	External MDM server API version does not match with what is configured in Cisco ISE.	Ensure that the MDM server API version is the same as what is configured in Cisco ISE. Update Cisco ISE MDM server configuration if needed.
External MDM Server Connection Failure	Connection to the external MDM server failed.	Ensure that the MDM server is up and Cisco ISE-MDM API service is running on the MDM server.

Table 25-2 Cisco ISE Alarms (continued)

Alarm Name	Alarm Description	Alarm Resolution
External MDM Server Response Error	External MDM Server response error.	Ensure that the Cisco ISE-MDM API service is properly running on the MDM server.
Firmware Update Required	A firmware update is required on this host.	Contact Cisco Technical Assistance Center to obtain firmware update
Insufficient Virtual Machine Resources	Virtual Machine (VM) resources such as CPU, RAM, Disk Space, or IOPS are insufficient on this host.	Ensure that a minimum requirements for the VM host, as specified in the Cisco ISE Hardware Installation Guide.
No Configuration Backup Scheduled	No Cisco ISE configuration backup is scheduled.	Create a schedule for configuration backup.
NTP Service Failure	The NTP service is down on this node.	This could be because there is a large time difference between NTP server and Cisco ISE node(more than 1000s). Ensure that your NTP server is working properly and use the ntp server <servername> CLI command to restart the NTP service and fix the time gap.
NTP Sync Failure	All the NTP servers configured on this node are unreachable.	Execute show ntp command from the CLI for troubleshooting. Ensure that the NTP servers are reachable from Cisco ISE. If NTP authentication is configured, ensure that the key ID and value matches with that of the server.
Operations DB Purge Failed	Unable to purge older data from the operations database. This could occur if M&T nodes are busy.	Check the Data Purging Audit report and ensure that the used_space is lesser than the threshold_space. Login to M&T nodes using CLI and perform the purge operation manually.
Patch Failure	A patch process has failed on the server.	Re-install the patch process on the server.
Patch Success	A patch process has succeeded on the server,	—
Profiler SNMP Request Failure	Either the SNMP request timed out or the SNMP community or user authentication data is incorrect.	Ensure that SNMP is running on the NAD and verify that SNMP configuration on Cisco ISE matches with NAD.
Replication Failed	The secondary node failed to consume the replicated message.	Login to the Cisco ISE GUI and perform a manual syncup from the deployment page. De-register and register back the affected Cisco ISE node.

Table 25-2 Cisco ISE Alarms (continued)

Alarm Name	Alarm Description	Alarm Resolution
Restore Failed	Cisco ISE restore operation failed.	Ensure the network connectivity between Cisco ISE and the repository. Ensure that the credentials used for the repository is correct. Ensure that the backup file is not corrupted. Execute the reset-config command from the CLI and restore the last known good backup.
ISE Services		
Authentication Inactivity	Cisco ISE policy service nodes are not receiving authentication requests from the network devices.	Check the ISE/NAD configuration. Check the network connectivity of the ISE/NAD infrastructure.
COA Failed	Network device has denied the Change of Authorization (CoA) request issued by Cisco ISE policy service nodes.	Ensure that the network device is configured to accept Change of Authorization (CoA) from Cisco ISE. Ensure if CoA is issued on a valid session.
Excessive Authentication Attempts ¹	Cisco ISE policy service nodes are experiencing higher than expected rate of authentications.	Check the re-auth timer in the network devices. Check the network connectivity of the Cisco ISE infrastructure.
Excessive Failed Attempts ¹	Cisco ISE policy service nodes are experiencing higher than expected rate of failed authentications.	Check the authentication steps to identify the root cause. Check the Cisco ISE/NAD configuration for identity and secret mismatch.
Identity Store Unavailable	Cisco ISE policy service nodes are unable to reach the configured identity stores.	Check the network connectivity between Cisco ISE and identity store.
Misconfigured Network Device Detected	Cisco ISE has detected too many RADIUS accounting information from NAS	Too many duplicate RADIUS accounting information has been sent to ISE from NAS. Configure NAS with accurate accounting frequency.
Misconfigured Supplicant Detected	Cisco ISE has detected mis-configured supplicant on the network	Ensure that the configuration on Supplicant is correct.
No Accounting Start	Cisco ISE policy service nodes have authorized a session but did not receive accounting start from the network device.	Ensure that RADIUS accounting is configured on the network device. Check the network device configuration for local authorization.

Table 25-2 Cisco ISE Alarms (continued)

Alarm Name	Alarm Description	Alarm Resolution
RADIUS Request Dropped	The authentication/accounting request from a NAD is silently discarded. This may occur due to unknown NAD, mismatched shared secrets, or invalid packet content per RFC.	Check that the NAD/AAA client has a valid configuration in Cisco ISE. Check whether the shared secrets on the NAD/AAA client and Cisco ISE matches. Ensure that the AAA client and the network device, have no hardware problems or problems with RADIUS compatibility. Also ensure that the network that connects the device to Cisco ISE has no hardware problems.
SGACL Drops	Secure Group Access (SGACL) drops occurred. This occurs if an SGA capable device drops packets due to SGACL policy violations.	Run the RBACL drop summary report and review the source causing the SGACL drops. Issue a CoA to the offending source to reauthorize or disconnect the session.
Supplicant stopped responding	Cisco ISE sent last message to the client 120 seconds ago but there is no response from the client.	Verify that the supplicant is configured properly to conduct a full EAP conversation with Cisco ISE. Verify that NAS is configured properly to transfer EAP messages to/from the supplicant. Verify that the supplicant or NAS does not have a short timeout for EAP conversation.
Unknown NAD	Cisco ISE policy service nodes are receiving authentication requests from a network device that is not configured in Cisco ISE.	Check if the network device is a genuine request and add it to the configuration. Ensure that the secret matches.
System Health		
Health Status Unavailable	The monitoring node has not received health status from the Cisco ISE node.	Ensure that Cisco ISE nodes are up and running. Ensure that Cisco ISE nodes are able to communicate with the monitoring nodes.
High Authentication Latency	Cisco ISE system is experiencing high authentication latency.	Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.
High Disk I/O Utilization	Cisco ISE system is experiencing high disk I/O utilization.	Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.

Table 25-2 Cisco ISE Alarms (continued)

Alarm Name	Alarm Description	Alarm Resolution
High Disk Space Utilization	Cisco ISE system is experiencing high disk utilization.	Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.
High Load Average	Cisco ISE system is experiencing high load average.	Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.
High Memory Utilization	Cisco ISE system is experiencing high memory utilization.	Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.
High Operations DB Usage	Cisco ISE monitoring nodes are experiencing higher volume of syslog data than expected.	Check and reduce the purge configuration window for the operations data.
Process Down	One of the Cisco ISE processes is not running.	Restart the Cisco ISE application.
Profiler Queue Size Limit Reached	The ISE Profiler queue size limit has been reached. Events received after reaching the queue size limit will be dropped.	Check if the system has sufficient resources, and ensure EndPoint attribute filter is enabled.
Licensing		
License Expiration	License installed on the Cisco ISE nodes has expired.	Contact Cisco Accounts team to purchase new licenses.
License Violation	Cisco ISE nodes have detected that you are exceeding or about to exceed the allowed license count.	Contact Cisco Accounts team to purchase additional licenses.
System Error		
Log Collection Error	Cisco ISE monitoring collector process is unable to persist the audit logs generated from the policy service nodes.	This will not impact the actual functionality of the Policy Service nodes. Contact TAC for further resolution.
Scheduled Report Export Failure	Unable to copy the exported report (CSV file) to configured repository.	Verify the configured repository. If it has been deleted, add it back. If it is not available or not reachable, reconfigure the repository to a valid one.

- Once the threshold is met, the **Excessive Authentication Attempts** and **Excessive Failed Attempts** alarms are triggered. The numbers displayed next to the Description column are the total number of authentications that are authenticated or failed against Cisco ISE in last 15 minutes.

Alarms are not triggered when you add users or endpoints to Cisco ISE.

After you upgrade from a previous Cisco ISE release to Cisco ISE, release 1.2, rules that you created in the previous release and alarms in alarms inbox will be deleted.

Related Topics

- [Enabling and Configuring Alarms, page 25-11](#)
- [Configuring Remote Syslog Collection Locations, page 11-4](#)
- [Configuring the SMTP Server to Support Notifications, page 5-5](#)

Enabling and Configuring Alarms

You can enable or disable Cisco ISE alarms and configure alarm notification behavior to notify you of critical conditions. For certain alarms you can configure thresholds like maximum failed attempts for Excessive Failed Attempts alarm or maximum disk utilization for High Disk Utilization alarm.

-
Step 1	Choose Administration > System > Settings > Alarm Settings .
Step 2	Select an alarm from the list of default alarms and click Edit .
Step 3	Select Enable or Disable .
Step 4	Configure alarm threshold if applicable.
Step 5	Click Submit .
-

Related Topics

- [Cisco ISE Alarms, page 25-5](#)
- [Configuring the SMTP Server to Support Notifications, page 5-5](#)

Monitoring Alarms

Cisco ISE provides system alarms which notify you whenever any critical system condition occurs. Alarms that are generated by Cisco ISE are displayed in the Alarm dashlet. These notifications automatically appear in the alarm dashlet.

The Alarm dashlet displays a list of recent alarms, which you can select from to view the alarm details. You can also receive notification of alarms through e-mail and syslog messages.

-
Step 1	Go to the Cisco ISE Dashboard .
Step 2	Click on an alarm in the Alarms dashlet. A new window opens with the alarm details and a suggested action.
Step 3	Click Refresh to refresh the alarms.
Step 4	Click Acknowledge to acknowledge selected alarms. You can select the alarms by clicking the check box available prior to the timestamp. This reduces the alarm counters (number of times an alarm is raised) when marked as read.
Step 5	Click the Details link corresponding to the alarm that you select. A new window opens with the details corresponding to the alarm that you select.

**Note**

The Details link corresponding to the previous alarms that were generated prior to persona change shows no data.

Related Topics

[Cisco ISE Alarms, page 25-5](#)

Log Collection

Monitoring services collect log and configuration data, store the data, and then process 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.

Related Topic

[Chapter 11, “Logging.”](#)

Alarm Syslog Collection Location

If you configure monitoring functions to send 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.

**Note**

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 G-39](#).

Related Topics

- [Configuring Remote Syslog Collection Locations, page 11-4](#)
- [Configuring the SMTP Server to Support Notifications, page 5-5](#)

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 shows the live authentication entries corresponding to the authentication events as they happen. In addition to authentication entries, this page also shows the live session entries corresponding to the events. You can also drill-down the desired session to view a detailed report corresponding to that session.

When a single endpoint authenticates successfully, two entries appear in the Live Authentications page: one corresponding to the authentication record and another corresponding to the session record (pulled from session live view). Subsequently, when the device performs another successful authentication, the repeat counter corresponding to the session record is incremented. The Repeat Counter that appears in the Live Authentications page shows the number of duplicate radius authentication success messages that are suppressed.

The Live Authentication data categories that are shown by default are described in [“Recent RADIUS Authentications” section on page C-1](#).

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.

Monitoring Live Authentications

The Live Authentications page provides a tabular account of recent RADIUS authentications, in the order in which they happen.

The last update shown at the bottom of the Live Authentications page shows the date of the server, time, and timezone.

-
Step 1	Choose Operations > Authentications .
Step 2	Select a time interval from the drop-down list to change the data refresh rate.
Step 3	Click the Refresh icon on the Live Authentications menu bar to manually update the data.
Step 4	Choose an option from the Show drop-down list to change the number of records that appear.
Step 5	Choose an option from the within drop-down list to specify a time interval,
Step 6	Click Add or Remove Columns and choose the options from the drop-down list to change the columns that are shown.
Step 7	Click Show Live Sessions to view live RADIUS sessions. You can use the dynamic Change of Authorization (CoA) feature for the Live Sessions that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a Network Access Device (NAD).
Step 8	Click Save at the bottom of the drop-down list to save your modifications.
-

Related Topics

- [Recent RADIUS Authentications, page C-1](#)
- [RADIUS Accounting Packets \(Attributes\) Not Coming from Switch, page G-6](#)

- [RADIUS Server Error Message Entries Appearing in Cisco ISE, page G-18](#)
- [RADIUS Server Connectivity Issues \(No Error Message Entries Appearing in Cisco ISE\), page G-19](#)
- [Cisco ISE Active RADIUS Sessions, page 26-4](#)
- [Changing Authorization for RADIUS Sessions, page 26-5](#)

Global Search for Endpoints

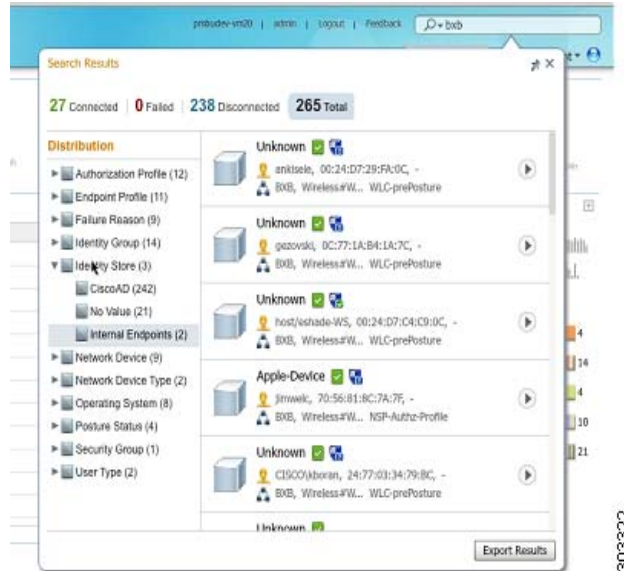
You can use the global search box available at the top of the Cisco ISE home page to search for endpoints. You can use any of the following criteria to search for an endpoint:

- User name
- MAC Address
- IP Address
- Authorization Profile
- Endpoint Profile
- Failure Reason
- Identity Group
- Identity Store
- Network Device name
- Network Device Type
- Operating System
- Posture Status
- Location
- Security Group
- User Type

You should enter at least three characters for any of the search criteria in the Search field to display data.

The search result provides a detailed and at-a-glance information about the current status of the endpoint, which you can use for troubleshooting. Search results display only the top 25 entries. It is recommended to use filters to narrow down the results.

[Figure 25-1](#) shows an example of the search result.

Figure 25-1 Search Result For Endpoints

You can use any of the properties in the left panel to filter the results. You can also click on any endpoint to see more detailed information about the endpoint, such as:

- Session trace
- Authentication details
- Accounting details
- Posture details
- Profiler details
- Client Provisioning details
- Guest accounting and activity

Related Topic

[Session Trace for an Endpoint, page 25-15](#)

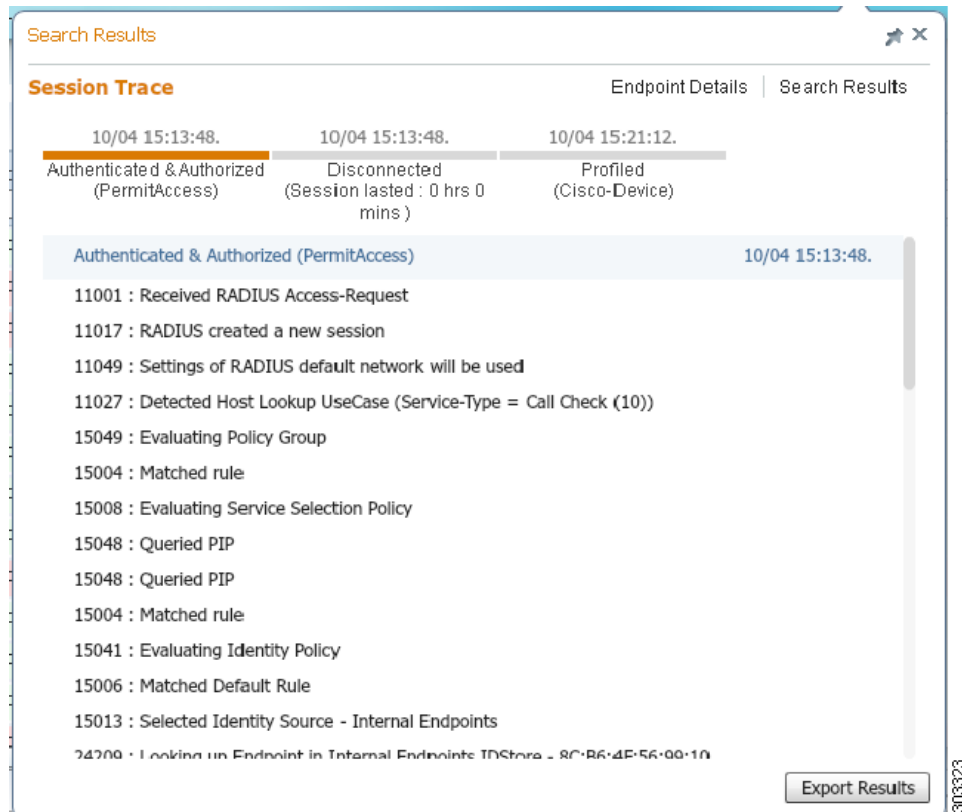
Session Trace for an Endpoint

You can use the global search box available at the top of the Cisco ISE home page to get session information for a particular endpoint. When you search with a criteria, you get a list of endpoints. Click on any of these endpoints to see the session trace information for that endpoint. [Figure 25-2](#) shows an example of the session trace information displayed for an endpoint.



Note

The dataset used for search is based on Endpoint ID as indexes. Therefore, when authentication occurs, it is mandatory to have Endpoint IDs for the endpoints for those authentications to include them in the search result set.

Figure 25-2 Session Trace of an Endpoint

You can use the clickable timeline at the top to see major authorization transitions. You can also export the results in .csv format by clicking the Export Results button. The report gets downloaded to your browser.

You can click on the Endpoint Details link to see more authentication, accounting, and profiler information for a particular endpoint. [Figure 25-3](#) shows an example of endpoint details information displayed for an endpoint.

Figure 25-3 **Endpoint Details**

Name	Value
Source Timestamp	2012-11-07 10:54:40.688
Received Timestamp	2012-11-07 10:54:40.689
Policy Server	ise230
Event	80002 Profiler EndPoint profiling event occurred
Mac Address	00:0C:29:95:A5:C1
Endpoint Policy	WindowsXP-Workstation
Static Assignment	
Source	
Oui	VMware, Inc.
Hostname	
Property	port=9,StaticAssignment=false,VlanName=VLAN0030,if OperStatus=1,cafSessionAuthorizedBy=Authentication Server;ifIndex=10109,ifDescr=GigabitEthernet1/0/9,cafSessionAuthUserName=00-0C-29-95-A5-C1,cafSessionDomain=2,BYODRegistration=Unknown,EndPointPolicyID=a5f92810-be86-11e1-ba69-0050568e002b,FirstCollection=1352205183395,TimeToProfile=70,LastNmapScanTime=0,cafSessionStatus

Session Removal from the Directory

Sessions are cleaned from the session directory on the Monitoring and Troubleshooting node as follows:

- Terminated sessions are cleaned 15 minutes after termination.
- If there is authentication but no accounting, then such sessions are cleared after one hour.
- All inactive sessions are cleaned after seven days.

Related Topic

[Global Search for Endpoints, page 25-14](#)

Troubleshooting Network Access Issues

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 Summary report.

-
- Step 1** Choose **Operations > Reports > Authentication Summary Report**.
- Step 2** Filter the report for Failure Reasons.

- Step 3** Review the data in the Authentication by Failure Reasons section of the report to troubleshoot your network access problem.

**Note**

As the Authentication Summary report collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.

Related Topics

- [Troubleshooting Unexpected RADIUS Authentication Results, page 25-18](#)
- [Running and Viewing Reports, page 26-2](#)

Diagnostic Troubleshooting Tools

Diagnostic tools help you diagnose and troubleshoot problems on a Cisco ISE network and provide a detailed instructions on how to resolve problems. You can use these tools to troubleshoot authentications and evaluate the configuration of any network device on your network, including Security Group Access devices.

This section describes diagnostic procedures and contains the following topics:

- [Troubleshooting Unexpected RADIUS Authentication Results, page 25-18](#)
- [Executing IOS Show Commands to Check Configuration, page 25-19](#)
- [Troubleshooting Network Device Configuration Issues, page 25-20](#)
- [Troubleshooting Endpoint Posture Failure, page 25-20](#)
- [Using TCP Dump to Monitor Network Traffic, page 25-21](#)
- [Saving a TCP Dump File, page 25-22](#)
- [Comparing Unexpected SGACL for an Endpoint or User, page 25-22](#)
- [Troubleshooting Connectivity Issues in an SGA-Enabled Network with SXP-IP Mappings, page 25-23](#)
- [Troubleshooting Connectivity Issues in an SGA-Enabled Network with IP-SGT Mappings, page 25-24](#)
- [Troubleshooting Connectivity Issues in an SGA-Enabled Network by Comparing Device SGT Mappings, page 25-24](#)

Troubleshooting Unexpected RADIUS Authentication Results

This tool allows you to search and select a RADIUS authentication for troubleshooting when there is an unexpected authentication result. You might use this tool if you expected an authentication to pass, but it failed or if you expected a user to have a certain level of privileges, and the user did not have those privileges.

- Searching RADIUS authentications based on Username, Endpoint ID, Network Access Service (NAS) IP address, and reasons for authentication failure for troubleshooting, Cisco ISE displays authentications only for the system (current) date.

- Searching RADIUS authentications based on NAS Port for troubleshooting, Cisco ISE displays all NAS Port values since the beginning of the previous month to the current date.

**Note**

When searching RADIUS authentications based on NAS IP address and Endpoint ID fields, a search is first performed in the operational database, and then in the configuration database.

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting**.
- Step 2** Specify the search criteria in the fields as needed.
- Step 3** Click **Search** to display the RADIUS authentications that match your search criteria.
- Step 4** Select a RADIUS authentication record from the table, and click **Troubleshoot**.
- Step 5** Click **User Input Required**, modify the fields as needed, and then click **Submit**.
- Step 6** Click **Done**.
- Step 7** Click **Show Results Summary** after the troubleshooting is complete.
- Step 8** To view a diagnosis, the steps to resolve the problem, and a troubleshooting summary, click **Done**.
-

Related Topics

- [RADIUS Authentication Troubleshooting Settings, page C-4](#)
- [Progress Details Settings, page C-10](#)
- [Results Summary, page C-10](#)
- [RADIUS Accounting Packets \(Attributes\) Not Coming from Switch, page G-6](#)
- [RADIUS Server Error Message Entries Appearing in Cisco ISE, page G-18](#)
- [RADIUS Server Connectivity Issues \(No Error Message Entries Appearing in Cisco ISE\), page G-19](#)

Executing IOS Show Commands to Check Configuration

The Execute Network Device Command diagnostic tool allows you to run the **show** command on any network device. The results are exactly what you would see on a console, and can be used to identify problems in the configuration of the device. You can use it when you suspect that the configuration is wrong, you want to validate it, or if you are just curious about how it is configured.

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Execute Network Device Command**.
- Step 2** Enter the information in the appropriate fields.
- Step 3** Click **Run** to execute the command on the specified network device.
- Step 4** Click **User Input Required**, and modify the fields as necessary.
- Step 5** Click **Submit** to run the command on the network device, and view the output.
-

Related Topics

- [Execute Network Device Command Settings, page C-5](#)
- [Progress Details Settings, page C-10](#)
- [Results Summary, page C-10](#)

Troubleshooting Network Device Configuration Issues

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.

-
Step 1	Choose Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator .
Step 2	Enter the Network Device IP address of the device whose configuration you want to evaluate, and specify other fields as necessary.
Step 3	Select the configuration options to compare against the recommended template.
Step 4	Click Run .
Step 5	Click User Input Required , and modify the fields as necessary.
Step 6	Check the check boxes next to the interfaces that you want to analyze, and click Submit .
Step 7	Click Show Results Summary .
-

Related Topics

- [Evaluate Configuration Validator Settings, page C-5](#)
- [Progress Details Settings, page C-10](#)
- [Results Summary, page C-10](#)

Troubleshooting Endpoint Posture Failure

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, and posture status.

-
Step 1	Choose Operations > Troubleshoot > Diagnostic Tools > General Tools > Posture Troubleshooting .
Step 2	Enter the information in the appropriate fields.
Step 3	Click Search .

- Step 4** To find an explanation and determine a resolution for an event, select the event in the list and click **Troubleshoot**.
-

Related Topics

- [Posture Troubleshooting Settings, page C-6](#)
- [Progress Details Settings, page C-10](#)
- [Results Summary, page C-10](#)

TCP Dump Utility to Validate the Incoming Traffic

This is a tool to sniff the packet, when you want to examine that the expected packet really reached a node. For example, when there is no incoming authentication or log indicated in the report, you may suspect that there is no incoming traffic or that the incoming traffic cannot reach Cisco ISE. In such cases, you can run this tool to validate.

This section shows you how to use the TCP Dump feature, and covers the following topics:

- [Using TCP Dump to Monitor Network Traffic, page 25-21](#)
- [Saving a TCP Dump File, page 25-22](#)



Caution

Starting a TCP Dump automatically deletes a previous dump file. To save a previous dump file, perform the [Saving a TCP Dump File, page 25-22](#) before you begin a new TCP Dump session.

Using TCP Dump to Monitor Network Traffic

You can configure the TCP Dump options and then collect data from the network traffic to help you troubleshooting a network issue.

Before You Begin

- The Network Interface drop-down list in the TCP Dump page displays only the network interface cards (NICs) that have an IPv4 or IPv6 address configured. By default, all NICs are connected on a VMware, and therefore, NICs are configured with an IPv6 address and displayed in the Network Interface drop-down list.
- You must have Adobe Flash Player installed on the Cisco ISE administration node to be able to view the tcpdump file.

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**.
- Step 2** Choose a **Host Name** as the source for the TCP Dump utility. Inline Posture nodes are not supported.
- Step 3** Choose a **Network Interface** to monitor from the drop-down list.
- Step 4** Set Promiscuous Mode by clicking the radio button to On or Off. The default is On.

Promiscuous mode is the default packet sniffing mode in which the network interface passes all traffic to the system's CPU. We recommend that you leave it set to On.

- Step 5** In the Filter text box, 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.
- 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 which is 500,000.
-

Related Topics

- [TCP Dump Settings, page C-6](#)
- [Saving a TCP Dump File, page 25-22](#)
- [Policy Service Node Not Passing Traffic, page G-7](#)

Saving a TCP Dump File

You can save a TCP dump file to use for troubleshooting purposes.

Before You Begin

You should have successfully completed [Using TCP Dump to Monitor Network Traffic, page 25-21](#).

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**.
- Step 2** Choose a Format from the drop-down list. Human Readable is the default.
- Step 3** Click **Download**, navigate to the desired location, and then click **Save**.
- Step 4** To get rid of the previous dump file without saving it first, click **Delete**.
-

You can also access TCPdump through the Cisco ISE CLI. For more information, refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

Comparing Unexpected SGACL for an Endpoint or User

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. You can use this tool when there is an unexpected SGACL for an endpoint or a user.

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > Egress (SGACL) Policy**.
- Step 2** Enter the Network Device IP address of the Security Group Access device whose SGACL policy you want to compare.
- Step 3** Click **Run**.
- Step 4** Click **User Input Required** and modify the fields as necessary.

- Step 5** Click **Submit**.
- Step 6** Click **Show Results Summary** to view the diagnosis and suggested resolution steps.
-

Related Topics

- [Progress Details Settings, page C-10](#)
- [Results Summary, page C-10](#)

Egress Policy Diagnostic Flow

The egress policy diagnostic tool uses the following process for its comparison:

1. Connects to the device with the 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.

Troubleshooting Connectivity Issues in an SGA-Enabled Network with SXP-IP Mappings

In a deployment where Security Exchange Protocol (SXP) is used and an endpoint or a user cannot reach a network resource, this tool validates the IP address and SGT mapping to see that the right IP address and SGT binding is established.

Security Group Access devices communicate with their peers and learn their SGT values. The 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 accessed earlier.

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > SXP-IP Mappings**.
- Step 2** Enter the network device IP address of the network device, and click **Select**.
- Step 3** 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 4** Click **User Input Required**, and enter the necessary information.
- Step 5** Check the check box of the peer SXP devices for which you want to compare SXP mappings, and enter the common connection parameters.
- Step 6** Click **Submit**.

Step 7 Click **Show Results Summary** to view the diagnosis and resolution steps.

Related Topics

- [SXP-IP Mappings, page C-7](#)

Troubleshooting Connectivity Issues in an SGA-Enabled Network with IP-SGT Mappings

For devices that are enabled with the Security Group Access solution, each user is assigned an SGT value through RADIUS authentication. When an endpoint or a user cannot reach a network resource, this tool validates the IP address and SGT mapping to see that the right IP address and SGT binding is established.

The IP User SGT diagnostic tool connects to the network device (with the IP address that you provide) and obtains a list of all IP-SGT assignments on the network device. It then checks the RADIUS authentication and accounting records for each IP-SGT pair to find out the IP-SGT-User value that is assigned most recently. Finally, it 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.

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > IP User SGT**.
- Step 2** Enter the information in the fields as needed.
- Step 3** Click **Run**. You are prompted for additional input.
- Step 4** Click **User Input Required**, modify the fields as necessary, and then click **Submit**.
- Step 5** Click **Show Results Summary** to view the diagnosis and resolution steps.
-

Related Topics

- [IP User SGT, page C-8](#)
- [Progress Details Settings, page C-10](#)
- [Results Summary, page C-10](#)

Troubleshooting Connectivity Issues in an SGA-Enabled Network by Comparing Device SGT Mappings

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 (with the IP address that you provide) and obtains the network device SGT value. It then checks the RADIUS authentication records to determine the SGT value that was assigned most recently. Finally, it displays the Device-SGT pairs in a tabular format, and identifies whether the SGT values are the same or different.

-
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > Device SGT**.
- Step 2** Enter the information in the fields as needed.
- The default port number for Telnet is 23 and SSH is 22.
- Step 3** Click **Run**.
- Step 4** Click **Show Results Summary** to view the results of the device SGT comparison.
-

Related Topics

[Device SGT Settings, page C-9](#)

Obtaining Additional Troubleshooting Information

Cisco ISE allows you to download support and troubleshooting information from the Admin portal. 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 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 Network Access Issues” section on page 25-17](#) for more information.

This section contains the following topics:

- [Cisco ISE Support Bundle, page 25-25](#)
- [Cisco ISE Debug Logs, page 25-27](#)

Cisco ISE Support Bundle

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 [“Debug Log Configuration Options” section on page 11-7](#) 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, public key infrastructure (PKI) information and monitoring and reporting.

Debug logs provide troubleshooting information for specific Cisco ISE components. See the [“Cisco ISE Debug Logs” section on page 25-27](#) for more information. To enable debug logs, see [Chapter 11, “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 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, refer to the [Cisco Identity Services Engine CLI Reference Guide, Release 1.2](#).

**Note**

For Inline Posture nodes, you cannot download the support bundle from the Admin portal. 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 Admin portal, 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.

Related Topic

[Downloading Support Bundles, page 25-26](#)

Downloading Support Bundles

You can download the support bundle to your local computer as a simple tar.gpg file. The support bundle will be named with the date and time stamps in the format `ise-support-bundle_ise-support-bundle-mm-dd-yyyy-hh-mm.tar.gpg`. The browser prompts you to save the support bundle to an appropriate location. You can extract the content of the support bundle and view the README.TXT file, which describes the contents of the support bundle, as well as how to import the contents of the ISE database if it is included in the support bundle.

Before You Begin

You must have Super Admin or System Admin privileges to perform the following task.

-
- Step 1** Choose **Operations > Troubleshoot > Download Logs > Appliance node list**.
 - Step 2** Click the node from which you want to download the support bundles.
 - Step 3** In the Support Bundle tab, choose the parameters that you want to be populated in your support bundle.
If you include all the logs, your support bundle will be excessively large and the download will take a long time. To optimize the download process, choose to download only the most recent *n* number of files.
 - Step 4** Enter and re-enter the encryption key for the support bundle.
 - Step 5** Click **Create Support Bundle**.
 - Step 6** Click **Download** to download the newly-created support bundle.

The support bundle is a tar.gpg file that is downloaded to the client system that is running your application browser.

Related Topic

[Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Next Step:

See “[Cisco ISE Debug Logs](#)” section on page 25-27 for information on how to obtain debug logs for specific components.

Cisco ISE Debug Logs

Debug logs provide troubleshooting information for various Cisco ISE components. While reporting problems, you might be asked to enable these debug logs and send them 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.
2. Download the debug logs.

Related Topics

- To configure debug logs for various components, see “[Debug Log Configuration Options](#)” section on page 11-7 and “[Configuring Debug Log Severity Levels](#)” section on page 11-7
- [Downloading Debug Logs](#), page 25-28

Cisco ISE Components and the Corresponding Debug Logs

[Table 25-3](#) provides a list of components and the corresponding debug logs that it generates.

Table 25-3 **Components and Corresponding Debug Logs**

Component	Debug Log
Active Directory	<i>ad_agent.log</i>
CacheTracker	<i>ise-tracking.log</i>
Entity Definition Framework (EDF)	<i>ise-edf.log</i>
JMS	<i>ise-psc.log</i>
License	<i>ise-psc.log</i>
NotificationTracker	<i>ise-tracking.log</i>
Replication-Deployment	<i>replication.log</i>
Replication-JGroup	<i>replication.log</i>
ReplicationTracker	<i>ise-tracking.log</i>
RuleEngine-Attributes	<i>ise-psc.log</i>
RuleEngine-Policy-IDGroups	<i>ise-psc.log</i>
accessfilter	<i>ise-psc.log</i>
admin-infra	<i>ise-psc.log</i>
boot-starp wizard	<i>ise-psc.log</i>

Table 25-3 Components and Corresponding Debug Logs (continued)

Component	Debug Log
cisco-mnt	<i>ise-psc.log</i>
client	<i>ise-psc.log</i>
cpm-clustering	<i>ise-psc.log</i>
cpm-mnt	<i>ise-psc.log</i>
epm-pdp	<i>ise-psc.log</i>
epm-pip	<i>ise-psc.log</i>
eps	<i>ise-psc.log</i>
ers	<i>ise-psc.log</i>
guest	<i>ise-psc.log</i>
guestauth	<i>ise-psc.log</i>
guestportal	<i>ise-psc.log</i>
identity-store-AD	<i>ise-psc.log</i>
infrastructure	<i>ise-psc.log</i>
mdm	<i>ise-psc.log</i>
mdm-pip	<i>ise-psc.log</i>
mnt-alarm	<i>mnt-alarm.log</i>
mnt-report	<i>mnt-report.log</i>
mydevices	<i>ise-psc.log</i>
nsf	<i>ise-psc.log</i>
nsf-session	<i>ise-psc.log</i>
org-apache	<i>ise-psc.log</i>
org-apache-cxf	<i>ise-psc.log</i>
org-apache-digester	<i>ise-psc.log</i>
posture	<i>ise-psc.log</i>
profiler	<i>profiler.log</i>
provisioning	<i>ise-psc.log</i>
prrt-JNI	<i>ise-prrt.log</i>
runtime-AAA	<i>prrt.log</i>
runtime-config	<i>prrt.log</i>
runtime-logging	<i>prrt.log</i>
sponsorportal	<i>ise-psc.log</i>
swiss	<i>ise-psc.log</i>

Downloading Debug Logs

You can use this process to download and save a debug log file.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Operations > Troubleshoot > Download Logs > Appliance node list**.
- Step 2** Click the node from which you want to download the debug logs.
- 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.
- 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
-

Related Topic

- [Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)
- [“Debug Log Configuration Options” section on page 11-7](#)

Monitoring Database

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 you to perform maintenance tasks, such as the topics covered in this section:

- [Back Up and Restore of the Monitoring Database, page 25-29](#)
- [Monitoring Database Purge, page 25-30](#)
- [Log Collection, page 25-12](#)

Back Up and Restore of the Monitoring Database

Monitoring database handles large volumes of data. Over time, the performance and efficiency of the monitoring node depends on how well you manage that data. To increase efficiency, we recommend 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**

You should not perform a backup when a purge operation is in progress. If you start a backup during a purge operation, the purge operation stops or fails.

If you register a secondary Monitoring node, we recommend that you first back up the primary Monitoring node and then restore the data to the new secondary Monitoring node. This ensures that the history of the primary Monitoring node is in sync with the new secondary node as new changes are replicated.

Related Topics

- [Performing an On-Demand Backup, page 12-4](#)
- [Scheduling a Backup, page 12-5](#)
- [Data Restoration Guidelines, page 12-7](#)
- [Restoration of Monitoring Database, page 12-10](#)

Monitoring Database Purge

The purging process allows you to manage the size of the Monitoring database by specifying the number of months to retain data during a purge. The default is three months. This value is utilized when the disk space usage threshold for purging (percentage of disk space) is met. For this option, each month consists of 30 days. A default of three months equals 90 days.

Related Topics

- [Guidelines for Purging the Monitoring Database, page 25-30](#)
- [Purging Older Monitoring Data, page 25-30](#)

Guidelines for Purging the Monitoring Database

The following are some guidelines to follow relating to monitoring database disk usage:

- If the Monitoring database disk usage is greater than 80 percent of the threshold setting, critical alarm is generated indicating that the database size has exceeded the allocated disk size. If the disk usage is greater than 90 percent another alarm is generated.

A purge process runs, creating a status history report that you can view by choosing **Operations > Reports > Deployment Status > Data Purging Audit**. An information (INFO) alarm is generated when the purge completes.

- Purging is also based on the percentage of consumed disk space for the database. When the consumed disk space for the monitoring database is equal to or exceeds the threshold (the default is 80 percent), the purge process starts. This process deletes only the last seven days of monitoring data, irrespective of what is configured in the Admin portal. It will continue this process in a loop until the disk space is below 80 percent. Purging always checks the Monitoring database disk space limit before proceeding.

Purging Older Monitoring Data

The purging process allows you to manage the size of the Monitoring database.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

-
- Step 1** Choose **Administration > System > Maintenance > Data Purging**.
- Step 2** Specify the time period in months, for which the data will be retained. All the data prior to the specified time period will be purged. For this option, each month consists of 30 days. The default of three months equals 90 days.



Note If the configured retention period is less than the existing retention thresholds corresponding to the diagnostics data, then the configured value overrides the existing threshold values. For example, if you configure the retention period as 3 days and this value is less than the existing thresholds in the diagnostics tables (for example, a default of 5 days), then data is purged according to the value that you configure (3 days) in this page.

- Step 3** Click **Submit**.
- Step 4** Verify the success of the data purge by viewing the Data Purging Audit report.
-

Related Topic

[Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions](#)

Next Steps

Proceed with one of the of the following tasks:

- [Log Collection, page 25-12](#)
- [Performing an On-Demand Backup, page 12-4](#)



PART 7

Reference



Administration User Interface Reference

This chapter is a reference for the Cisco Identity Services Engine (ISE) Admin Portal elements, and contains the following Administration related sections:

- [System Administration, page A-1](#)
- [Identity Management, page A-25](#)
- [Network Resources, page A-35](#)
- [Web Portal Management, page A-46](#)

System Administration

Deployment Settings

The Deployment Nodes page enables you to configure **Cisco** ISE and Inline Posture nodes and to set up a deployment.

- To configure Administration, Policy Service, and Monitoring nodes, see [General Node Settings, page A-2](#) and [Profiling Node Settings, page A-5](#).
- To configure an Inline Posture node, see [Inline Posture Node Settings, page A-6](#).

Deployment Nodes List Page

The following table describes the fields on the Deployment Nodes List page, which you can use to configure Cisco ISE and Inline Posture nodes in a deployment. The navigation path for this page is: Administration > System > Deployment.

Table A-1 **Deployment Nodes List Page**

Fields	Usage Guidelines
Hostname	Displays the hostname of the node.
Node Type	Displays the node type. It can be one of the following: • Cisco ISE • Inline Posture node

Table A-1 *Deployment Nodes List Page (continued)*

Fields	Usage Guidelines
Personas	(Only appears if the node type is Cisco ISE) Lists the personas that an Cisco 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 node - SEC(A)—Refers to a secondary Administration node - PRI(M)—Refers to a primary Monitoring node - SEC(M)—Refers to a secondary Monitoring node
Services	(Only appears if the Policy Service persona is enabled) Lists the services that run on this Cisco ISE node. Services can include any one of the following: - Session - Profiling - All
Node Status	Indicates the status of each ISE node in a deployment for data replication. - Green (Connected)—Indicates that an ISE node, which is already registered in the deployment is in sync with the primary Administration node. - Red (Disconnected)—Indicates that an ISE node is not reachable or is down or data replication is not happening. - Orange (In Progress)—Indicates that an ISE node is newly registered with the primary Administration node or you have performed a manual sync operation or the ISE node is not in sync (out of sync) with the primary Administration node. For more details, click the quick view icon for each ISE node in the Node Status column.

General Node Settings

The following table describes the fields on the General Node Settings page, which you can use to set up your deployment and configure services to be run on each of the nodes. The navigation path for this tab is: Administration > System > Deployment > ISE Node > Edit > General Settings.

For Inline Posture Node Settings, see [Inline Posture Node Settings, page A-6](#).

Table A-2 *General Node Settings*

Fields	Usage Guidelines
Hostname	Displays the hostname of the Cisco ISE node.
FQDN	Displays the fully qualified domain name of the Cisco ISE node. For example, ise1.cisco.com.
IP Address	Displays the IP address of the Cisco ISE node.
Node Type	Displays the node type. Could be any one of the following: - Identity Services Engine (ISE) - Inline Posture Node

Table A-2 General Node Settings (continued)

Fields	Usage Guidelines
Personas	
Administration	Check this check box if you want an Cisco 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 7, “Cisco ISE Licenses” • Role—Displays 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 Cisco ISE node. You can have only one primary Cisco 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 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 A-2 General Node Settings (continued)

Fields	Usage Guidelines
Monitoring	Check this check box if you want a Cisco ISE node to assume the Monitoring persona and function as your log collector. There must be at least one Monitoring node in a distributed deployment. At the time of configuring your primary Administration node, you must enable the Monitoring persona. After you register a secondary Monitoring node in your deployment, you can edit the primary Administration node and disable the Monitoring persona, if required. 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 node. If there is only one Monitoring node in your deployment, it assumes the standalone role. If you have two Monitoring nodes in your deployment, Cisco ISE displays the name of the other monitoring node for you to configure the Primary-Secondary roles. To configure these roles, choose one of the following: • Primary—For the current node to be the primary Monitoring node. • Secondary—For the current node to be the secondary Monitoring node. • None—If you do not want the Monitoring nodes to assume the primary-secondary roles. If you configure one of your Monitoring nodes as primary or secondary, the other Monitoring node automatically becomes the secondary or primary node, respectively. Both the primary and secondary Monitoring nodes receive Administration and Policy Service logs. If you change the role for one Monitoring node to None, the role of the other Monitoring node also becomes None, thereby cancelling the high availability pair. After you designate a node as a Monitoring node, you will find this node listed as a syslog target in the following page: Administration > System > Logging > Remote Logging Targets

Table A-2 **General Node Settings (continued)**

Fields	Usage Guidelines
Policy Service	Check this check box to 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. - Choose the group to which this Policy Service node belongs from the Include Node in Node Group drop-down list. Choose <none> if you do not want this Policy Service node to be part of any group. 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 “Configuring Probes per Cisco ISE Node” section on page 21-13. Note When you enable or disable any of the services that run on the Policy Service 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.

Profiling Node Settings

The following table describes the fields on the Profiling Configuration page, which you can use to configure the probes for the profiler service. The navigation path for this page is: Administration > System > Deployment > ISE Node > Edit > Profiling Configuration.

Table A-3 **Profiling Node Settings**

Fields	Usage Guidelines
NetFlow	Check this check box if you want to enable NetFlow per Cisco ISE node that has assumed the Policy Service persona to receive Netflow packets sent from the routers. Choose these options: - Interface—Choose the interface on the ISE node. - Port—Enter the NetFlow listener port number on which NetFlow exports are received from the routers. The default port is 9996.
DHCP	Check this check box if you want to enable DHCP per Cisco ISE node that has assumed the Policy Service persona to listen for DHCP packets from IP helper. Choose these options: - Interface—Choose the interface on the ISE node. - Port—Enter the DHCP server UDP port number. The default port is 67.
DHCP SPAN	Check this check box if you want to enable DHCP SPAN per Cisco ISE node that has assumed the Policy Service persona to collect DHCP packets. Interface—Choose the interface on the ISE node.

Table A-3 Profiling Node Settings (continued)

Fields	Usage Guidelines
HTTP	Check this check box if you want to enable HTTP per Cisco ISE node that has assumed the Policy Service persona to receive and parse HTTP packets. Interface—Choose the interface on the ISE node.
RADIUS	Check this check box if you want to enable RADIUS per ISE node that has assumed the Policy Service persona to collect RADIUS session attributes as well as CDP, LLDP attributes from the IOS Sensor enabled devices.
Network Scan (NMAP)	Check this check box if you want to run a manual network scan on a subnet from the ISE node that has assumed the Policy Service persona to scan endpoints for open ports and the operating system. Enter a valid subnet in the Manual Scan Subnet field and click Run Scan to start a manual subnet scan. For example, you can enter 10.0.10.10/24.
DNS	Check this check box if you want to enable DNS per ISE node that has assumed the Policy Service persona to perform a DNS lookup for the FQDN. Enter the timeout period in seconds. Note For the DNS probe to work on a particular Cisco ISE node in a distributed deployment, you must enable any one of the following probes: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. For DNS lookup, one of the probes mentioned above must be started along with the DNS probe.
SNMP Query	Check this check box if you want to enable SNMP Query per ISE node that has assumed the Policy Service persona to poll network devices at specified intervals. Enter values for the following fields: Retries, Timeout, Event Timeout, and an optional Description. Note In addition to configuring the SNMP Query probe, you must also configure other SNMP settings in the following location: Administration > Network Resources > Network Devices. When you configure SNMP settings on the network devices, ensure that you enable the Cisco Device Protocol (CDP) and Link Layer Discovery Protocol (LLDP) globally on your network devices.
SNMP Trap	Check this check box if you want to enable SNMP Trap probe per ISE node that has assumed the Policy Service Persona to receive linkUp, linkDown, and MAC notification traps from the network devices. Choose any of the following: - Link Trap Query—Check this check box to receive and interpret linkup and linkdown notifications received through the SNMP Trap. - MAC Trap Query—Check this check box to receive and interpret MAC notifications received through the SNMP Trap. - Interface—Choose an interface on the ISE node. - Port—Enter the UDP port of the host to use. The default port is 162.

Inline Posture Node Settings

The following table describes the fields on the Deployment Nodes List page for an Inline Posture node, which you can use to configure the Inline Posture nodes in your deployment. The navigation path for this page is: Administration > System > Deployment > Inline Posture Node > Edit.

Table A-4 *Inline Posture Node Settings*

Fields	Usage Guidelines
Basic Information	
Time Sync Server	Enter the IP address of the primary, secondary, and tertiary time sync server.
DNS Server	Enter the IP address of the primary, secondary, and tertiary DNS server.
Trusted Interface (to protected network)	Enter the Management VLAN ID (all the other information is automatically populated for these options)
Untrusted Interface (to management network)	Enter the IP Address, Subnet Mask, Default Gateway, and Management VLAN ID for the untrusted interface.
Deployment Modes	
Routed Mode	Choose this option for this node to provide router (hop in the wire) functionality for Inline Posture.
Bridged Mode	Choose this option for this node to provide 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. 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.
Filters	
MAC Address	Enter the MAC Address of the device on which to avoid policies. Note For security reasons, we recommend that you always include the IP address along with the MAC address in a MAC filter entry. For more information, see the Warning in Deploying an Inline Posture Node, page 4-13.
IP Address	Enter the IP Address of the device on which to avoid policies.
Description	Enter a description of the MAC Filter.
Subnet Address	Enter the subnet Address of the device on which to avoid policies.
Subnet Mask	Enter the subnet Mask of the device on which to avoid policies
Description	Enter a description of the Subnet Filter.
RADIUS Config¹	
Primary Server	Enter the IP address, shared secret, timeout in seconds, and number of retries for the primary RADIUS server, usually the Policy Service node.
Secondary Server	Enter the IP address, shared secret, timeout in seconds, and number of retries for the secondary RADIUS server.
Client	Enter the IP address, shared secret, timeout in seconds, and number of retries for the device that requests access on behalf of clients, WLC or VPN. Note WLC roaming is not supported in Cisco ISE Release 1.1.1.

Table A-4 Inline Posture Node Settings (continued)

Fields	Usage Guidelines
Enable KeyWrap	Check this check box and specify the following Authentication Settings: • Key Encryption Key • Message Authenticator Code Key • Key Input Format: ASCII 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.
Failover	
Displays only if you have deployed an Inline Posture high availability pair.	
HA Peer Node	Choose the HA Peer Node from the drop-down list. A list of eligible standalone Inline Posture nodes appear from which to choose. 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 Cisco ISE node is a standalone or primary node. • Sync Status—(Only appears for secondary Cisco 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 Cisco ISE node. – Not Applicable—Displayed if the Cisco ISE node is a standalone node.
Service IP (Trusted)	Enter the Trusted Service IP address (eth0) for the traffic interface of the primary node.
Service IP (Untrusted)	Enter the Untrusted Service IP address (eth1) for the traffic interface of the primary node. In the bridged mode, the service IP address is the same for both trusted and untrusted networks.

Table A-4 **Inline Posture Node Settings (continued)**

Fields	Usage Guidelines
Link Detect (Trusted)	Enter the IP address (optional, but recommended as a best practice) for the Link-Detect system for the trusted and untrusted sides. This address is usually the IP address of the Policy Service node, because both the active and standby nodes should always be able to reach the Policy Service node.
Link Detect (Untrusted)	Enter the IP address for the Link-Detect system for the untrusted side.
Link Detect Timeout	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 node. If the active node does not receive notification (ping) from the Policy Service node at the specified intervals, the active node fails over to the standby node.
Heart Beat Timeout	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.
Syncup Peer Node	If the sync status for any secondary node is out of sync, click Syncup Peer Node to force a full database replication. Note You must use the Syncup option to force a full replication if the Sync Status is <i>Out of Sync</i> or the Replication Status is <i>Failed</i> .

1. The timeout and retry values that you specify in the RADIUS config tab for the primary and secondary servers should be based on the timeout and retries that you define on the client such as WLC or ASA. We recommend the following: (IPEP RADIUS Config Timeout * No. of Retries) < (Client device's Timeout * No. of Retries). For example, on the primary and secondary servers, you can configure the timeout to be 5 seconds and the number of retries to be 1, and on the client, you can configure the timeout to be 5 seconds and the number of retries to be 3. So the timeout * no. of retries configured on the IPEP server (5*1=5) is lesser than the value configured on the client (5*3=15).

License Page Parameters

The following table describes the fields on the Current Licenses Page, which you can edit to add or upgrade a license. The navigation path for this page is: **Administration > System > Licensing > Current Licenses**.

Table A-5 **License Page Parameters**

Parameter	Description
Administration Node	Name of the Cisco ISE server instance where the primary node is installed.
ID (PID, VID, SN)	Administration node ID containing PID, VID, and SN, obtained from the licensing information.
Version	Version number of Cisco ISE.

Table A-5 **License Page Parameters**

Parameter	Description
License Type	- Base—The status or type of any Base License that is currently installed on the Administration node. - Advanced—The status or type of any Advanced License that is currently installed on the Administration node. - Wireless—The status or type of any 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 reflects a Wireless License with <x> days remaining on the life of the license. - Wireless Upgrade—The status or type of any Wireless Upgrade License that is currently installed on the Administration node. After the 90-day Evaluation License expires and you install a Wireless Upgrade License, the Current Licenses page reflects a Wireless License with <x> days remaining on the life of the license.
Licensed To	Name of the organization to which the license has been allotted.
Base (Active/Allowed)	A ratio representing 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, the ratio is 1/100. When you install a Wireless or Wireless Upgrade License, the applicable Active/Allowed user counts are automatically calculated to reflect the capabilities of the specific license(s) and are represented in the same existing Base and Advanced columns.
Advanced (Active/Allowed)	A ratio representing 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, the ratio is 1/100. When you install a Wireless or Wireless Upgrade License, the applicable Active/Allowed user counts are automatically calculated to reflect the capabilities of the specific license(s) and are represented in the same existing Base and Advanced columns.

Certificate Store Settings

The Certificate Store page enables you to configure certificates in Cisco ISE that can be used for authentication. This section contains the following topics;

- [Certificate Store Page, page A-11](#)
- [Certificate Store Import Settings, page A-11](#)
- [Certificate Store Edit Settings, page A-12](#)

Certificate Store Page

The following table describes the fields on the Certificate Store page, which you can use to view the certificates that are added to the Administration node. The navigation path for this page is: Administration > System > Certificates > Certificate Store.

Table A-6 **Certificate Store Page**

Fields	Usage Guidelines
Status	Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Friendly Name	Displays the name of the certificate.
Trust for Client Auth	A green checkmark icon indicates that the certificate will be used for establishing trust in all situations, including for client certificates presented to ISE. A yellow dash icon indicates certificate is not used for client authentication, and is only used to verify server certificates (from other ISE nodes or LDAP servers).
Issued To	Common Name (CN) of the certificate subject.
Issued By	Common Name (CN) of the certificate issuer.
Valid From	The “Not Before” certificate attribute.
Expiration	The “Not After” certificate attribute.
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: - Green—Expiring in more than 90 days - Blue—Expiring in 90 days or less - Yellow—Expiring in 60 days or less - Orange—Expiring in 30 days or less - Red—Expired
Include in Trust Store	Indicates whether the certificate is available for utilization as trust certificate. This is initially set to false. To include the certificate as a trust certificate, set the flag to true from the Certificate Store Edit page.

Certificate Store Import Settings

The following table describes the fields on the Certificate Store Import page, which you can use to add Certificate Authority (CA) certificates to Cisco ISE. The navigation path for this page is: Administration > System > Certificates > Certificate Store > Import.

Table A-7 **Certificate Store Import Settings**

Fields	Description
Browse	Click Browse to choose the certificate file from the computer that is running the browser.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <i><common name>#<issuer>#<nnnnn></i> , where <i><nnnnn></i> is a unique five-digit number.

Table A-7 *Certificate Store Import Settings (continued)*

Fields	Description
Trust for client authentication	Check the check box if you want this certificate to be used in authenticating client certificates that are presented to ISE. If the box is not checked, the certificate will only be used to verify server certificates (from other ISE nodes or LDAP servers).
Enable Validation of Certificate Extensions	(Only 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.
Description	Enter an optional description.

Certificate Store Edit Settings

The following table describes the fields on the Certificate Store Edit Certificate page, which you can use to edit the Certificate Authority (CA) certificate attributes. The navigation path for this page is:
Administration > System > Certificates > Certificate Store > Certificate > Edit.

Table A-8 *Certificate Store Edit Settings*

Fields	Usage Guidelines
Certificate Issuer	
Friendly Name	Enter a friendly name for the certificate.
Description	Enter an optional description.
Status	Choose Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Include in Trust Store	Check the check box to include the certificate as a trust certificate.
Certificate Usage	
Trust for client authentication	Check the check box if you want this certificate to be used in authenticating client certificates that are presented to ISE. If the box is not checked, the certificate will only be used to verify server certificates (from other ISE nodes or LDAP servers).
Enable Validation of Certificate Extensions	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.
Certificate Status Validation	
Validate Against OCSP Service	ISE supports two ways of checking the revocation status of a client or server certificate that is issued by a particular CA. The first is to validate the certificate using the Online Certificate Status Protocol (OCSP), which makes a request to an OCSP service maintained by the CA. The second is to validate the certificate against a Certificate Revocation List (CRL) which is downloaded from the CA into ISE. Both of these methods can be enabled, in which case OCSP is used first, and only if a status determination cannot be made then the CRL is used.
	Check the check box to validate the certificate against OCSP services. You must first create an OCSP Service to be able to check this box. See the “OCSP Services” section on page 8-31 for more information on OCSP services.

Table A-8 Certificate Store Edit Settings (continued)

Fields	Usage Guidelines
Reject the request if certificate status could not be determined by OCSP	Check the check box to reject the request if certificate status is determined by OCSP. If you check this check box, an unknown status value returned by the OCSP service will cause ISE to reject the client or server certificate currently being evaluated. See the “OCSP Services” section on page 8-31 for more information on OCSP services.
Download CRL	Check the check box for the Cisco ISE to download a CRL.
CRL Distribution URL	Enter the URL to download the CRL from a CA. This field will be automatically populated if it is specified in the certificate authority certificate. The URL must begin with “http”, “https”, or “ldap.”
Retrieve CRL	The CRL can be downloaded automatically or periodically. Configure the time interval between downloads.
If download failed, wait	Configure the time interval to wait before Cisco ISE tries to download the CRL again.
Bypass CRL Verification if CRL is not Received	Check this check box, for the client requests to be accepted before the CRL is received. If you uncheck this check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file.
Ignore that CRL is not yet valid or expired	Check this check box if you want Cisco ISE to ignore the start date and expiration date and continue to use the not yet active or expired CRL and permit or reject the EAP-TLS authentications based on the contents of the CRL. Uncheck this check box if you want Cisco ISE to check 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.

Logging Settings

These pages allow you to configure the severity of debug logs, create an external log target, and enable Cisco ISE to send log messages to these external log targets.

Remote Logging Target Settings

The following table describes the fields on the Remote Logging Targets page, which you can use to create external locations (syslog servers) to store logging messages. The navigation path for this page is: Administration > System > Logging > Remote Logging Targets.

Table A-9 Remote Logging Target Settings

Fields	Usage Guidelines
Name	Enter the name of the new target.
Target Type	Select the target type. By default it is set to UDP Syslog.
Description	Enter a brief description of the new target.
IP Address	Enter the IP address of the destination machine where you want to store the logs.
Port	Enter the port number of the destination machine.
Facility Code	Choose the syslog facility code to be used for logging. Valid options are Local0 through Local7.

Table A-9 Remote Logging Target Settings (continued)

Fields	Usage Guidelines
Maximum Length	Enter the maximum length of the remote log target messages. Valid options are from 200 to 8192 bytes.
Buffer Message When Server Down	Check this check-box if you want Cisco ISE to buffer the syslog messages when TCP syslog targets and secure syslog targets are unavailable. ISE retries sending the messages to the target when the connection resumes. After the connection resumes, messages are sent by the order from oldest to newest and buffered messages are always sent before new messages. If the buffer is full, old messages are discarded.
Buffer Size (MB)	Set the buffer size for each target. By default, it is set to 100 MB. Changing the buffer size clears the buffer and all existing buffered messages for the specific target are lost.
Reconnect Timeout (Sec)	Give in seconds how long will the TCP and secure syslogs be kept before being discarded, when the server is down.
Select CA Certificate	Select a client certificate.
Ignore Server Certificate Validation	Check this check-box if you want ISE to ignore server certificate authentication and accept any syslog server. By default, this option is set to off unless the system is in FIPS mode when this is disabled.

Related Topics[Configuring Remote Syslog Collection Locations, page 11-4](#)

Logging Category Settings

The following table describes the fields on the Logging Categories page, which you can use to configure the log severity level and choose logging targets for the logs of selected categories to be stored. The navigation path for this page is: Administration > System > Logging > Logging Categories.

Table A-10 *Logging Category Settings*

Fields	Usage Guidelines
Name	Displays the name of the logging category.
Log Severity Level	Allows you to choose the severity level for the diagnostic logging categories from the following options: • 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.
Local Logging	Check this check box to enable logging event for the category on the local node.
Target	Allows you to change the targets for a category by transferring the targets between the Available and the Selected boxes using the left and right icons. 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.

Related Topics

[Setting Severity Levels for Message Codes, page 11-6](#)

Maintenance Settings

These pages help you to manage data using the backup, restore, and data purge features.

Repository Settings

The following table describes the fields on the Repository List page, which you can use to create repositories to store your backup files. The navigation path for this page is: Administration > System > Maintenance > Repository.

Table A-11 *Repository Settings*

Fields	Usage Guidelines
Repository	Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.
Protocol	Choose one of the available protocols that you want to use.
Server Name	(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.

Table A-11 **Repository Settings (continued)**

Fields	Usage Guidelines
Path	Enter the path to your repository. 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.
User Name	(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 =. Supports up to 15 alphanumeric characters.

Related Topics[Creating Repositories, page 12-2](#)

On-Demand Backup Settings

The following table describes the fields on the On-Demand Backup page, which you can use to obtain a backup at any point of time. The navigation path for this page is: Administration > System > Backup & Restore.

Table A-12 **On-Demand Backup Settings**

Fields	Usage Guidelines
Backup Name	Enter the name of your backup file.
Type	Select one of the following: - Configuration backup—contains both application-specific and Cisco ADE operating system configuration data. - Operational backup—contains Monitoring and Troubleshooting data.
Repository Name	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.
Encryption Key	This key is used to encrypt and decrypt the backup file.

Related Topics[Performing an On-Demand Backup, page 12-4](#)

Scheduled Backup Settings

The following table describes the fields on the Scheduled Backup Page, which you can use to restore a full or incremental backup. The navigation path for this page is: Administration > System > Backup and Restore.

Table A-13 **Scheduled Backup Settings**

Fields	Usage Guidelines
Name	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. 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.
Description	Enter a description for the backup.
Repository Name	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.
Encryption Key	Enter a key to encrypt and decrypt the backup file.
Schedule Options	Choose the frequency of your scheduled backup and fill in the other options accordingly.

Related Topics

[Scheduling a Backup, page 12-5](#)

Admin Access Settings

These pages enable you to configure access settings for administrators.

Administrator Password Policy Settings

The following table describes the fields on the Administrator Password Policy page, which you can use to define a criteria that administrator passwords should meet. The navigation path for this page is:

Administration > System > Admin Access > Authentication.

Table A-14 **Administrator Password Policy Settings**

Fields	Usage Guidelines
Minimum Length	Specifies the minimum length of the password (in characters). The default is six characters.
Password should 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 should 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 should not contain <i>variable</i> 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 should 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.

Table A-14 Administrator Password Policy Settings (continued)

Fields	Usage Guidelines
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. Also, specifies the number of characters that must be different from the previous 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.
Lock or Suspend Account with Incorrect Login Attempts	Specifies the number of times Cisco ISE records incorrect administrator passwords before locking the administrator out of Cisco ISE, and suspending or disabling account credentials. An e-mail is sent to the administrator whose account gets locked out. You can enter a custom e-mail remediation message.

Session Timeout and Session Info Settings

The following table describes the fields on the Session page, which you can use to define session timeout and terminate an active administrative session. The navigation path for this page is: Administration > System > Admin Access > Settings > Session.

Table A-15 Session Timeout and Session Info Settings

Fields	Usage Guidelines
Session Timeout	
Session Idle Timeout	Enter the 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.
Session Info	
Invalidate	Check the check box next to the session ID that you want to terminate and click Invalidate .

Related Topics

- [Configuring Session Timeout for Administrators, page 6-15](#)

- [Terminating an Active Administrative Session, page 6-15](#)

Settings

These pages enable you to configure general settings for the various services.

Posture General Settings

The following table describes the fields on the Posture General Settings page, which you can use to configure general posture settings such as remediation time and posture status. The navigation path for this page is: Administration > System > Settings > Posture > General Settings.

Table A-16 **Posture General Settings**

Fields	Usage Guidelines
Remediation Timer	Enter a time value in minutes. The default value is 4 minutes. The valid range is 1 to 300 minutes.
Network Transition Delay	Enter a time value in seconds. The default value is 3 seconds. The valid range is 2 to 30 seconds.
Default Posture Status	Choose Compliant or Noncompliant. The non-agent devices like Linux assumes this status while connecting to the network.
Automatically Close Login Success Screen After	Check the check box to close the login success screen automatically after the specified time. Enter a time value in seconds, in the field next to the check box. You can configure the timer to close the login screen automatically between 0 to 300 seconds. If the time is set to zero, then the NAC Agents and Web Agents do not display the login success screen.

Posture Reassessment Configuration Settings

The following table describes the fields in the Posture Reassessment Configurations Page, which you can use to configure posture reassessment. The navigation path for this page is: Administration > System > Settings > Posture > Reassessments.

Table A-17 **Posture Reassessment Configuration Settings**

Fields	Usage Guidelines
Configuration Name	Enter the name of PRA configuration.
Configuration Description	Enter a description for PRA configuration.
Use Reassessment Enforcement?	Check the check box to apply the PRA configurations for the user identity groups.

Table A-17 *Posture Reassessment Configuration Settings (continued)*

Fields	Usage Guidelines
Enforcement Type	Choose the action to be enforced: • Continue — The user continues to have the privileged access without any user intervention to remediate the client irrespective of the posture requirement. • Logoff — If the client is not compliant, the user is forced to logoff from the network. When the client logs in again, the compliance status is unknown. • Remediate — If the client is not compliant, the agent waits for a specified time for the remediation to happen. Once 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 logoff from the network. 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.
Interval	Enter a time interval in minutes to initiate PRA on the clients after the first successful login. The default value is 240 minutes. Minimum value is 60 minutes and maximum is 1440 minutes.
Grace time	Enter a time interval in minutes to allow the client to complete remediation. The grace time cannot be zero, and should be greater than the PRA interval. It can range between the default minimum interval (5 minutes) and the minimum PRA interval. The minimum value is 5 minutes and the maximum value is 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.
Select User Identity Groups	Choose a unique group or a unique combination of groups for your PRA configuration.
PRA configurations	Displays existing PRA configurations and user identity groups associated to PRA configurations.

Posture Acceptable Use Policy Configuration Settings

The following table describes the fields in the Posture Acceptable Use Policy Configurations Page, which you can use to configure an acceptable use policy for posture. The navigation path for this page is: Administration > System > Settings > Posture > Acceptable Use Policy.

Table A-18 *Posture AUP Configurations Settings*

Fields	Usage Guidelines
Configuration Name	Enter the name of the AUP configuration that you want to create.
Configuration Description	Enter the description of the AUP configuration that you want to create.

Table A-18 Posture AUP Configurations Settings (continued)

Fields	Usage Guidelines
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 users (for NAC Agents, and Web Agents on Windows only) the link to network usage terms and conditions for your network and 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, 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, which contains the index.html at the top level. The .zip file can include other files and subdirectories in addition to the index.html file. These files can reference each other using HTML tags.
AUP URL	Enter the URL to the AUP, which clients must access upon successful authentication and posture assessment.
AUP File	In the AUP File, 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 file at the top level.
Select User Identity Groups	In the Select User Identity Groups drop-down list, 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.
Acceptable use policy configurations—Configurations list	Lists existing AUP configurations and end user identity groups associated with AUP configurations.

EAP-FAST Settings

The following table describes the fields on the Protocol Settings page, which you can use to configure the EAP-FAST, EAP-TLS, and PEAP protocols. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-FAST > EAP FAST Settings.

Table A-19 **Configuring EAP-FAST Settings**

Fields	Usage Guidelines
Authority Identity Info Description	Enter 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	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.

Related Topics

[Configuring EAP-FAST Settings, page 19-11](#)

Generate PAC for EAP-FAST Settings

The following table describes the fields on the Generate PAC page, which you can use to configure protected access credentials for EAP-FAST authentication. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-FAST > Generate PAC.

Table A-20 **Generating PAC for EAP-FAST Settings**

Fields	Usage Guidelines
Tunnel PAC	Click this radio button to generate a tunnel PAC.
Machine PAC	Click this radio button to generate a machine PAC.
SGA PAC	Click this radio button to generate an SGA PAC.
Identity	(For the Tunnel and Machine PAC identity field) 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. This is the hostname as defined on the Adaptive Security Appliance (ASA). The identity string must match the ASA hostname otherwise, ASA cannot import the PAC file that is generated. If you are generating an 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 24-18 for more information on SGA PAC.
PAC Time to Live	(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.

Table A-20 **Generating PAC for EAP-FAST Settings (continued)**

Fields	Usage Guidelines
Encryption Key	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.

Related Topics

[Generating the PAC for EAP-FAST, page 19-12](#)

EAP-TLS Settings

The following table describes the fields on the EAP-TLS Settings page, which you can use to configure the EAP-TLS protocol settings. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-TLS.

Table A-21 **EAP-TLS Settings**

Fields	Usage Guidelines
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.

Related Topics

[Configuring EAP-TLS Settings, page 19-12](#)

PEAP Settings

The following table describes the fields on the PEAP Settings page, which you can use to configure the PEAP protocol settings. The navigation path for this page is: Administration > System > Settings > Protocols > PEAP.

Table A-22 **PEAP Settings**

Fields	Usage Guidelines
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.

Table A-22 *PEAP Settings (continued)*

Fields	Usage Guidelines
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.

Related Topics[Configuring PEAP Settings, page 19-13](#)

RADIUS Settings

The following table describes the fields on the RADIUS Settings page, which you can use to detect the clients that fail to authenticate and to suppress the repeated reporting of successful authentications. The navigation path for this page is: Administration > System > Settings > Protocols > RADIUS.

Table A-23 *RADIUS Settings*

Fields	Usage Guidelines
Suppress Anomalous Clients	Check this check box to detect the clients for which the authentications fail repeatedly. A summary of the failures will be reported every Reporting Interval.
Detection Interval	Enter the time interval in minutes for the clients to be detected.
Reporting Interval	Enter the time interval in minutes for the failed authentications to be reported.
Reject Requests After Detection	Check this check box to reject the requests after the detection. The requests for anomalous clients will be rejected every Request Rejection Interval.
Request Rejection Interval	Enter the time interval in minutes for which the requests to be rejected. This option is available only when you have checked Reject Requests After Detection.
Suppress Repeated Successful Authentications	Check this check box to prevent repeated reporting of successful authentication requests in last 24 hours that have no change in identity context, network device, and authorization.
Accounting Suppression Interval	Enter the time interval in seconds for which the reporting of accounting requests to be suppressed.
Long Processing Step Threshold Interval	Enter the time interval in milliseconds. The steps are displayed in authentication details reports. If execution of a single step exceeds the specified threshold, then it will be highlighted in the authentication details report.

Related Topics[Configuring RADIUS Settings, page 19-13](#)

Security Group Access Settings

For Cisco ISE to function as an Security Group Access (SGA) server and provide SGA services, you must define some global SGA settings. The following table describes fields in Security Group Access page. The navigation path for this page is: Administration > System > Settings > Security Group Access.

Table A-24 **Configuring Security Group Access Settings**

Fields	Usage Guidelines
Tunnel PAC Time to Live	Specify 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. The valid ranges follow: • 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	Cisco 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%.
All Tags Automatically Generated by System	Choose this option if you want all the SGTs to be automatically generated by Cisco ISE. 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. Cisco ISE creates an SGT by default: Unknown, which takes the value as 0. If you configure a range of SGTs, Cisco ISE will not use the values in this range while generating SGT values.
All tags are manually defined	Choose this option to define the SGTs manually.

Identity Management

These pages enable you to configure and manage identities in Cisco ISE.

Endpoints

These pages enable you to configure and manage endpoints that connect to your network.

Endpoint Settings

The following table describes the fields on the Endpoints page, which you can use to create endpoints and assign policies for endpoints. The navigation path for this page is: Administration > Identity Management > Identities > Endpoints.

Table A-25 **Endpoint Settings**

Fields	Usage Guidelines
MAC Address	Enter the MAC address in hexadecimal format to create an endpoint statically. The MAC address is the device identifier for the interface that is connected to the Cisco ISE enabled network
Static Assignment	Check this check box when you want to create an endpoint statically in the Endpoints page and the status of static assignment is set to static. You can toggle the status of static assignment of an endpoint from static to dynamic or from dynamic to static.
Policy Assignment	(Disabled by default unless the Static Assignment is checked) Choose a matching endpoint policy from the Policy Assignment drop-down list. You can do one of the following: • If you do not choose a matching endpoint policy, but use the default endpoint policy Unknown, then the static assignment status is set to dynamic for the endpoint that allows dynamic profiling of an endpoint. • If you choose a matching endpoint policy other than Unknown, then the static assignment status is set to static for that endpoint and the Static Assignment check box is automatically checked.
Static Group Assignment	(Disabled by default unless the Static group Assignment is checked) Check this check box when you want to assign an endpoint to an identity group statically. In you check this check box, the profiling service does not change the endpoint identity group the next time during evaluation of the endpoint policy for these endpoints, which were previously assigned dynamically to other endpoint identity groups. If you uncheck this check box, then the endpoint identity group is dynamic as assigned by the ISE profiler based on policy configuration. 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 policy.
Identity Group Assignment	Choose an endpoint identity group to which you want to assign the endpoint. 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 policy for an endpoint. Cisco ISE includes the following system created endpoint identity groups: • Blacklist • GuestEndpoints • Profiled – Cisco IP-Phone – Workstation • RegisteredDevices • Unknown

Endpoint Import from LDAP Settings

The following table describes the fields on the Import from LDAP page, which you can use to import endpoints from an LDAP server. The navigation path for this page is: Administration > Identity Management > Identities > Endpoints.

Table A-26 *Endpoint Import from LDAP Settings*

Fields	Usage Guidelines
Connection Settings	
Host	Enter the hostname, or the IP address of the LDAP server.
Port	Enter the port number of the 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	Check the Enable Secure Connection check box to import from an LDAP server over SSL.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates. The Root 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 in Cisco ISE.
Anonymous Bind	Check the Anonymous Bind check box to enable the anonymous bind. You must enable either the Anonymous Bind check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.
Admin DN	Enter the distinguished 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.
Query Settings	
MAC Address objectClass	Enter the query filter, which is used for importing the MAC address. For example, ieee802Device.
MAC Address Attribute Name	Enter the returned attribute name for import. For example, macAddress.

Table A-26 **Endpoint Import from LDAP Settings (continued)**

Fields	Usage Guidelines
Profile Attribute Name	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.

Groups

These pages enable you to configure and manage endpoint identity groups.

Endpoint Identity Group Settings

The following table describes the fields on the Endpoint Identity Groups page, which you can use to create an endpoint group. The navigation path for this page is: Administration > Identity Management > Groups > Endpoint Identity Groups.

Table A-27 **Endpoint Identity Group Settings**

Fields	Usage Guidelines
Name	Enter the name of the endpoint identity group that you want to create.
Description	Enter a description for the endpoint identity group that you want to create.
Parent Group	Choose an endpoint identity group from the Parent Group drop-down list to which you want to associate the newly created endpoint identity group. Cisco ISE includes the following five endpoint identity groups: • Blacklist • GuestEndpoints • Profiled • RegisteredDevices • Unknown In addition, it creates two more identity groups, Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group.

External Identity Sources

These pages enable you to configure and manage external identity sources that contain user data that Cisco ISE uses for authentication and authorization.

LDAP Identity Source Settings

The following table describes the fields on the LDAP Identity Sources page, which you can use to create an LDAP instance and connect to it. The navigation path for this page is: Administration > Identity Management > External Identity Sources > LDAP.

LDAP General Settings

The following table describes the fields in the General tab.

Table A-28 **LDAP General Settings**

Fields	Usage Guidelines
Name	Enter a name for the LDAP instance. 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	Enter a description for the LDAP instance. This value is of type string, and has a maximum length of 1024 characters.
Schema	Choose any one of the following built-in schema types and the schema details are prepopulated and are hidden: - Active Directory - Sun Directory Server - Novell eDirectory Note You can edit the details from the predefined schema, but Cisco ISE detects the change and creates a Custom schema. You can click the arrow next to Schema to view the schema details.
Note The following fields contain schema details are displayed only when you choose the Custom schema.	
Subject Objectclass	Enter a value to be 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	Enter the name of the attribute containing the username in the request. The value is of type string and the maximum length is 256 characters.
Certificate Attribute	Enter the attribute that contains the certificate definitions. For certificate-based authentication, these definitions are used to validate certificates that are presented by clients.
Group Objectclass	Enter a value to be 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	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.

Table A-28 LDAP General Settings (continued)

Fields	Usage Guidelines
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	(Only available when you select the Group Objects Contain Reference To Subjects radio button) Specifies how members are sourced in the group member attribute and defaults to the DN.

LDAP Connection Settings

The following table describes the fields in the Connection Settings tab.

Table A-29 LDAP Connection Settings

Fields	Usage Guidelines
Enable Secondary Server	Check this option to enable the secondary LDAP server to be used as a backup if 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	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	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	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 has permission to search all required users under the User Directory Subtree and to search 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 server.
Password	Enter the LDAP administrator account password.
Secure Authentication	Click to use SSL to encrypt communication between Cisco 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 to enable secure authentication with a certificate. See the “Certificate Store” section on page 8-24 and “Adding a Certificate to Certificate Store” section on page 8-27 for information on CA certificates.
Server Timeout	Enter the number of seconds that Cisco 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 A-29 LDAP Connection Settings (continued)

Fields	Usage Guidelines
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.

LDAP Directory Organization Settings

The following table describes the fields in the Directory Organization tab.

Table A-30 LDAP Directory Organization Settings

Fields	Usage Guidelines
Subject Search Base	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.
Group Search Base	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.

Table A-30 LDAP Directory Organization Settings (continued)

Fields	Usage Guidelines
Search for MAC Address in Format	Enter a MAC Address format for Cisco ISE to use for search in the LDAP database. 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 Cisco ISE receives a host lookup request, Cisco ISE converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list to enable searching for MAC addresses in a specific format, where <i><format></i> 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, Cisco 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 <i><start_string></i> box, Cisco 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\user1, Cisco ISE submits user1 to an LDAP server. Note The <i><start_string></i> 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 (<). Cisco ISE does not allow these characters in usernames.
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, Cisco 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, Cisco ISE strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is @ and the username is user1@domain, then Cisco ISE submits user1 to the LDAP server. Note The <i><end_string></i> 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 (<). Cisco ISE does not allow these characters in usernames.

Related Topics

- [LDAP, page 14-19](#)
- [Adding LDAP Identity Sources, page 14-24](#)
- [Configuring Primary and Secondary LDAP Servers, page 14-25](#)

RADIUS Token Identity Sources Settings

The following table describes the fields on the RADIUS Token Identity Sources page, which you can use to configure and connect to an external RADIUS identity source. The navigation path for this page is: Administration > Identity Management > External Identity Sources > RADIUS Token.

Table A-31 RADIUS Token Identity Source Settings

Fields	Usage Guidelines
Name	Enter a name for the RADIUS token server. The maximum number of characters allowed is 64.
Description	Enter a description for the RADIUS token server. 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 Cisco ISE to use 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 Cisco 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 Cisco ISE can authenticate using the secondary RADIUS token server if the primary server cannot be reached. After this time elapses, Cisco ISE reattempts to authenticate against the primary server.
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 Cisco 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 Cisco 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 Cisco 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 Cisco ISE should make to reconnect to the secondary server before dropping the request. Valid values are 1 to 9. The default is 3.

Related Topics

- [RADIUS Token Identity Sources, page 14-27](#)
- [Adding a RADIUS Token Server, page 14-31](#)

RSA SecurID Identity Source Settings

The following table describes the fields on the RSA SecurID Identity Sources page, which you can use to create and connect to an RSA SecurID identity source. The navigation path for this page is: Administration > Identity Management > External Identity Sources > RSA SecurID.

RSA Prompt Settings

The following table describes the fields in the RSA Prompts tab.

Table A-32 **RSA Prompt Settings**

Fields	Usage Guidelines
Enter Passcode Prompt	Enter a text string to obtain the passcode.
Enter Next Token Code	Enter a text string to request the next token.
Choose PIN Type	Enter a text string to request the PIN type.
Accept System PIN	Enter a text string to accept the system-generated PIN.
Enter Alphanumeric PIN	Enter a text string to request an alphanumeric PIN.
Enter Numeric PIN	Enter a text string to request a numeric PIN.
Re-enter PIN	Enter a text string to request the user to re-enter the PIN.

RSA Message Settings

The following table describes the fields in the RSA Messages tab.

Table A-33 **RSA Messages Settings**

Fields	Usage Guidelines
Display System PIN Message	Enter a text string to label the system PIN message.
Display System PIN Reminder	Enter a text string to inform the user to remember the new PIN.
Must Enter Numeric Error	Enter a message that instructs users to enter only numbers for the PIN.
Must Enter Alpha Error	Enter a message that instructs users to enter only alphanumeric characters for PINs.
PIN Accepted Message	Enter a message that the users see when their PIN is accepted by the system.
PIN Rejected Message	Enter a message that the users see when the system rejects their PIN.
User Pins Differ Error	Enter a message that the users see when they enter an incorrect PIN.
System PIN Accepted Message	Enter a message that the users see when the system accepts their PIN.
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.

Related Topics

- [RSA Identity Sources, page 14-32](#)
- [Adding RSA Identity Sources, page 14-35](#)

Identity Management Settings

User Password Policy Settings

The following table describes the fields on the User Password Policy page, which you can use to define a criteria for user passwords. The navigation path for this page is: Administration > Identity Management > Settings > Password Policy.

Table A-34 *User Password Policy Settings*

Option	Description
Minimum Length	Sets the 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 reversed 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
Password History	Enter the number of previous versions from which the password must be different to prevent the repeated use of the same password You can also enter the number of characters that must be different from the previous 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
Lock or Suspend Account with Incorrect Login Attempts	Specifies the number of times Cisco ISE records incorrect user passwords before locking the user out of Cisco ISE, and suspending or disabling account credentials. An e-mail is sent to the user whose account gets locked out. You can enter a custom e-mail remediation message.

Network Resources

Network Devices

These pages enable you to add and manage network devices.

Network Device Definition Settings

The following table describes the fields on the Network Devices page, which you can use to a network access device in Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Devices.

This section covers the Admin portal elements for the following configuration:

- [RADIUS Authentication Settings, page A-37](#)
- [SNMP Settings, page A-38](#)
- [SGA Device Attribute Settings, page A-39](#)

Table A-35 **Network Device Definition Settings**

Fields	Description
Name	Enter the name for the network device. You can provide a descriptive name to the network device that can be different from the hostname of the device. The device name is a logical identifier. Note You cannot edit the name of a device once configured.
Description	Enter the description for the device.
IP Address/Mask	Enter a single IP address and a subnet mask. The following are the 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. 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. • 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.
Model Name	Click the drop-down list to choose the device model, for example, the Cisco Catalyst 6K, the Cisco 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	Click the drop-down list d to choose the version of the software running on the network device, for example, Cisco IOS Release 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.
Network Device Group	Click the Location and Device Type drop-down lists to choose a location and device type that can be associated with the network device. If you do not specifically assign a device to a group when you configure it, it becomes a part of the default device groups (root NDGs), which is All Locations by location and All Device Types by device type and the default device groups (root NDGs) are assigned. For example, All Locations and All Device Groups.

RADIUS Authentication Settings

The following table describes the fields on the New Network Device page, which you can use to configure RADIUS authentication settings for the device. The navigation path for this page is: Administration > Network Resources > Network Devices.

Table A-36 **RADIUS Authentication Settings**

Fields	Usage Guidelines
Protocol	Displays RADIUS as the selected protocol.
Shared Secret	Enter a shared secret, which can be up to 128 characters in length. The shared secret is the key that you have configured on the network device using the radius-host command with the pac option.
Enable KeyWrap	Check this check box only when supported on the network device, which increases RADIUS security via an AES KeyWrap algorithm. Note When you run Cisco ISE in FIPS mode, you must enable KeyWrap on the network device.
Key Encryption Key	(Only appears when you enable KeyWrap) Enter an encryption key that is used for session encryption (secrecy).
Message Authenticator Code Key	(Only appears when you enable KeyWrap) Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
Key Input Format	Choose one of the following formats: • 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. You can specify the key input format that you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that is available on the WLC. (The value that you specify must be the correct [full] length for the key, and shorter values are not permitted.)

SNMP Settings

The following table describes the fields on the New Network Device page, which you can use to configure SNMP settings for the device. The navigation path for this page is: Administration > Network Resources > Network Devices.

Table A-37 *SNMP Settings*

Fields	Usage Guidelines
SNMP Version	Choose an SNMP version from the Version drop-down list to be used for requests. Version includes the following: 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	(Only for SNMP Versions 1 and 2c when selected) Enter the Read Only Community string that provides Cisco ISE with a particular type of access to the device.
SNMP Username	(Only for SNMP Version 3) Enter SNMP username.
Security Level	(Only for SNMP Version 3) Choose the security level from the following: - Auth—Enables Message Digest 5 or Secure Hash Algorithm (SHA) packet authentication - No Auth—No authentication and no privacy security level - Priv—Enables Data Encryption Standard (DES) packet encryption
Auth Protocol	(Only for SNMP Version 3 when the security levels Auth and Priv are selected) Choose the authentication protocol that you want the network device to use. Authentication Protocol includes one of the following for security levels of Auth and Priv: - MD5 - SHA
Auth Password	(Only for SNMP Version 3 when the security levels Auth and Priv are selected) Enter the authentication key that must be at least 8 characters in length. Click Show to display the Auth Password that is already configured for the device.
Privacy Protocol	(Only for SNMP Version 3 when the security level Priv is selected) Choose the privacy protocol that you want the network device to use. Privacy Protocols are one of the following: - DES - AES128 - AES192 - AES256 3DES

Table A-37 *SNMP Settings (continued)*

Fields	Usage Guidelines
Privacy Password	(Only for SNMP Version 3 when the security level Priv is selected) Enter the privacy key. Click Show to display the Privacy Password that is already configured for the device.
Polling Interval	Enter the polling interval in seconds. The default is 3600 seconds.
Link Trap Query	Check this check box to receive and interpret linkup and linkdown notifications received through the SNMP Trap.
Mac Trap Query	Check this check box to receive and interpret MAC notifications received through the SNMP Trap
Originating Policy Service Node	Indicates which ISE server to be used to poll for SNMP data. By default, it is automatic, but you can overwrite the setting by assigning different values.

SGA Device Attribute Settings

The following table describes the fields on the New Network Device page, which you can use to configure SGA Attributes for the device. The navigation path for this page is: Administration > Network Resources > Network Devices.

Table A-38 *SGA Device Attribute Settings*

Fields	Usage Guidelines
SGA Device Notification and Updates Settings	
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. If you check this check box, then the Device Name appears in the Device Id field. You can also change this Device Id to a descriptive name of your choice.
Device Id	(Only when the Use Device ID for SGA Identification check box is not checked). You can use the Device Name as the logical identifier when populated in this field.
Password	Enter the password to authenticate the SGA device (the same password that you have configured on the SGA device command-line interface [CLI]). Click Show to display the password that is used to authenticate the SGA device.
Download Environment Data Every	Specify the expiry time that allows you to configure the time interval in seconds, minutes, hours, weeks, or days between to download the SGA device environment information from Cisco ISE. For example, if you enter 60 in seconds, the device would download its environment data from Cisco ISE every minute. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.
Download Peer Authorization Policy Every	Specify the expiry time that allows you to configure the time interval in seconds, minutes, hours, weeks, or days between to download the peer authorization policy from Cisco ISE. For example, if you enter 60 in seconds, the device would download its peer authorization policy from Cisco ISE every minute. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.

Table A-38 SGA Device Attribute Settings (continued)

Fields	Usage Guidelines
Reauthentication Every	Specify the 802.1X reauthentication period that allows you to configure the time interval in seconds, minutes, hours, weeks or days between for reauthentication. In a network that is configured with the SGA solution, after initial authentication, the SGA device re authenticates itself against Cisco ISE. For example, if you enter 1000 seconds, the device would authenticate itself against Cisco ISE every 1000 seconds. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.
Download SGACL Lists Every	Specify the expiry time for SGACL lists that allow you to configure the time interval in seconds, minutes, hours, weeks or days between to download SGACLs from Cisco ISE. For example, if you enter 3600 seconds, the network device obtains the SGACL lists from Cisco ISE every 3600 seconds. The default value is 86,400 seconds or one day. The 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 SGA device. If you uncheck this check box, the peer devices do not trust this device, and all packets that arrive from this device will be colored or tagged accordingly.
Notify this device about SGA configuration changes	Check this check box if you want Cisco ISE to send SGA CoA notifications to this SGA device.
Device Configuration Deployment Settings	
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 device interface credentials.
Exec Mode Username	Enter the username that has privileges to edit the device configuration in the Exec mode.
Exec Mode Password	Enter the password of the user having privileges to edit the device configuration in the Exec mode.
Enable Mode Password	Enter the password to enable Exec mode password for the device that would allow you to edit its configuration. Click Show to display the Exec mode password that is already configured for this device.
Out Of Band (OOB) SGA PAC Display	
Issue Date	Displays the issuing date of the last SGA PAC that has been generated by Cisco ISE for this SGA device.
Expiration Date	Displays the expiration date of the last SGA PAC that has been generated by Cisco ISE for this SGA device.
Issued By	Displays the name of the issuer (an SGA administrator) of the last SGA PAC that has been generated by Cisco ISE for this device.
Generate PAC	Click Generate PAC to create SGA Protected Access Credentials (PAC). By default, Out Of Band SGA Protected Access Credentials (PAC) information is empty, but appears disabled when populated. SGA PAC information can be automatically populated when you generate SGA PAC for any SGA enabled device.

Default Network Device Definition Settings

The following table describes the fields on the Default Network device page, which allows you to configure a default network device that Cisco ISE can use for RADIUS authentications. The navigation path for this page is: Administration > Network Resources > Network Devices > Default Device.

Table A-39 **Default Network Device Definition Settings**

Fields	Usage Guidelines
Default Network Device Status	Choose Enable from the Default Network Device Status drop-down list to enable the default network device definition.
Protocol	Displays RADIUS as the selected protocol.
Shared Secret	Enter the shared secret that can be up to 128 characters in length. The shared secret is the key that you have configured on the network device using the radius-host command with the pac option.
Enable KeyWrap	Check this check box only when supported on the network device, which increases RADIUS security via an AES KeyWrap algorithm. When you run Cisco ISE in FIPS mode, you must enable KeyWrap on the network device.
Key Encryption Key	Enter an encryption key that is used for session encryption (secrecy) when you enable KeyWrap.
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages when you enable KeyWrap.
Key Input Format	Choose one of the following formats: • 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. You can specify the key input format that you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that is available on the WLC. (The value that you specify must be the correct [full] length for the key, and shorter values are not permitted.)

Network Device Import Settings

The following table describes the fields on the Network Device Import Page, which you can use to import network device details into Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Devices.

Table A-40 **Network Devices Import Settings**

Fields	Usage Guidelines
Generate a Template	Click this link to create a comma-separated value (.csv) template file. You must update the template with network devices information in the same format, and save it locally to import those network devices into any Cisco ISE deployment.
File	Click Browse to the location of the comma-separated value file that you might have created or previously exported from any Cisco ISE deployment. You can import network devices in another Cisco ISE deployment with new and updated network devices information using import.
Overwrite Existing Data with New Data	Check this check box if you want Cisco ISE to replace 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.
Stop Import on First Error	Check this check box if you want Cisco ISE to discontinue import when it encounters an error during import, but Cisco ISE imports network devices until that time of an error. If this check box is not checked and an error is encountered, the error is reported, and Cisco ISE continues to import devices.

Network Device Groups

These pages enable you to configure and manage network device groups.

Network Device Group Settings

The following table describes the fields on the Network Device Groups Page, which you can use to create network device groups. The navigation path for this page is: Administration > Network Resources > Network Device Groups > Groups.

Table A-41 **Network Device Group Settings**

Fields	Usage Guidelines
Name	Enter the name for the root Network Device Group (NDG). For all subsequent child network device groups under the root NDG, enter the name of the new network device group. The full name of the Network Device Group that 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.

Table A-41 **Network Device Group Settings (continued)**

Fields	Usage Guidelines
Description	Enter the description for the root or the child Network Device Group.
Type	Enter the type for the root Network Device Group. For all subsequent child network device groups under the root NDG, the type is inherited from the parent NDG and therefore all the child NDGs under a root NDG will be of the same type. If this NDG is a root NDG, then the type will be 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.

Network Device Group Import Settings

The following table describes the fields on the Network Device Group Import Page, which you can use to import network device groups into Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Device Groups > Groups.

Table A-42 **Network Device Groups Import Settings**

Fields	Usage Guidelines
Generate a Template	Click this link to create a comma-separated value (.csv) template file. You must update the template with network device groups information in the same format, and save it locally to import those network device groups into any Cisco ISE deployment.
File	Click Browse to the location of the comma-separated value file that you might have created or previously exported from any Cisco ISE deployment. You can import network device groups in another Cisco ISE deployment with new and updated network device groups information using import.
Overwrite Existing Data with New Data	Check this check box if you want Cisco ISE to replace existing network device groups with the device groups in your import file. If you do not check this check box, new network device group that are available in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box if you want Cisco ISE to discontinue import when it encounters an error during import, but Cisco ISE imports network device groups until that time of an error. If this check box is not checked and an error is encountered, the error is reported, and Cisco ISE continues to import device groups.

External RADIUS Server Settings

The following table describes the fields on the External RADIUS Server page, which you can use to configure a RADIUS server. For Cisco ISE to act as a RADIUS server, you must configure it in this page. The navigation path for this page is: Administration > Network Resources > External RADIUS Servers.

Table A-43 External RADIUS Server Settings

Fields	Usage Guidelines
Name	Enter the name of the external RADIUS server.
Description	Enter a description of the external RADIUS server.
Host IP	Enter the IP address of the external RADIUS server.
Shared Secret	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	Enable this option to increase the RADIUS protocol security via an AES KeyWrap algorithm, to help enable FIPS 140-2 compliance in Cisco ISE.
Key Encryption Key	(Only if you check the Enable Key Wrap check box) Enter a key to be used for session encryption (secrecy).
Message Authenticator Code Key	(Only if you check the Enable Key Wrap check box) Enter a key to be 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	Enter the RADIUS authentication port number. The valid range is from 1 to 65535. The default is 1812.
Accounting Port	Enter the RADIUS accounting port number. The valid range is from 1 to 65535. The default is 1813.
Server Timeout	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	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.

RADIUS Server Sequences

The following table describes the fields on the RADIUS Server Sequences page, which you can use to create a RADIUS server sequence. The navigation path for this page is: Administration > Network Resources > RADIUS Server Sequences.

Table A-44 RADIUS Server Sequences

Fields	Usage Guidelines
Name	Enter the name of the RADIUS server sequence.
Description	Enter an optional description.

Table A-44 RADIUS Server Sequences (continued)

Fields	Usage Guidelines
Host IP	Enter the IP address of the external RADIUS server.
User Selected Service Type	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.
Remote Accounting	Check this check box to enable accounting in the remote policy server.
Local Accounting	Check this check box to enable accounting in Cisco ISE.
Advanced Attribute Settings	
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\userA and the separator is \, the username becomes userA.
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 userA@abc.com and the separator is @, the username becomes userA. - 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. - If you activate <i>both</i> the \ and @ stripping functions, and you are using Cisco AnyConnect, Cisco ISE does not accurately trim the first \ from the string. However, each stripping function that is used individually, however, works as it is designed with Cisco AnyConnect.
Modify Attributes in the Request to the External RADIUS Server	Check this check box to allow Cisco ISE to manipulate attributes that come from or go to the authenticated RADIUS server. The attribute manipulation operations include these: Add—Add additional attributes to the overall RADIUS request/response. Update—Change the attribute value (fixed or static) or substitute an attribute by another attribute value (dynamic). Remove—Remove an attribute or an attribute-value pair. RemoveAny—Remove any occurrences of the attribute.
Continue to Authorization Policy	Check this check box to divert the proxy flow to run the authorization policy for further decision making, based on identity store group and attribute retrieval. If you enable this option, attributes from the response of the external RADIUS server will be applicable for the authentication policy selection. Attributes that are already in the context will be updated with the appropriate value from the AAA server accept response attribute.
Modify Attributes before send an Access-Accept	Check this check box to modify the attribute just before sending a response back to the device.

NAC Manager Settings

The following table describes the fields on the New NAC Managers page, which you can use to add a NAC Manager. The navigation path for this page is: Administration > Network Resources > NAC Managers.

Table A-45 NAC Manager Settings

Fields	Usage Guidelines
Name	Enter the name of the Cisco Access Manager (CAM).
Status	Click the Status check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.
Description	Enter the description of the CAM.
IP Address	Enter the IP address of the CAM. Once you have created and saved a CAM in 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. 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.
Username	Enter the username of the CAM administrator that allows you to log on to the user interface of the CAM.
Password	Enter the password of the CAM administrator that allows you to log on to the user interface of the CAM.

Web Portal Management

Sponsor Group Policy Settings

The following table describes the fields on the Sponsor Group Policy page, which you can use to define sponsor group policies. The navigation path for this page is: Administration > Web Portal Management > Sponsor Group Policy.

You are not allowed to delete sponsor groups that are in use in a sponsor group policy

Table A-46 Sponsor Group Policy Settings

Fields	Usage Guidelines
Status	Choose to enable or disable the policy.
Policy Name	Enter a descriptive name for the new policy.
Identity Groups	Choose the identity group to associate with the defined sponsor group. For example, the default Manage All Accounts policy includes the SponsorAllAccount identity group.
Other Conditions	Choose or create additional conditions.
Sponsor Groups	Choose the sponsor group to which you want to apply these settings. For example, the default Manage All Accounts policy defines the sponsor group as SponsorAllAccounts.

Related Topics

- [Sponsor Group Policies, page 16-6](#)
- [Creating a Sponsor Group Policy, page 16-6](#)

Sponsor Group Settings

The following table describes the fields on the Guest Sponsor Group page, which you can use to define sponsor groups. The navigation path for this page is: Administration > Web Portal Management > Sponsor Groups. You are not allowed to delete sponsor groups that are in use in a sponsor group policy

Table A-47 ***Sponsor Group Settings***

Fields	Usage Guidelines
General	
Name	Enter a name for the sponsor group. When choosing a name, you might want to consider which identity groups with which you will be associating the sponsor group. For example, the default sponsor groups have names similar to the default user identity groups to assist you in associating the correct identity group and sponsor group when creating the sponsor policies.
Description	Enter a description for the sponsor group.
Authorization Levels	
Allow Login	Indicate whether or not to allow sponsors to sign into the Sponsor portal.
Create Single Account	Indicate whether sponsors can create individual guest accounts.
Create Random Accounts	Indicate whether sponsors can create random guest accounts.
Import CSV	Indicate whether sponsors can import guest accounts.
Send Email	Indicate whether sponsors can email the account details to guest users.
Send SMS	Indicate whether sponsors to send text messages with the account details to guest users.
View Guest Password	Indicate whether sponsors can view guest passwords when creating accounts.
Allow Printing Guest Details	Indicate whether sponsors can print the account details for guest users.
View/Edit Accounts	Choose one of these settings: • 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.

Table A-47 **Sponsor Group Settings (continued)**

Fields	Usage Guidelines
Suspend/Reinstate Accounts	Choose one of these settings: - 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.
Account Start Time	Restrict 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.
Maximum Duration of Account	Specify 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 when creating a guest account when this value is less than the one specified in the time profile.
Guest Roles	
Guest Roles	Choose the guest roles that a sponsor in this group can use to assign different levels of access to a guest account. These roles are used in the authorization policies to associate guest user accounts to identity groups. Guest roles with a yellow icon indicate that they are an ActivatedGuest role.
Time Profiles	
Available Currently Selected	Choose any available default or custom time profiles: - DefaultEightHours—The guest user can login within eight hours of the account creation, after which the account expires. The account start time is equal to the user creation time, and the end time is eight hours from the start time. - DefaultFirstLoginEight—The account start time starts when the guest user first logs in to the guest portal, and the end time is eight hours later. - DefaultStartEnd—The sponsor can set the account start and end time.

Related Topics

- [Sponsor Groups, page 16-5](#)
- [Creating Sponsor Groups, page 16-5](#)

Web Portal Management Settings

These pages enable you to apply changes to all Cisco ISE web portals.

General Portal Theme Settings

The following table describes the fields on the Portal Theme Page, which you can use to determine the look and feel of all the Cisco ISE web portals. The navigation path for this page is: Administration > Web Portal Management > Settings > General > Portal Theme.

Table A-48 **General Portal Theme Settings**

Fields	Usage Guidelines
Style Settings	
Login Page Logo	Upload a jpeg, gif, or png image file to use as the logo on the portal Login page for the Guest, Sponsor, and My Devices portals. When you upload the image, it is automatically resized to fit an image size of 86 pixels (width) by 46 pixels (height). To avoid distortion, resize your image to fit these dimensions.
Login Page Background Image	Change the background image on the portal login page for the Guest, Sponsor, and My Devices portals. Supported image formats include jpeg, gif, and png. The supported size image size is 533 pixels (width) by 314 pixels (height).
Banner Logo	Upload a jpeg, gif, or png image file to use as the banner logo on the Guest, Sponsor, and My Devices portals. When you upload the image, it is automatically resized to fit an image size of 86 pixels (width) by 45 pixels (height). To avoid distortion, resize your image to fit these dimensions.
Banner Background Image	Upload a jpeg, gif, or png image file to use as the background image for the Guest, Sponsor, or My Devices portals. Change the portal banner background image. The supported size image size is 1724 pixels (width) x 133 pixels (height), but the banner background color displays to fill the remaining area.
Login Background Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format to change the background color of the portal login page for the Guest, Sponsor, and My Devices portals. The logic background color displays only if the logic page background image is not set or is too small to fill the designated area.
Banner Background Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format to change the banner background color of the portal. The banner background color displays only if the banner background image is not set or is too small to fill the designated area.
Banner Text Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format.
Banner Link Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format.
Mobile Device Style Settings	
Logo Image	Upload a jpeg, gif, or png image file to use as the banner logo on the mobile-optimized Guest portal. The recommended image size is 100 pixels (width) x 61 pixels (height).

Table A-48 **General Portal Theme Settings**

Fields	Usage Guidelines
Banner Image	Upload a jpeg, gif, or png image file to use as the banner image on the mobile-optimized Guest portal. The recommended image size is 754 pixels (width) x 47 pixels (height), but it resizes appropriately when switching between portrait and landscape orientation on mobile devices.
Banner Background Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format.
Banner Text Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format.
Display Settings	
Display pre-login banner	Check to display messages to users before they log into the Sponsor, My Devices, or Guest portals. The pre-login banner displays on the login page for each portal.
Display post-login banner	Check to briefly display messages to users after they log into the Sponsor or My Devices portals. The post-login banner displays for 15 seconds on the Sponsor and My Devices portal and does not apply to the Guest portal.

Related Topics

- [Customizing the Web Portal Images and Color Scheme, page 15-5](#)
- [Displaying Banner Messages to Users When Logging In or Out of Portals, page 15-6](#)

Port Settings for Web Portals

The following table describes the fields on the Web Portal Settings page, which you can use to define ports and interfaces for the different Cisco ISE web portals. The navigation path for this page is: Administration > Web Portal Management > Settings > General > Ports.

Table A-49 **Port Settings for Web Portals**

Fields	Usage Guidelines
Admin Portal Settings	
HTTP Port	The default value is 80, and you cannot change this setting.
HTTPS Port	The default value is 443, and you cannot change this setting.
Blacklist Portal Settings	
HTTPS Port	Enter the port value between 8000-8999; the default value is 8444. You cannot set this value to be the same as the Guest, Sponsor, or My Devices portals. If you upgraded to Cisco ISE 1.2 with port 8444 already assigned to another portal, the Blacklist portal will be set to an unused port in 8000 to 8999 range instead.

Table A-49 Port Settings for Web Portals (continued)

Fields	Usage Guidelines
Allowed Interfaces	Check to partition portal traffic to specific Gigabit Ethernet interfaces. You must configure the Ethernet interfaces using IP addresses on different subnets. Any portals assigned to the same HTTPS port also use the same Ethernet interfaces. For example, if you assign both the Sponsor and My Devices portals to port 8443, and you disable GigabitEthernet 0 on the Sponsor portal, that interface is also automatically disabled for the My Devices portal.
Guest Portal, Client Provisioning, My Devices, and Sponsor Portal Settings	
HTTPS Port	Enter the port value between 8000-8999; the default value is 8443. The port range restriction is new in Cisco ISE 1.2. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction. For posture assessments and remediation only, the Client Provisioning portal uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.
Allowed Interfaces	Check to partition portal traffic to specific Gigabit Ethernet interfaces. You must configure the Ethernet interfaces using IP addresses on different subnets. Any portals assigned to the same HTTPS port also use the same Ethernet interfaces. For example, if you assign both the Sponsor and My Devices portals to port 8443, and you disable GigabitEthernet 0 on the Sponsor portal, that interface is also automatically disabled for the My Devices portal.
Portal FQDNs	
Default Sponsor Portal FQDN	Check these options if you want to change the URLs from the default settings. You must enter a fully-qualified domain name (such as mydevices.yourcompany.com). The default settings are: - My Devices portal: <code>https://ip_address:8443/mydevices/</code>, where <i>ip_address</i> is the IP address of the Cisco ISE server. - Sponsor portal: <code>https://ip_address:8443/sponsorportal/</code>, where <i>ip_address</i> is the IP address of the Cisco ISE server. You must also update DNS to ensure the FQDN of the new URL resolves to a valid policy service node IP address. Additionally, to avoid certificate warning messages due to name mismatches, you should also include the FQDN of the customized URL in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE policy service node. This requires that you specify the SAN attribute outside of Cisco ISE, such as from the certificate authority (CA) server when submitting the Certificate Signing Request (CSR) or by using a utility like openssl to create a custom CSR.
Default My Devices Portal FQDN	

Related Topics

- [Specifying Ports and Ethernet Interfaces for End-User Portals, page 15-2](#)
- [Specifying the Fully Qualified Domain Name for Sponsor and My Devices Portals, page 15-3](#)

Guest Purge Settings

The following table describes the fields on the Purge Settings page, which you can use to remove expired guest accounts. The navigation path for this page is: Administration > Web Portal Management > Settings > General > Purge.

Table A-50 **Guest Purge Settings**

Fields	Usage Guidelines
Enable purge settings for expired guest accounts	Check this option to schedule a purge of expired guest accounts.
Purge occurs every	Enter the purge interval from 1-365 days. Default setting is 15 days.
Hour of the day when the last purge should occur	Specify the hour of the day when the purge should occur. Default setting is at 23:00 hours.
Date of last purge	Displays the date of the most recent purge.
Date of next purge	Displays the date of the next scheduled purge.
Purge Now	Click to immediately purge the expired guest user records.

Related Topics

[Purging Expired Guest Accounts, page 16-24](#)

Sponsor Language Template Settings

The following table describes the fields on the Sponsor Language Template page, which you can use to customize the Sponsor Portal. The navigation path for this page is: Administration > Web Portal Management > Settings > Sponsor > Language Template.

Keep these guidelines in mind when editing these fields:

- You should 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.
- You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

Table A-51 **Sponsor Portal Language Template Settings**

Fields	Usage Guidelines
Configure Template Definition	Enter a unique name and description and a valid locale to associate with the language. 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}.
Configure Home Page	Customize the fields displayed on the main page in the Sponsor portal.
Configure Login Page	Customize the information displayed when users log into the Sponsor portal.
Configure Change Password	Customize the fields that display when sponsors change their passwords.

Table A-51 ***Sponsor Portal Language Template Settings (continued)***

Fields	Usage Guidelines
Configure Common Table Headers	Specify the fields that appear as column headings in tables.
Configure Create Single Guest Account	Specify the fields that display when sponsors create a single guest account.
Configure Create Random Guest Accounts	Specify the fields that display when sponsors create random accounts.
Configure Import Guest Accounts	Specify the fields that display when sponsors import accounts.
Configure Bulk Create Status Display	Specify the fields that display when sponsors create multiple accounts.
Configure Print Tabular Display	Specify the fields that display when sponsors print account details.
Configure Sponsor Settings Customizations	Specify the fields that display in My Settings page in the Sponsor portal.
Configure Email Notification	Customize the fields and content of the e-mail that will be sent to guests with their account details.
Configure SMS Text Message Notification	Customize the fields and content of the SMS text message that will be sent to guests with their account details.
Configure Print Notification	Customize the fields and content of the message to be printed for guests with their account details.
Configure Date/Time Formats	Choose the format in which to display the date and time.
Configure Info/Error Messages	Customize the error messages display to users while using the Sponsor portal.
Configure JavaScript Enable Instructions	Customize the instructions for enabling JavaScript in supported web browsers.
Configure Popup Dialog Messages	Customize the information that displays to users while using the Sponsor portal.
Configure Common Items	Customize the fields common across the pages in the Sponsor portal.

My Devices Portal Language Template Settings

The following table describes the fields on the My Devices Language Template Page, which you can use to select a language and to customize the My Devices Portal. The navigation path for this page is: Administration > Web Portal Management > Settings > My Devices > Language Template.

Keep these guidelines in mind when editing these fields:

- You should 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.
- You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

Table A-52 *My Devices Portal Language Template Settings*

Fields	Usage Guidelines
Configure Template Definition	Enter a unique name and description and a valid locale to associate with the language. 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}.
Configure Login Page	Customize the information displayed when users log into the My Devices portal.
Configure Device Management Page	Customize the field names and labels for the options available to users when manage their devices. Users can enter only a maximum of 256 characters in the Page Description text box when they add devices.
Configure Acceptable Use Policy Page	Customize the acceptable use policy for your company, which appears on the login page and the device registration page of the My Devices portal.
Configure Info/Error Messages	Customize the error messages and information that display to users while using the My Devices portal.
Configure JavaScript Enable Instructions	Customize the instructions for enabling JavaScript in supported web browsers.
Configure Miscellaneous Items	Indicate the field names and labels for remaining UI elements.
Configure Blackhole Portal Items	Indicate portal name and error message that displays when a user attempts to access the My Devices portal using a blacklisted device.

Related Topics

[Customizing the Portal Language, Text, and Error Messages, page 15-4](#)

My Devices Portal Settings

The following table describes the fields on the My Devices Portal Settings page, which you can use to configure the My Devices Portal. The navigation path for this page is: **Administration > Web Portal Management > Settings > My Devices > Portal Configuration**.

Table A-53 *My Devices Portal Settings*

Fields	Usage Guidelines
Enable My Devices Portal	Check to allow employees to register and manage their devices using the My Devices portal.
Enable the Acceptable Use Policy link	Check to require an acceptable use policy for employees. You must also update the language template to reflect your company's policy.
The maximum number of devices to register	Enter the maximum number of devices that an employee can register. The default value is set to 5 devices.

Table A-53 *My Devices Portal Settings (continued)*

Fields	Usage Guidelines
Email Address	Customize the e-mail address associated with the Contact link on the login and main page of the My Devices Portal.
Phone Number	Customize the phone number associated with the Contact link on the login and main page of the My Devices Portal.

Related Topics

- [Customizing the Portal Language, Text, and Error Messages, page 15-4](#)

Guest Portal Language Template Settings

The following table describes the fields on the Guest Language Template page, which you can use to select a language for the Guest Portal and to customize it. The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Language Template.

Keep these guidelines in mind when editing these fields:

- You should 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.
- You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

Table A-54 *Guest Portal Language Template Settings*

Fields	Usage Guidelines
Configure Template Definition	Enter a unique name and description and a valid locale to associate with the language. 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}.
Configure Login Page	Customize the information displayed when users log into the Guest portal.
Configure Acceptable Use Policy Page	Customize the acceptable use policy for your company, which appears on the login page and the device registration page of the Guest portal.
Configure Change Password	Customize the fields that display when guests change their passwords.
Configure Self Registration	Customize the fields that display when guests register independently.
Configure Device Registration	Customize the fields that display when guests register their devices.
Configure VLAN/Install Release	Customize the fields that display when forcing a VLAN reconfiguration.
Configure Error Messages	Customize the error messages displayed to users when using the Guest portal.
Configure JavaScript Enable Instructions	Customize the instructions for enabling JavaScript in supported web browsers.
Configure Popup Dialog Messages	Customize the information that displays to users while using the Guest portal.

Table A-54 Guest Portal Language Template Settings (continued)

Fields	Usage Guidelines
Configure Miscellaneous Items	Customize the field names and labels for remaining items.
Configure Self-Provisioning Portal (Registration)	Customize the registration page for the Self-Provisioning portal.
Configure Self-Provisioning Portal (Install)	Customize the installation page for the Self-Provisioning portal.
Configure Mobile Device Management (MDM)	Customize the field names for the MDM enrollment and compliance pages.

Related Topics

- [Customizing Portal UI Fields and Error Messages, page 15-5](#)
- [Requiring an Acceptable Use Policy for Guests, page 16-19](#)

Multi-Portal Configuration Settings

The following table describes the fields on the Multi-Portal Configurations page, which you can use to.

The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations.

Table A-55 Multi-Portal Configurations Settings

Fields	Usage Guidelines
General	
Name	Enter the name of the portal to use to access the portal. This name also 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 <i>ClientPortal</i> will have the following access URL: <code>https://ip address:port number/guestportal/portals/ClientPortal/portal.jsp</code>
Description	Enter an optional description.
Portal type	Choose a portal type: • 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
EndPoint Identity Group	(Only for DRW portals) Choose an endpoint identity group. Cisco ISE provides the GuestEndpoints default identity group to use for the DRW portal.
Operations	

Table A-55 **Multi-Portal Configurations Settings (continued)**

Fields	Usage Guidelines
Acceptable use policy	Choose whether guests must accept an acceptable use policy to fully enable their account. If guests do not accept the policy, they will not obtain network access. Default setting for the DefaultGuestPortal is First Login. For new portals, the default is Not Used.
Enable Self-Provisioning Flow	Check to allow employees to directly connect their personal devices to the network. This option enables them to provision these devices using the native supplicant, which is available for Windows, Mac, iPhone, iPad, and Android devices. If you do not want to enable self-provisioning from the devices directly, you do not need to enable this feature. Employees can still add personal devices using the My Devices Portal. This feature requires an advanced license and is off by default when upgrading and on by default for new installations.
Enable Mobile Portal	Check to allow guests using mobile devices to access a mobile-optimized version of the Guest portal.
Allow guest users to change password	Check to allow guest users to change their password after the sponsor creates their initial account credentials. If guest users change their passwords, sponsors cannot provide guests with their login credentials if lost. The sponsor must create a new guest account.
Require guest users to change password at expiration and first login	Check to require guest users to change their password both at first login and after expiration. Sponsors cannot provide guests with their login credentials if lost. The sponsor must create a new guest account.
Guest users should download the posture client	Check to redirect the guest user to the Client Provisioning portal. Guests will be required to download a client provisioning agent for controlling posture before obtaining full network access. If you choose this option, the guest login flow performs a central web authorization (CWA), and the guest portal is redirected to the Client Provisioning portal after performing AUP and change password checks. In this case, the posture subsystem performs a CoA to the NAD to reauthenticate the client connection once the posture has been assessed. If you choose Vlan Dhcp Release, posture will perform the client side IP release and renew operation. Client Provisioning does not occur in Local Web Authentication scenarios.

Table A-55 **Multi-Portal Configurations Settings (continued)**

Fields	Usage Guidelines
Guest users should be allowed to do self service	Check to allow guest users to complete their personal information and create a new user account. When enabled, the Self Registration screen appears as a link on the guest user login page. User accounts are created with a random generated password. This password follows the password policy that is set for the guest users. To use this feature, you must also configure the default guest roles and time profiles in the Guest Portal Policy page.
Guest users should be allowed to do device registration	Check to allow guests to add devices to the network. When enabled, the Device Registration screen appears as a link on the guest user login page. You can configure the maximum number of devices per user from the Guest Portal Policy page. You can also add the 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.
Vlan Dhcp Release	Check the VLAN DHCP Release option to refresh the IP address for Windows, Mac OS, Unix, or LINUX devices after a VLAN change in both wired or wireless environments for Guest with no posture. This affects the Central WebAuth (CWA) flow during final authorization when the network access changes the guest VLAN to a new VLAN. The guest's old IP address must be released before the VLAN change and a new guest IP must be requested through DHCP once the new VLAN access is in place. An applet downloads to perform the IP release renew operation. The VLAN DHCP Release option does not work on mobile devices. Instead, guests must manually reset the IP address. This method varies by devices. For example, on Apple iOS devices, users can select the Wi-Fi network and click the Renew Lease button.
Delay to Release	Enter the delay to release time. Enter a brief time because it must 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.
Delay to COA	Enter the time to delay Cisco ISE from executing the CoA. 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.\
Delay to Renew	Enter the delay to renew value. This time 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.
Customization	
Language template	Choose the display language to use for the Guest portal. You cannot change this setting if the User browser locale option is checked.
Use browser locale	Check this option to allow the Guest portal to use the browser locale as the display language.

Table A-55 **Multi-Portal Configurations Settings (continued)**

Fields	Usage Guidelines
Authentication	
Identity Store Sequence	Specify the identity store sequence to apply for the guest flow. This sequence defines the order in which Cisco ISE will look for user credentials in the different databases. You can use one of the default sequences or first define a new one to use from Identity Management > Identity Source Sequences .
File Uploads (Available only when creating a custom portal)	
Upload File	Upload the HTML files you have created for the Login, AUP, Change Password, and Self Registration pages. 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 back end scripts in the Cisco ISE server. Only HTML, HTM, JPEG, GIF, PNG, and CSS files are allowed.
Delete File	Select the uploaded files you want to delete.
File Mapping	
Login file	Indicate the uploaded HTML files to associate with each guest page. Based on the selections you made on the General tab, some fields might be grayed out. Required files are based on the selections made in the General tab. To ensure that the guest flow redirects and displays the appropriate portal pages, you must be sure to associate all required files.
AUP file	
Change Password file	
Self Registration file	
Self Registration Results file	
Device Registration file	
Guest Success file	
Error Page file	

Guest Portal Policy Settings

The following table describes the fields on the Guest Portal Policy page, which you can use to configure the Guest Portal. The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Portal Policy.

Table A-56 **Guest Portal Policy Settings**

Fields	Usage Guidelines
Self-Registration	
Guest Role	Choose the default guest role to assign to the guest user after self-registration. This role associates the guest user to an identity group based on the policies defined in the system. Guest roles with a yellow icon indicate that they are an ActivatedGuest role.
Time Profile	Choose the default time profile to assign to the guest user after self-registration.
Login Restrictions	

Table A-56 Guest Portal Policy Settings (continued)

Fields	Usage Guidelines
Allow only one guest session per user	Check to restrict guest users to connecting to the network with only one device at a time. If a guest user attempts to connect another device, the currently-connected device is disconnected from the network.
Maximum Login Failures	Enter the maximum number of failed logins that can occur before a guest account is suspended. The default value is five.
Device Registration Portal Limit	Enter the maximum number of devices that can be registered for each guest. The device registration portal will not allow the guest user to add more devices if the maximum number has been reached. You can limit this setting below the maximum number of devices currently registered to a guest account, but this change will not affect the existing registered devices.
Guest Password Expiration (Days)	Enter the number of days after which the guest password will expire and the guest will have to reset their password. You must also require guests to change their passwords at expiration from: Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration > Operations.

Guest Time Profile Settings

The following table describes the fields on the Guest Time Profiles page, which you can use to create new time profiles to specify how long guests' have network access. These changes are global and affect all Guest portals. The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Time Profiles.

Table A-57 Guest Time Profile Settings

Fields	Usage Guidelines
Name	Enter a name for the time profile using alphanumeric characters only; do not include spaces or any special characters. Keep this name brief yet descriptive enough for sponsors to be able to interpret it when creating guest accounts.
Description	Enter an optional description.
Time Zone for Restrictions	Choose a time zone to be used for the time restrictions.
Account Type	Choose one of these options: - FromCreation—The guest user can login within the specified duration time from the account creation, after which the account expires. - FromFirstLogin—The account start time starts when the guest user first logs in to the guest portal, and the end time equals the specified duration time. - StartEnd—The sponsor can set the account start and end time.

Table A-57 **Guest Time Profile Settings (continued)**

Fields	Usage Guidelines
Duration	Enter the time 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 FromCreation or FromFirstLogin.
Restrictions	Enter the day of the week and a start and end clock time. The Time Zone for Restrictions value affects these time settings. 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. The time profile can have restrictions that fall outside the start and end time specified in a Guest account during 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. For the DefaultEightHours and DefaultFirstLoginEight time profiles, the expiration date will be calculated based on the sponsor group duration or time profile duration, whichever is the minimum.

Guest Username Policy Settings

The following table describes the fields on the Guest Username Policy page, which you use to specify requirements and guidelines for guest usernames. These changes are global and affect all Guest portals. The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Username Policy.

Table A-58 **Guest Username Policy Settings**

Fields	Usage Guidelines
General	
Create username from email address	Select this option if you want the guest username to be formed from the guest’s e-mail address.
Create username from 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.

Table A-58 **Guest Username Policy Settings (continued)**

Fields	Usage Guidelines
Minimum Username Length	Enter the minimum number of characters required for usernames. If the guest usernames formed by the e-mail 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 <i>Firstname Lastname</i>, the first username would be <i>lastname</i> and the second username would be <i>lastname1</i>. Similarly, if the Minimum Username length is set to eleven, then the two usernames would be generated as <i>lastname01</i> and <i>lastname02</i>.
Random	
Username may include the alphabetic characters	Enter all allowable uppercase and lowercase letters from A-Z.
Minimum number to include	Enter the minimum number of required alphabetic characters. Random username length is determined by combining this value with that of the numeric and special character minimum values. The length of the username defines the total number of unique names that can be created. For example, if you need to create 10,000 users, you cannot create enough unique values with usernames of only two characters in length.
Username may include the numeric characters	Enter all allowable numeric characters from 0-9.
Minimum number to include	Enter the minimum number of required numeric characters. Random username length is determined by combining this value with that of the alphabetic and special character minimum values.
Username may include the special characters	Enter any of the following special characters: \$ () < > ~ ` / * - _ @
Minimum number to include	Enter the minimum number of required special characters. Random username length is determined by combining this value with that of the alphabetic and numeric character minimum values.



Policy User Interface Reference

This chapter is a reference for the Cisco Identity Services Engine (ISE) Admin Portal elements, and contains the following Policy related sections:

- [Authentication, page B-1](#)
- [Authorization Policy Settings, page B-5](#)
- [Endpoint Profiling Policies Settings, page B-5](#)
- [Dictionaries, page B-8](#)
- [Conditions, page B-9](#)
- [Results, page B-18](#)

Authentication

This section contains the following topics:

- [Simple Authentication Policy Configuration Settings, page B-1](#)
- [Rule-Based Authentication Policy Configuration Settings, page B-2](#)

Simple Authentication Policy Configuration Settings

The following table describes the fields in the simple authentication policy page, which allows you to configure simple authentication policies. The navigation path for this page is: Policy > Authentication > Simple.

Table B-1 **Simple Authentication Policy Configuration Settings**

Fields	Usage Guidelines
Network Access Service	Choose an allowed protocol that you have already created.

Table B-1 Simple Authentication Policy Configuration Settings (continued)

Fields	Usage Guidelines
Identity Source	Choose the identity source that you want to use for authentication. You can also choose an identity source sequence if you have configured it. See the “Creating Identity Source Sequences” section on page 14-38 for information on how to configure identity source sequences.
Options	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.

Related Topics

- [Configuring a Simple Authentication Policy](#), page 19-21
- See the [“Creating Identity Source Sequences”](#) section on page 14-38 for information on how to configure identity source sequences.

Rule-Based Authentication Policy Configuration Settings

The following table describes the fields in the rule-based authentication policy page, which allows you to configure rule-based authentication policies. The navigation path for this page is: Policy > Authentication > Rule-Based.

Table B-2 Rule-Based Authentication Policy Configuration Settings

Fields	Usage Guidelines
Status	Choose the status of this policy. It 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 view the results of this policy condition in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. 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.
Standard Rule	Enter a name for this policy and select condition and allowed protocol.

Table B-2 **Rule-Based Authentication Policy Configuration Settings (continued)**

Fields	Usage Guidelines
Conditions	Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it. Click Select Existing Condition from Library or Create New Condition (Advanced Option) Select Existing Condition from Library—You can define an expression by selecting Cisco predefined conditions from the policy elements library. Create New Condition (Advanced Option)—You can define an expression by selecting attributes from various system or user-defined dictionaries.
Select Existing Condition from Library	You can do the following: 1. You can choose the predefined conditions that you would have defined for authentication in the policy elements, and then use an AND or OR operator to add multiple conditions. You cannot select certain predefined conditions that contain the following dictionaries or attributes: • Dictionary “Certificate”, with any attribute • Dictionary “Network Access”, with the following attributes: – Device IP Address – ISE Host Name – NetworkDeviceName – Protocol – UseCase In case such conditions are available, the first entry in the select box will be “Only relevant conditions are selectable”. 2. Click the Action icon to do the following in the subsequent steps: • Add Attribute/Value—You can add ad-hoc attribute/value pairs • Add Condition from Library—You can add Cisco predefined conditions • Duplicate—Create a copy of the selected condition • Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library • Delete—Delete the selected condition.

Table B-2 *Rule-Based Authentication Policy Configuration Settings (continued)*

Fields	Usage Guidelines
Create New Condition (Advance Option)	You can do the following: 1. You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions. 2. Click the Action icon to do the following in the subsequent steps: – Add Attribute/Value—You can add ad-hoc attribute/value pairs – Add Condition from Library—You can add Cisco predefined conditions – Duplicate—Create a copy of the selected condition – Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library – Delete—Delete the selected condition. Here, you can use the AND or OR operator
Select Network Access	Choose from allowed protocols or RADIUS server sequence.
	Click to define conditions for the identity source selection.
Identity Source Sequence	
Action Icon	Click the action icon in the default identity source row, and click Insert new row above .
Enter a store rule name 1	Enter a name for your identity source rule.
	Click the button to define the conditions based on which you want to choose the identity source.
Internal Users	Choose the identity source sequence or the identity source and the action that you want Cisco ISE to take.

Related Topics

[Configuring a Rule-Based Authentication Policy, page 19-22](#)

Authorization Policy Settings

The following table describes the fields in the authorization policy page, which allows you to configure authorization policies. The navigation path for this page is: Policy > Authorization.

Table B-3 *Authorization Policy Settings*

Fields	Usage Guidelines
Status	Choose one of the following to enforce the policies: • 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 view the results of this policy condition in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. 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.
Rule Name	Enter a name for the Rule Name.
Conditions (identity groups and other conditions)	Choose an identity group from the first drop-down. Choose a condition from the second drop-down. You can either select from the existing conditions or create a new condition.
Permissions	Choose an authorization profile from the Standard category.

Related Topics

[Configuring Authorization Policies, page 20-8](#)

Endpoint Profiling Policies Settings

The following table describes the fields in the Endpoint Policies page. The navigation path for this page is: Policy > Profiling > Profiling Policies.

Table B-4 *Endpoint Profiling Policies Settings*

Fields	Usage Guidelines
Name	Enter the name of the endpoint profiling policy that you want to create.
Description	Enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	By default, the Policy Enabled check box is checked to associate a matching profiling policy when you profile an endpoint. When unchecked, the endpoint profiling policy is excluded when you profile an endpoint.
Minimum Certainty Factor	Enter the minimum value that you want to associate with the profiling policy. The default value is 10.

Table B-4 **Endpoint Profiling Policies Settings (continued)**

Fields	Usage Guidelines
Exception Action	Choose an exception action, which you want to associate with the conditions when defining a rule in the profiling policy. The default is NONE. The exception actions are defined in the following location: Policy > Policy Elements > Results > Profiling > Exception Actions.
Network Scan (NMAP) Action	Choose a network scan action from the list, which you want to associate with the conditions when defining a rule in the profiling policy, if required. The default is NONE. The exception actions are defined in the following location: Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions.
Create an Identity Group for the policy	Check one of the following options to create an endpoint identity group: • Yes, create matching Identity Group • No, use existing Identity Group hierarchy
Yes, create matching Identity Group	Choose this option to use an existing profiling policy. This option creates a matching identity group for those endpoints and the identity group will be the child of the Profiled endpoint identity group when an endpoint profile matches an existing profiling policy. For example, the Xerox-Device endpoint identity group is created in the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile.
No, use existing Identity Group hierarchy	Check this check box to assign endpoints to the matching parent endpoint identity group using hierarchical construction of profiling policies and identity groups. 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 the Profiled endpoint identity group. For example, • If endpoints match the Cisco-IP-Phone profile, then they are grouped under the Cisco-IP-Phone endpoint identity group. • If endpoints match the Workstation profile, then they are grouped under the Workstation endpoint identity group. The Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.
Parent Policy	Choose a parent profiling policy that are defined in the system to which you want to associate the new endpoint profiling policy. You can choose a parent profiling policy from which you can inherit rules and conditions to its child.

Table B-4 **Endpoint Profiling Policies Settings (continued)**

Fields	Usage Guidelines
Associated CoA Type	Choose one of the following CoA types that you want to associate with the endpoint profiling policy: • No CoA • Port Bounce • Reauth • Global Settings that is applied from the profiler configuration set in Administration > System > Settings > Profiling
Rules	One or more rules that are defined in endpoint profiling policies determine the matching profiling policy for endpoints, which allows you to group endpoints according to their profiles. One or more profiling conditions from the policy elements library are used in rules for validating endpoint attributes and their values for the overall classification.
Conditions	Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it. Click Select Existing Condition from Library or Create New Condition (Advanced Option) Select Existing Condition from Library—You can define an expression by selecting Cisco predefined conditions from the policy elements library. Create New Condition (Advanced Option)—You can define an expression by selecting attributes from various system or user-defined dictionaries. You can associate one of the following with the profiling conditions: • An integer value for the certainty factor for each condition • Either an exception action or a network scan action for that condition Choose one of the following predefined settings to associate with the profiling condition: • Certainty Factor Increases—Enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification. • Take Exception Action—Triggers an exception action that is configured in the Exception Action field for this endpoint profiling policy. • Take Network Scan Action—Triggers a network scan action that is configured in the Network Scan (NMAP) Action field for this endpoint profiling policy.

Table B-4 *Endpoint Profiling Policies Settings (continued)*

Fields	Usage Guidelines
Select Existing Condition from Library	You can do the following: - You can choose Cisco predefined conditions that are available in the policy elements library, and then use an AND or OR operator to add multiple conditions. - Click the Action icon to do the following in the subsequent steps: - Add Attribute/Value—You can add ad-hoc attribute/value pairs - Add Condition from Library—You can add Cisco predefined conditions - Duplicate—Create a copy of the selected condition - Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library - Delete—Delete the selected condition.
Create New Condition (Advance Option)	You can do the following: - You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions. - Click the Action icon to do the following in the subsequent steps: - Add Attribute/Value—You can add ad-hoc attribute/value pairs - Add Condition from Library—You can add Cisco predefined conditions - Duplicate—Create a copy of the selected condition - Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library - Delete—Delete the selected condition. Here, you can use the AND or OR operator

Dictionaries

RADIUS Vendor Dictionary Attribute Settings

The following table describes the fields in the Dictionary page for RADIUS vendors, which allows you to configure dictionary attributes for the RADIUS vendors. The navigation path for this page is: Policy > Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors.

Table B-5 *RADIUS Vendor Dictionary Attribute Settings*

Fields	Usage Guidelines
Attribute Name	Enter the vendor specific attribute name for the selected RADIUS vendor.
Description	Enter an optional description for the vendor specific attribute.
Internal Name	Enter the name for the vendor specific attribute that refers to it internally in the database.

Table B-5 *RADIUS Vendor Dictionary Attribute Settings (continued)*

Fields	Usage Guidelines
Data Type	Choose one of the following data types for the vendor specific attribute: • STRING • OCTET_STRING • UNIT32 • UNIT64 • IPV4
Enable MAC option	Check this check box to enable the comparison of RADIUS attribute as MAC address. By default, for the RADIUS attribute calling-station-id this option is marked as enabled and you cannot disable it. For other dictionary attributes (of string types) within the RADIUS vendor dictionary, you can enable or disable this option. Once you enable this option, while setting the authentication and authorization conditions, you can define whether the comparison is clear string by selecting the Text option or whether it is MAC address by selecting the MAC address option.
Direction	Choose one of the options that applies to RADIUS messages:
ID	Enter the vendor attribute ID. The valid range is 0 to 255.
Allow Tagging	Check this check box.
Allow multiple instances of this attribute in a profile	Check this check box when you want multiple instances of this RADIUS vendor specific attribute in profiles.

Conditions

This section includes the following field setting tables:

- [Profiler Condition Settings, page B-9](#)
- [Posture Conditions Settings, page B-10](#)
- [Time and Date Condition Settings, page B-17](#)

Profiler Condition Settings

The following table describes the fields in the Profiler Condition page. The navigation path for this page is: Policy > Policy Elements > Conditions > Profiling.

Table B-6 *Profiler Condition Settings*

Fields	Usage Guidelines
Name	Name of the profiler condition.
Description	Description of the profiler condition.
Type	Choose any one of the predefined types.
Attribute Name	Choose an attribute on which to base the profiler condition.
Operator	Choose an operator.

Table B-6 *Profiler Condition Settings (continued)*

Fields	Usage Guidelines
Attribute Value	Enter the value for the attribute that you have chosen. For Attribute Names that contain pre-defined Attribute Values, this option displays a drop-down list with the pre-defined values, and you can choose a value.
System Type	Profiling conditions can be any one of the following types: • Cisco Provided—Profiling conditions that are provided by Cisco ISE when deployed are identified as Cisco Provided. You cannot edit or delete them from the system. • Administrator Created—Profiling conditions that you create as an administrator of Cisco ISE are identified as Administrator Created.

Related Topics

[Profiler Conditions, page 18-4](#)

Posture Conditions Settings

This section contains the following field setting tables:

- [File Condition Settings, page B-10](#)
- [Registry Condition Settings, page B-11](#)
- [Application Condition Settings, page B-12](#)
- [Service Conditions Settings, page B-13](#)
- [Posture Compound Condition Settings, page B-13](#)
- [Antivirus Compound Condition Settings, page B-13](#)
- [Antispyware Compound Condition Settings, page B-15](#)
- [Dictionary Simple Conditions Settings, page B-16](#)
- [Dictionary Compound Condition Settings, page B-16](#)

File Condition Settings

The following table describes the fields in the File Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > File Condition.

Table B-7 *File Condition Settings*

Fields	Usage Guidelines
Name	Enter the name of the file condition.
Description	Enter a description for the file condition.

Table B-7 File Condition Settings (continued)

Fields	Usage Guidelines
File Path	Choose one of the 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	Choose one of the 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	(Available only if you select FileDate as the File Type) Choose a file data type.
File Operator/Operator	The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately: FileExistence - Exists - DoesNotExist FileDate - EarlierThan - LaterThan - EqualTo FileVersion - EarlierThan - LaterThan - EqualTo
Date and Time	(Available only if you select File Date as the File Type) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.
File Version	(Available only if you have selected File Version as the File Type) Enter the version of the file to be checked.
Operating System	Select the operating system to which the file condition should be applied.

Registry Condition Settings

The following table describes the fields in the Registry Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Registry Condition.

Table B-8 Registry Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the registry condition.
Description	Enter a description for the registry condition.
Registry Type	Choose one of the predefined settings as the registry type.
Registry Root Key	Choose one of the predefined settings as the registry root key.
Sub Key	Enter the sub key without the backslash (“\”) to check the registry key in the path specified in the Registry Root Key. For example, SOFTWARE\Symantec\Norton AntiVirus\version will check the key in the following path: HKLM\SOFTWARE\Symantec\NortonAntiVirus\version
Value Name	(Available only if you select RegistryValue or RegistryValueDefault as the Registry Type) Enter the name of the registry key value to be checked for RegistryValue. This is the default field for RegistryValueDefault.
Value Data Type	(Available only if you select RegistryValue or RegistryValueDefault as the Registry Type) Choose one of the following settings: • Unspecified—Checks whether the registry key value exists or not. This option is available only for RegistryValue. • Number—Checks the specified number in the registry key value • String—Checks the string in the registry key value • Version—Checks the version in the registry key value
Value Operator	Choose the settings appropriately.
Value Data	(Available only if you select RegistryValue or RegistryValueDefault as the Registry Type) Enter the value of the registry key according to the data type you have selected in Value Data Type .
Operating System	Select the operating system to which the registry condition should be applied.

Application Condition Settings

The following table describes the fields in the Application Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Application Condition.

Table B-9 Application Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the application condition.
Description	Enter a description of the application condition.
Process Name	Enter the name of the application to be checked.
Application Operator	Choose the status to be checked.
Operating System	Select the operating system to which the application condition should be applied.

Service Conditions Settings

The following table describes the fields in the Service Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Service Condition.

Table B-10 **Service Conditions Settings**

Fields	Usage Guidelines
Name	Enter a name for the service condition.
Description	Enter a description of the service condition.
Service Name	Enter the name of the service to be checked.
Service Operator	Choose the status to be checked.
Operating System	Select the operating system to which the service condition should be applied.

Posture Compound Condition Settings

The following table describes the fields in the Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Compound Condition.

Table B-11 **Posture Compound Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the compound condition that you want to create.
Description	Enter the description of the compound condition that you want to create.
Operating System	Select one or more Windows operating systems. This allow you to associate Windows operating systems to which the condition is applied.
Parentheses ()	Click the parentheses to 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	Choose from a list of simple conditions of the following types: file, registry, application, and service conditions. You can also create simple conditions of file, registry, application and service conditions from the object selector. Click the quick picker (down arrow) on the Action button to create simple conditions of file, registry, application, and service conditions.

Antivirus Compound Condition Settings

The following table describes the fields in the AV Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > AV Compound Condition.

Table B-12 **Antivirus Compound Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the antivirus compound condition that you want to create.
Description	Enter the description of the antivirus compound condition that you want to create.
Operating System	Select an operating system 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 the Products for Selected Vendor table.
Check Type	Choose whether to check an installation or check the latest definition file update on the client.
Installation	Choose to check only the installation of an antivirus program on the client.
Definition	Choose to check only the latest definition file update of an antivirus product on the client.
Check against latest AV definition file version, if available. (Otherwise check against latest definition file date).	(Available only when you choose Definition check type) Choose 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, this option 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 (Enabled)	(Available only when you choose Definition check type) Choose 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	Define 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).
latest file date	Choose to check the antivirus definition file date on the client, which can be older by the number of days that you define in the 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.

Table B-12 **Antivirus Compound Condition Settings (continued)**

Fields	Usage Guidelines
current system date	Choose to checks the antivirus definition file date on the client, which can be older by the number of days that you define in the 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.
Products for Selected Vendor	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.

Antispyware Compound Condition Settings

The following table describes the fields in the AS Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > AS Compound Condition.

Table B-13 **Antispyware Compound Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the antispyware compound condition that you want to create.
Description	Enter the description of the antispyware compound condition that you want to create.
Operating System	Selecting an 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.
Vendor	Choose a vendor from the drop-down list. The selection of Vendor retrieves their antispyware products and versions, which are displayed in the Products for Selected Vendor table.
Check Type	Choose if you want to choose a type whether to check an installation, or check the latest definition file update on the client.
Installation	Choose if you want to check only the installation of an antispyware program on the client.
Definition	Choose if you want to check only the latest definition file update of an antispyware product on the client.
Allow virus definition file to be (Enabled)	Check this check box when you are 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 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	Define 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).

Table B-13 Antispyware Compound Condition Settings (continued)

Fields	Usage Guidelines
The current system date	Choose to check the antispyware definition file date on the client, which can be older by the number of days that you define in the 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	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.

Dictionary Simple Conditions Settings

The following table describes the fields in the Dictionary Simple Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Dictionary Simple Condition.

Table B-14 Dictionary Simple Condition Settings

Fields	Usage Guideline
Name	Enter the name of the dictionary simple condition that you want to create.
Description	Enter the description of the dictionary simple condition that you want to create.
Attribute	Choose an attribute from the dictionary.
Operator	Choose an operator to associate a value to the attribute that you have selected.
Value	Enter a value that you want to associate to the dictionary attribute, or choose a predefined value from the drop-down list.

Dictionary Compound Condition Settings

The following table describes the fields in the Dictionary Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Dictionary Compound Condition.

Table B-15 Dictionary Compound Condition Settings

Fields	Usage Guidelines
Name	Enter the name of the dictionary compound condition that you want to create.
Description	Enter the description of the dictionary compound condition that you want to create.
Select Existing Condition from Library	Define an expression by selecting pre-defined conditions from the policy elements library or add ad-hoc attribute/value pairs to your expression in the subsequent steps.
Condition Name	Choose dictionary simple conditions that you have already created from the policy elements library.
Expression	The Expression is updated based on your selection from the Condition Name drop-down list.

Table B-15 Dictionary Compound Condition Settings (continued)

Fields	Usage Guidelines
AND or OR operator	Choose an AND, or an OR operator to logically combine dictionary simple conditions, which can be added from the library. Click the Action icon to do the following: - Add Attribute/Value - Add Condition from Library - Delete
Create New Condition (Advance Option)	Select attributes from various system or user-defined dictionaries. You can also add predefined conditions from the policy elements library in the subsequent steps.
Condition Name	Choose a dictionary simple condition that you have already created.
Expression	From the Expression drop-down list, you can create a dictionary simple condition.
Operator	Choose an operator to associate a value to an attribute.
Value	Enter a value that you want to associate to the dictionary attribute, or choose a value from the drop-down list.

Related Topics

[Creating Endpoint Profiling Policies, page 21-22](#)

Time and Date Condition Settings

The following table describes the fields in the Time and Date Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Common > Time and Date.

Table B-16 Time and Date Condition Settings

Fields	Usage Guidelines
Condition Name	Enter the name of the time and date condition.
Description	Enter a description of the time and date condition.
Standard Settings	
All Day	(Default) Set for the entire day.
Specific Hours	Configure hours, minutes, and AM/PM to set a to-and-from time range.
Every Day	(Default) Set for every day.
Specific Days	Configure one or more specific days of the week.
No Start and End Dates	(Default) Set with no start or end date.
Specific Date Range	Configure the month, day, and year to set a to-and-from date range.
Specific Date	Configure a specific month, day, and year.
Exceptions	
Time Range	Configure the hours, minutes, and AM/PM to set a to-and-from time range.

Table B-16 *Time and Date Condition Settings (continued)*

Fields	Usage Guidelines
Week Days	Configure one or more specific days of the week.
Date Range	Choose on the following 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.

Related Topics

[Creating Time and Date Conditions, page 18-8](#)

Results

This section contains the following topics:

- [Allowed Protocols Services Settings, page B-19](#)
- [PAC Options, page B-22](#)
- [Authorization Profile Settings, page B-23](#)
- [Profiling Exception Action Settings, page B-25](#)
- [File Remediation, page B-26](#)
- [Link Remediation, page B-26](#)
- [Antivirus Remediation, page B-26](#)
- [Antispyware Remediation, page B-27](#)
- [Launch Program Remediation, page B-27](#)
- [Windows Update Remediation, page B-28](#)
- [Windows Server Update Services Remediation, page B-29](#)
- [Client Posture Requirements, page B-30](#)

Allowed Protocols Services Settings

The following table describes the fields in the Allowed Protocols Services page, which allows you to configure the protocols to be used during authentication. The navigation path for this page is: Policy > Policy Elements > Results > Authentication > Allowed Protocols.

Table B-17 **Allowed Protocols Services Settings**

Fields	Usage Guidelines
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	Check this check box to 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. This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol.
Allow CHAP	Check this check box to check the Detect CHAP as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup request. If you enable this option, ISE will allow MAB on non-Cisco devices. 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	Check this check box to enable MS-CHAPv1.
Allow MS-CHAPv2	Check this check box to enable MS-CHAPv2.
Allow EAP-MD5	Check this check box to enable 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.
Allow EAP-TLS	Check this check box to enable 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 8, “Managing Certificates” for more information on certificates.
Allow LEAP	Check this check box to enable Lightweight Extensible Authentication Protocol (LEAP) authentication.

Table B-17 *Allowed Protocols Services Settings (continued)*

Fields	Usage Guidelines
Allow PEAP	Check this check box to enable 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. • Allow PEAPv0 only for legacy clients—Check this check box to allow PEAP supplicants to negotiate using PEAPv0. Some legacy clients do not conform to the PEAPv1 protocol standards. To ensure that such EAP conversations are not dropped, check this check box.
Allow EAP-FAST	Check this check box to enable 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. See PAC Options, page B-22 for using protected access credentials with EAP-FAST. Refer to Guidelines for Using EAP-FAST as Authentication Protocol, page 19-11 for information on EAP chaining. 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 PACs¹ 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.

Related Topics

[Defining Allowed Protocols for Network Access, page 19-14](#)

PAC Options

The following table describes the fields after you select Use PACs in the Allowed Protocols Services List page. The navigation path for this page is: Policy > Policy Elements > Results > Authentication > Allowed Protocols.

Table B-18 **PAC Options**

Fields	Usage Guidelines
Use PAC	• Tunnel PAC Time To Live—The Time to Live (TTL) 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. 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. Cisco ISE only supports Active Directory as an external identity source for machine authentication. After these details are correctly verified, no further authentication is performed. 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). • 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.

Related Topics

[Defining Allowed Protocols for Network Access, page 19-14](#)

Authorization Profile Settings

The following table describes the fields in the Standard Authorization Profiles page. The navigation path for this page is: Policy > Policy Elements > Results > Authorization > Authorization Profiles.

Table B-19 **Authorization Profile settings**

Fields	Usage Guidelines
Name	Enter a name that identifies the new authorization profile.
Description	Enter a description of the authorization profile.
Access Type	Choose the access type options (ACCESS_ACCEPT or ACCESS_REJECT).
Service Template	Check the check box to enable Cisco ISE to support sessions connecting from SAnet capable devices. ISE implements service templates as authorization profiles that contain a special flag that marks them as “Service Template” compatible. This way, the service template, which is also an authorization profile, can be used in a single policy to support connection with SAnet as well as non-SAnet devices.
Common Tasks	
DACL Name	Check the check box and choose existing downloadable ACL options available (for example, Cisco ISE provides two default values in the drop-down list: PERMIT_ALL_TRAFFIC or DENY_ALL_TRAFFIC). The list will include all current DACLs in the local database.
VLAN	Check 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 <i>Tunnel-Private-Group-ID:VLANnumber</i>. Note If you do not select 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 reflects the following value: Tunnel-Private-Group-ID = 1:123.
Voice Domain Permission	Check 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	Check 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 ac1119, this is reflected in the Attributes Details pane as: cisco-av-pair = url-redirect-acl = ac1119. The Attributes Details pane also displays: cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&action=cpp.

Table B-19 Authorization Profile settings (continued)

Fields	Usage Guidelines
Centralized Web Authentication	Check 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 Default or Manual as the redirect option. 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. Check the Static IP/Host Name check box to specify an exact IP address or hostname to which you want the user to be redirected to. If this check box is not checked, the user will be redirected to the FQDN of the policy service node that received this request.
Web Redirection (CWA, RWA, MDM, NSP, CPP)	
Auto SmartPort	Check 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	Check 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	Check 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 choosing to use either the default (a value of 0) or RADIUS-Request (a value of 1). Setting this to the RADIUS-Request value maintains connectivity during the reauthentication process.
MACSec Policy	Check 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: 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	Check the check box to enable Network Edge Access Topology (NEAT), a feature that extends identity recognition between networks. Checking this check box displays the following value in the Attributes Details pane: cisco-av-pair = device-traffic-class=switch.
Web Authentication (Local Web Auth)	Check 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)	Check 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	Check the check box to enable an Adaptive Security Appliances (ASA) VPN group policy. From the Attribute list, choose a value to configure this setting.
Advanced Attributes Settings	
Dictionaries	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.

Table B-19 Authorization Profile settings (continued)

Fields	Usage Guidelines
Attribute Values	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.

Related Topics

[Configuring Permissions for New Standard Authorization Profiles, page 20-10](#)

Profiling Exception Action Settings

The following table describes the fields in the New Profiler Exception Action page. The navigation path for this page is: Policy > Policy Elements > Results > Profiling > Exception Actions.

Table B-20 Creating an Exception Action

Fields	Usage Guidelines
Name	Enter the name of the exception action that you want to create.
Description	Enter the description of the exception action that you want to create.
CoA Action to enforce CoA	Check the CoA Action check box to enforce CoA. When you associate an exception action in the endpoint profiling policy and enforce a CoA, you must configure CoA globally in Cisco ISE that can be done in the following location: Administration > System > Settings > Profiling. For information, see Setting up COA, SNMP RO Community and Endpoint Attribute Filter, page 21-15.
Policy Assignment	Click the Policy Assignment drop-down list that displays endpoint profiling policies that are configured in Cisco ISE, and choose the profiling policy against which the endpoint will be profiled when the exception action is triggered, regardless of its matched value.
System Type	Exception Actions can be any one of the following types: - Cisco Provided—Includes AuthorizationChange, EndpointDelete, and FirstTimeProfile - Administrator Created—Includes that are created by you as an administrator of Cisco ISE.

Related Topics

[Creating Exception Actions, page 21-30](#)

File Remediation

The following table describes the fields in the File Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > File Remediation.

Table B-21 *File Remediation*

Fields	Usage Guidelines
File Remediation Name	Enter a name for the file remediation. Once created and saved, you cannot edit the name of the file remediation.
File Remediation Description	Enter a description for the file remediation.
Version	Enter the file version.
File to upload	Click Browse to locate the name of the file to be uploaded to the Cisco ISE server. This is the file that will be downloaded to the client when the file remediation action is triggered.

Link Remediation

The following table describes the fields in the Link Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Link Remediation.

Table B-22 *Link Remediation*

Fields	Usage Guidelines
Link Remediation Name	Enter a name for link remediation.
Link Remediation Description	Enter a description for the link remediation.
Remediation Type	Choose one of the following: Automatic—When selected, you should enter values for the Interval and Retry Count. Manual—When selected, Retry Count and Interval fields are not editable.
Retry Count	Enter the number of attempts that clients can try to remediate from the link.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate from the link after previous attempts.
URL	Enter a valid URL that leads to a remediation page or resource.

Antivirus Remediation

The following table describes the fields in the AV Remediation page. The navigation path is Policy > Policy Elements > Results > Posture > Remediation Actions > AV Remediation.

Table B-23 *Antivirus Remediation*

Fields	Usage Guidelines
Name	Enter a name for the antivirus remediation.
Description	Enter a description for the antivirus remediation.

Table B-23 **Antivirus Remediation (continued)**

Fields	Usage Guidelines
Remediation Type	Choose one of the following: • Automatic—When selected, you should enter values for the Interval and Retry Count. • Manual—When selected, Retry Count and Interval fields are not editable.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to update an antivirus definition.
Operating System	Choose one of the following: • Windows • Macintosh—when selected Remediation Type, Interval, and Retry Count fields are not editable
AV Vendor Name	Choose the antivirus vendor.

Antispyware Remediation

The following table describes the fields in the AS Remediation page. The navigation path is Policy > Policy Elements > Results > Posture > Remediation Actions > AS Remediation.

Table B-24 **Antispyware Remediation**

Fields	Usage Guidelines
Name	Enter a name for the antispyware remediation.
Description	Enter a description for the antispyware remediation.
Remediation Type	Choose one of the following: • Automatic—When selected, you should enter values for the Interval and Retry Count. • Manual—When selected, Retry Count and Interval fields are not editable.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to update an antispyware definition.
Operating System	Choose one of the following: • Windows • Macintosh—when selected, Remediation Type, Interval, and Retry Count fields are not editable
AS Vendor Name	Choose the antispyware vendor.

Launch Program Remediation

The following table describes the fields in the Launch Program Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Launch Program Remediation.

Table B-25 **Launch Program Remediation**

Fields	Usage Guidelines
Name	Enter a name for the launch program remediation.
Description	Enter a description for the launch program remediation that you want to create.
Remediation Type	Choose one of the following: • Automatic—When selected, you should enter the Retry Count and Interval options. • Manual—When selected, Interval and Retry Count fields are not editable.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to launch required programs.
Program Installation Path	From the drop-down list, choose the path where the remediation program has to be installed. • 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 of Windows system
Program Executable	Enter the name of the remediation program executable, or an installation file.
Program Parameters	Enter required parameters for the remediation programs.
Existing Programs	Existing Programs table displays the installation paths, name of the remediation programs, and parameters if any. • Click Add to add remediation programs to the Existing Programs list. • Click the delete icon to remove the remediation programs from the list.

Windows Update Remediation

The following table describes the fields in the Windows Update Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Windows Update Remediation.

Table B-26 **Windows Update Remediation**

Fields	Usage Guidelines
Name	Enter a name for the Windows update remediation.
Description	Enter a description for the Windows update remediation.
Remediation Type	Choose one of the following: • Automatic—When selected, you should enter the Retry Count and Interval options. • Manual—When selected, Interval and Retry Count fields are not editable.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.

Table B-26 Windows Update Remediation (continued)

Fields	Usage Guidelines
Retry Count	Enter the number of attempts that Windows clients can try for Windows updates.
Windows Update Setting	Choose from the following: - Do not change setting—The Windows Automatic Updates client configuration does not change during or after Windows update remediation. - Notify to download and install—Windows only notifies clients, but does not automatically download, or install them. - Automatically download and notify to install—Windows downloads updates for clients, and notifies clients to install Windows updates. - Automatically download and install—Windows automatically downloads, and installs Windows updates. This is the highly recommended setting for Windows clients.
Override User's Windows Update setting with administrator's	Check this check box to enforce the administrator-specified setting for Windows Automatic Updates on all the clients during, and after Windows update remediation. If unchecked, the setting enforces the following: - The 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.

Windows Server Update Services Remediation

The following table describes the fields in the Windows Update Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Windows Update Remediation.

Table B-27 WSUS Remediation

Fields	Usage Guidelines
Name	Enter a name for the WSUS remediation.
Description	Enter a description for the WSUS remediation.
Remediation Type	Choose from the following: Automatic—The NAC Agents automatically updates Windows clients with the latest WSUS updates. Manual—If selected, the Interval and Retry Count fields are not 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)	Enter 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	Enter the number of attempts that the NAC Agents and web Agents retry to update Windows clients with WSUS updates.

Table B-27 WSUS Remediation (continued)

Fields	Usage Guidelines
Validate Windows updates using	Choose from the following: • Cisco Rules—If you choose this option, you can select custom or preconfigured rules as conditions in the posture requirement • Severity Level—If you choose this option, you can select custom or preconfigured rules as conditions in the posture requirement, but they are not used. 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	Choose the severity level: • 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 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.
Update to latest OS Service Pack	Check this check box to allow WSUS remediation install 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.
Windows Updates Installation Source	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	Allows you to display the installation wizard on the client during WSUS updates: • Show UI—Displays the Windows Update Installation Wizard progress on Windows clients. Users must have Administrator privileges on clients to view the installation wizard during WSUS updates. • No UI—Hides the Windows Update Installation Wizard progress on Windows clients.

Client Posture Requirements

The following table describes the fields in the Posture Requirements page. The navigation path is: Policy > Policy Elements > Results > Posture > Requirements.

Table B-28 **Posture Requirement**

Fields	Usage Guidelines
Name	Enter a name for the requirement.
Operating Systems	Choose an operating system. Click plus [+] to associate more than one operating system to the policy. Click minus [-] to remove the operating system from the policy.
Conditions	Choose a Condition from the list. You can also create any user defined condition by clicking the Action Icon and associate it with the requirement. You cannot edit the associated parent operating system while creating user defined conditions. The pr_WSUSRule is a dummy compound condition, which is used in a posture requirement with an associated Windows Server Update Services (WSUS) remediation. 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. The pr_WSUSRule cannot be viewed in the Compound conditions list page. You can only select the pr_WSUSRule from the Conditions widget.
Remediation Actions	Choose a Remediation from the list. You can also create a remediation action and associate it with the requirement. You 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 communicate to Agent users about the non compliance of clients with messages. The Message Text Only option informs Agent users about the noncompliance. It also provides optional instructions to the user to contact the Help desk for more information, or to remediate the client manually. In this scenario, the NAC Agent does not trigger any remediation action.



Operations User Interface Reference

This chapter is a reference for Cisco Identity Services Engine (ISE) user interface elements, and contains the settings for the following features:

- [Recent RADIUS Authentications, page C-1](#)
- [Diagnostic Tools, page C-4](#)

Recent RADIUS Authentications

The following table describes the fields on the Authentications page, which displays recent RADIUS authentications. The navigation path for this page is: Operations > Authentications > Show Live Authentication.

Table C-1 **Live Authentications**

Option	Usage Guidelines
Misconfigured Supplicants	Shows the number of times misconfigured supplicants were detected in last 24 hours. Note Do not consider supplicants that stopped responding, as misconfigured supplicants.
Misconfigured Network Devices	Shows the number of times misconfigured network devices were detected in last 24 hours.
RADIUS Drops	Shows the number of times the RADIUS requests were dropped in last 24 hours. Note The number of dropped RADIUS requests that this option displays does not include the drop counts corresponding to the RADIUS Accounting requests. You can view details corresponding to these RADIUS Accounting requests drops in the RADIUS Errors report. For more information on the RADIUS Errors report, see “Available Reports” section on page 26-6 .
Client Stopped Responding	Shows the number of times the client stopped responding in last 24 hours. Note Do not consider supplicants that stopped responding, as misconfigured supplicants.
Repeat Counter	Shows the number of time the authentication requests were repeated in last 24 hours, without any change in the context of identity, network devices, and authorization
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.

Table C-1 *Live Authentications (continued)*

Option	Usage Guidelines
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.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2), 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.

Related Topics

[Monitoring Live Authentications, page 25-13](#)

Show Live Sessions

The following table describes the fields on the live sessions page, which displays live authentication sessions. The navigation path for this page is: Operations > Authentications > Show Live Sessions.

Table C-2 *Live Sessions*

Field	Description
Reset Repeat Counts	Click to reset the Retry options for all the endpoints
Initiated	Shows the timestamp when the authentication session was initiated.
Updated	Shows the timestamp when the session was last updated due to any change, like a CoA action.
Session Status	Shows the current status of the endpoint device.
CoA Action	Use this to dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session.
Repeat Count	Shows the number of times the session has been retried

Table C-2 *Live Sessions (continued)*

Field	Description
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of the endpoint device.
IP Address	Shows the IP address of the endpoint device.
Endpoint Profile	Shows the endpoint profile for the device.
Posture Status	Shows the status of posture validation and details on the authentication.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service from which the log was generated.
Auth Method	Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2), 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.
NAS IP Address	Shows IP address of the network devices.
Device Port	Shows the connected port to the network device.

Live Authentication Details

The following table describes the fields on the live authentication details drill-down page. The navigation path for this page is: Operations > Authentications > Show Live Authentication > Details Icon. This page also displays text that describes the link between session entry and passed authentication entry.

Table C-3 *Live Authentication Drill-down*

Field	Description
Event	Shows the number of successful passed authentication events.
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.
Endpoint Profile	Shows the endpoint profile for the device.
Authorization Profiles	Shows an authorization profile that was used for authentication.
AuthorizationPolicyMatchedRule	Shows the authorization policy rule used for authentication.
ISEPolicySetName	Shows the ISE policy set name.
IdentitySelectionMatchedRule	Shows the identity selection rule used for authentication.
Source Timestamp	Shows the time stamp of the source.
Received Timestamp	Shows the time when the authorization event is received.
Policy Server	Shows the policy server name.
Failure Reason	Shows the reason for failed authentications.

Diagnostic Tools

This section contains the following topics:

- [RADIUS Authentication Troubleshooting Settings, page C-4](#)
- [Execute Network Device Command Settings, page C-5](#)
- [Evaluate Configuration Validator Settings, page C-5](#)
- [Posture Troubleshooting Settings, page C-6](#)
- [TCP Dump Settings, page C-6](#)
- [SXP-IP Mappings, page C-7](#)
- [IP User SGT, page C-8](#)
- [Device SGT Settings, page C-9](#)
- [Progress Details Settings, page C-10](#)
- [Results Summary, page C-10](#)

RADIUS Authentication Troubleshooting Settings

The following table describes the fields on the RADIUS authentication troubleshooting page which allow you to identify and resolve RADIUS authentication problems. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting.

Table C-4 *RADIUS Authentication Troubleshooting Settings*

Option	Usage Guidelines
Username	Enter the username of the user whose authentication you want to troubleshoot.
MAC Address	Enter the MAC address of the device that you want to troubleshoot.
Audit Session ID	Enter the audit session ID that you want to troubleshoot.
NAS IP	Enter the NAS IP address.
NAS Port	Enter the NAS port number.
Authentication Status	Choose the status of your RADIUS authentication.
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. The RADIUS authentication records that are created during this time range are used.
Start Date-Time	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 <i>mm/dd/yyyy</i> format and time in the <i>hh:mm</i> format.
End Date-Time	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 <i>mm/dd/yyyy</i> format and time in the <i>hh:mm</i> 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.

Related Topics[Troubleshooting Unexpected RADIUS Authentication Results, page 25-18](#)

Execute Network Device Command Settings

The following table describes the fields on the Execute Network Device Command page, which you use to execute the **show** command on a network device. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > General Tools > Execute Network Device Command.

Table C-5 *Execute Network Device Command Settings*

Option	Usage Guidelines
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.

Related Topics[Executing IOS Show Commands to Check Configuration, page 25-19](#)

Evaluate Configuration Validator Settings

The following table describes the fields on the Evaluate Configuration Validator page, which you use to evaluate the configuration of a network device and identify any configuration problems. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator.

Table C-6 *Evaluate Configuration Validator Settings*

Option	Usage Guidelines
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	Check this check box to compare the web authentication configuration.
Profiler Configuration	Check 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 available options.

Related Topics

[Troubleshooting Network Device Configuration Issues, page 25-20](#)

Posture Troubleshooting Settings

The following table describes the fields on the Posture troubleshooting page, which you use to find and resolve posture problems on the network. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > General Tools > Posture Troubleshooting.

Table C-7 *Posture Troubleshooting Settings*

Option	Usage Guidelines
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
Posture Status	Select the authentication status to filter on:
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. The RADIUS authentication records that are created during this time range are used.
Start Date-Time:	(Available only when 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 <i>mm/dd/yyyy</i> format and time in the <i>hh:mm</i> format.
End Date-Time:	(Available only when 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 <i>mm/dd/yyyy</i> format and time in the <i>hh:mm</i> 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

Related Topics

[Troubleshooting Endpoint Posture Failure, page 25-20](#)

TCP Dump Settings

The following table describes the fields on the **tcpdump** utility page, which you use to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump.

Table C-8 **TCP Dump Settings**

Option	Usage Guidelines
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. Note Inline Posture Nodes are not supported.
Network Interface	Choose the network interface to monitor from the drop-down list. Note You must configure all network interface cards (NICs) with an IPv4 or IPv6 address so that they are displayed in the Cisco ISE Admin portal.
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.
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 <pre> File size: 3,744 bytes Format: Raw Packet Data Host Name: Positron Network Interface: GigabitEthernet 0 Promiscuous Mode: On </pre> - Download—Click to download the most recent dump file. - Delete—Click to delete the most recent dump file.

Related Topics

[Using TCP Dump to Monitor Network Traffic, page 25-21](#)

SXP-IP Mappings

The following table describes the fields on the SXP-IP mappings page, which you use to compare mappings between a device and its peers. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > SXP-IP Mappings.

Peer SXP Devices

Table C-9 Peer SXP Devices for SXP-IP Mappings

Option	Usage Guidelines
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.
Protocol	Choose the protocol. 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.

Related Topics

[Troubleshooting Connectivity Issues in an SGA-Enabled Network with SXP-IP Mappings, page 25-23](#)

IP User SGT

The following table describes the fields on the IP User SGT page, which you use to compare IP-SGT values on a device with an ISE assigned SGT. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > IP User SGT.

Table C-10 IP User SGT

Option	Usage Guidelines
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.

Table C-10 *IP User SGT (continued)*

Option	Usage Guidelines
User IP Address	Enter the IP address of the user whose records you want to troubleshoot.
SGT	Enter the user SGT value.

Related Topics

[Troubleshooting Connectivity Issues in an SGA-Enabled Network with IP-SGT Mappings, page 25-24](#)

Device SGT Settings

The following table describes the fields on the Device SGT page, which you use to compare the device SGT with the most recently assigned value. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > Security Group Access Tools > Device SGT.

Table C-11 *Device SGT Settings*

Option	Usage Guidelines
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. 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.

Related Topics

[Troubleshooting Connectivity Issues in an SGA-Enabled Network by Comparing Device SGT Mappings, page 25-24](#)

Progress Details Settings

The following table describes the fields on the Progress Details page, which is displayed when you click the **User Input Required** button in any of the diagnostic tools. This page displays detailed troubleshooting information. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > *Any Diagnostic Tool*.

Table C-12 *Progress Details Settings*

Option	Usage Guidelines
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. 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	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.

Results Summary

The following table describes the fields on the result summary page, which is displayed as a result when you use any diagnostic tool.

Table C-13 *RADIUS Authentication Troubleshooting Results Summary*

Option	Usage Guidelines
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.

Table C-13 *RADIUS Authentication Troubleshooting Results Summary*

Option	Usage Guidelines
Troubleshooting Summary	
<Summary>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. Any configuration errors are indicated by red text.



Sample Code for Sponsor and Guest Portal Customizations

Cisco ISE enables you to customize the guest notifications in the Sponsor portal and the look-and-feel of the Guest portal.

- [Sample Code for Custom Guest Notifications from Sponsor Portal, page D-1](#)
- [Sample HTML for Custom Pages for the Guest Portal, page D-3](#)

Sample Code for Custom Guest Notifications from Sponsor Portal

You can customize the templates used by sponsors to send guests their login credentials:

- [E-Mail Notification Template, page D-1](#)
- [SMS Text Message Notification Template, page D-2](#)
- [Print Notification Template, page D-3](#)

E-Mail Notification Template

The following is an example of the login information for the body of an e-mail 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 e-mail body, you can use special variables to provide the details for the created guest account. When using these variables, you must use all uppercase or all lowercase letters, and you cannot mix them. For example, the string for username can be either *\$USERNAME\$* or *\$username%*, but it cannot be *\$UserName\$*.

You can use these variables in the e-mail notification template:

- *\$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 e-mail 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 log in.
- \$TIMEPROFILE\$ = The name of the time profile assigned.

SMS Text Message Notification Template

In the text message, you can use special variables to provide the details for the created guest account. When using these variables, you must use all uppercase or all lowercase letters, and you cannot mix them. For example, the string for username can be either \$USERNAME\$ or \$username%, but it cannot be \$UserName\$.

You can use these variables in the SMS text message notification template:

- \$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 e-mail 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 log in.
- \$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.

Print Notification Template

In the printed copy, you can use special variables to provide the details for the created guest account. When using these variables, you must use all uppercase or all lowercase letters, and you cannot mix them. For example, the string for username can be either `$USERNAME$` or `$username%`, but it cannot be `$UserName$`.

You can use these variables in the print notification template:

- `$USERNAME$` = 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 e-mail 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 log in.
- `$TIMEPROFILE$` = The name of the time profile assigned.

Sample HTML for Custom Pages for the Guest Portal

You can use these examples to create HTML pages for the guest portal pages. When you create custom portals by uploading your own HTML pages, the details policy, language templates, and portal themes do not apply. So, if these features are important to you, you will need to write the HTML code to deliver similar functionality, or use the standard portal pages instead.

When you upload custom html files, these changes apply only to the guest portal. The other portals use the settings defined in the portal theme (see [“Customizing the Web Portal Images and Color Scheme” section on page 15-5](#)). To better synchronize the look-and-feel amongst the portals, upload your custom logos and banners to the portal theme too.

These HTML examples reference a directory structure for a portal named demo2:

- [Fields Used on Custom HTML Pages, page D-4](#)

- [Login Page Sample HTML, page D-5](#)
- [Detect Cookies at Login Sample HTML, page D-8](#)
- [Successful Guest Login Page Sample HTML, page D-9](#)
- [Error Page Sample HTML, page D-10](#)
- [Acceptable Use Policy \(AUP\) Page Sample HTML, page D-11](#)
- [Change Password Page Sample HTML, page D-13](#)
- [Self-Registration Page Sample HTML, page D-14](#)
- [Self-Registration Result Page Sample HTML, page D-17](#)
- [Device Registration Page Sample HTML, page D-18](#)
- [Sample style.css for Custom Guest Portal HTML Pages, page D-19](#)

Fields Used on Custom HTML Pages

You must define some of these fields in the Cisco ISE Admin UI, including:

- Guest password policy: Choose **Administration > Web Portal Management > Settings > Guest > Password Policy**.
- Guest username policy: Choose **Administration > Web Portal Management > Settings > Guest > Username Policy**.

Table D-1 Custom HTML Pages Fields

Field	ID Name	Restrictions
Login Page		
Username	guestUser.name	1000 alphanumeric, and special characters. Specified in Cisco ISE Admin.
Password	guestUser.password	1000 characters, alphanumeric. Specified in Cisco ISE Admin.
Self Registration Page		
First name	guestUser.firstName	100 alphanumeric, and special characters
Last name	guestUser.lastName	100 alphanumeric, and special characters
Email address	guestUser.emailAddress	100 alphanumeric, and special characters
Phone number	guestUser.phoneNumber	1000 alphanumeric, and special characters
Company	guestUser.company	1000 alphanumeric, and special characters

Table D-1 Custom HTML Pages Fields

Field	ID Name	Restrictions
Optional data 1-5	guestUser.optionaData 1 guestUser.optionaData 2 guestUser.optionaData 3 guestUser.optionaData 4 guestUser.optionaData 5	4000 alphanumeric, and special characters
TimeZone	guestUser.timezone	drop-down box
Change Password Page		
Username	username	1000 alphanumeric, and special characters. Specified in Cisco ISE Admin.
Old password	currentpassword	1000 alphanumeric, and special characters. Specified in Cisco ISE Admin.
New password	newpassword	1000 alphanumeric, and special characters. Defined in Cisco ISE Admin.
Confirm password	confirmpassword	1000 alphanumeric, and special characters. Specified in Cisco ISE Admin.
AUP Page		
Accept terms and conditions	guestUser.acceptUsePolicy	check box
Device Registration Page		
Device ID	registeredMac	6-pair alphanumeric character set

Login Page Sample HTML

```

<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">&nbsp;  </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%"></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">&nbsp;  </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">&nbsp;  </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">&nbsp;</td>
        <td align="left">&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</td>
        </tr>
        <tr>
        <td align="left" valign="middle">&nbsp;</td>
        <td align="left"><a href="javascript:doChangePassword();" class="link"
>Change Password</a>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</td>
        <a href="javascript:doSelf();" class="link">SelfService</a>&nbsp;&nbsp;&nbsp;&nbsp;&nbsp;</td>
        <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>
```

Detect Cookies at Login Sample HTML

If users have cookies disabled in their web browser, Cisco ISE redirects them to the default guest portal when logging in, which bypasses your customized portal. You can prevent this redirect by adding code to detect whether cookies are disabled. If they are disabled, an error message displays instructing users to enable cookies and the login button is disabled.

```
<script>
```

```
var UI_METHODS = UI_METHODS || {};
```

```
UI_METHODS.manageCookies = {
```

```
    createCookie : function ( name, value, days ) {
```

```
        var expires = "";
```

```
        if (days) {
```

```
            var date = new Date();
```

```
            date.setTime( date.getTime() + (days * 24 * 60 * 60 * 1000) );
```

```
            expires = "; expires=" + date.toGMTString();
```

```
        }
```

```
        document.cookie = name + "=" + value + expires + "; path=/";
```

```
        return true;
```

```
    },
```

```
    readCookie : function ( name ) {
```

```
        var nameEQ = name + "=";
```

```
        var ca = document.cookie.split(';');
```

```
        for (var i=0;i < ca.length;i++) {
```

```
            var c = ca[i];
```

```
            while (c.charAt(0)==' ') c = c.substring(1, c.length);
```

```
            if (c.indexOf(nameEQ) == 0) return c.substring(nameEQ.length, c.length);
```

```
        }
```

```
        return null;
```

```
    },
```

```
    eraseCookie : function ( name ) {
```

```
        UI_METHODS.manageCookies.createCookie(name, '', -1);
```

```
        return true;
```

```
    }
```

```
};
```

```
var are_cookies_enabled = function ( ) {
```

```
    // Cannot rely on this: Some browsers (like IE) will return "true" here even if
```

```
all cookies are blocked!
```

```
    // var cookieEnabled = (navigator.cookieEnabled) ? true : false;
```

```
    var areCookiesEnabled = false,
```

```
    cookieName = "testcookie";
```

```
    UI_METHODS.manageCookies.createCookie( cookieName, 1, 365 );
```

```
    areCookiesEnabled = ( UI_METHODS.manageCookies.readCookie( cookieName ) != null )
```

```
?
```

```
        UI_METHODS.manageCookies.eraseCookie( cookieName ) :
```

```
areCookiesEnabled;
```

```

        return ( areCookiesEnabled );
    };
</script>

<script type="text/javascript">
    document.getElementById('loginsubmit').disabled=false;
    if ( !are_cookies_enabled() ) {
        document.getElementById('cookieMsg')['style']['display'] = 'block';
        document.getElementById('loginsubmit').disabled=true;
    }
</script>

```

Successful Guest Login Page Sample HTML

[illegible]

```

        </tr>
      </form>
    </table></td>
  </tr>
  <tr>
    <td align="left">&nbsp;</td>
  </tr>
  <tr>
    <td align="left">&nbsp;</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>

```

Error Page Sample HTML

```

<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">&nbsp;</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%"></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>

```

Acceptable Use Policy (AUP) Page Sample HTML

Cisco Identity Services Engine User Guide, Release 1.2

```

<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 else's account, sending unsolicited bulk e-mail, collection of other
  people'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 system's website and will
  be effective as to existing users 30 days after posting same.
  </br></br></td>
</tr>
<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">&nbsp;</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">&nbsp;</td>
</tr>
</tr>
</table>
</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 Page Sample HTML

```

<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">&nbsp;</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%"></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">&nbsp;</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"
cellpadding="0" cellspacing="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">&nbsp;</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 Page Sample HTML

```

<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"></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>&nbsp;</td>
    </tr>
    <tr>
        <td align="left" class="heading2">Self Registration</td>
    </tr>
    <tr>
        <td align="left">&nbsp;</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>
            </form>
        </td>
    </tr>
</table>

```

```

        <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">&nbsp;</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">&nbsp;</td>
</tr>
<tr>
    <td align="left">&nbsp;</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>

```

Self-Registration Result Page Sample HTML

```

<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"></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>&nbsp;</td>
      </tr>
      <tr>
        <td align="left" class="headding2"> Self Registration
created user: fsdf</td><!--END HEADER HERE -->
      </tr>
      <tr>
        <td align="left">&nbsp;</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">&nbsp;</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">&nbsp;</td>
      </tr>
    </table>
  </tr>
  <tr>
    <td align="left">&nbsp;</td>
  </tr>

```

```

        </tr>
        <tr>
            <td align="left">&nbsp;</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>

```

Device Registration Page Sample HTML

```

<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"></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>&nbsp;</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">&nbsp;</td>
    </tr>

    <tr>
        <td align="left">
</td>
    </tr>
    <tr>
        <td align="left">&nbsp;</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>

```

Sample style.css for Custom Guest Portal HTML Pages

```

@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; }

```




Network Access Flows

This appendix describes the authentication flows in Cisco Identity Services Engine (Cisco ISE) by using RADIUS-based Extensible Authentication Protocol (EAP) and non-EAP protocols.

Password-Based Authentication

Authentication verifies user information to confirm user identity. Traditional authentication uses a name and a fixed password. This is the most popular, simplest, and least-expensive method of authentication. 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.

Secure Authentication Using Encrypted Passwords and Cryptographic Techniques

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 such as in the following examples:

- In the communication between an end-user client that dials up over a phone line
- On an ISDN line that terminates at a network access server
- Over a Telnet session between an end-user client and the hosting device

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.

Authentication Methods and Authorization Privileges

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.

RADIUS Protocol Support in Cisco ISE

RADIUS is a client/server protocol through which remote-access servers communicate with a central server to authenticate dial-in users and 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 the [“Dictionaries and Dictionary Attributes” section on page 10-1](#) 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 for Users

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 E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)

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)

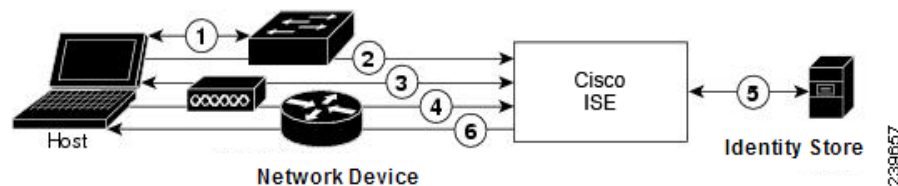
RADIUS-Based Non-EAP Authentication Flow

This section describes 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 request (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. A RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

Figure E-1 shows a RADIUS-based authentication without EAP.

Figure E-1 RADIUS-Based Authentication Without EAP



This section describes the non-EAP protocols supported by Cisco ISE and contains the following topics:

- [Password Authentication Protocol, page E-3](#)
- [Challenge Handshake Authentication Protocol, page E-4](#)
- [Microsoft Challenge Handshake Authentication Protocol Version 1, page E-4](#)
- [Microsoft Challenge Handshake Authentication Protocol Version 2, page E-5](#)

Password Authentication Protocol

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. PAP is not a strong authentication method because it offers little protection from repeated trial-and-error attacks.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based Protocols Without EAP, page E-2](#)
- [RADIUS-Based PAP Authentication in Cisco ISE, page E-3](#)

RADIUS-Based PAP Authentication in Cisco ISE

Cisco ISE checks the username and password pair against the identity stores, until it eventually acknowledges the authentication or terminates the connection.

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.

Cisco ISE supports standard RADIUS PAP authentication that is based on the RADIUS UserPassword attribute. RADIUS PAP authentication is compatible with all identity stores.

The RADIUS-with-PAP-authentication flow includes logging of passed and failed attempts.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based Protocols Without EAP, page E-2](#)
- [Password Authentication Protocol, page E-3](#)

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.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based Protocols Without EAP, page E-2](#)

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

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based Protocols Without EAP, page E-2](#)

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
- Microsoft Active Directory identity store

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based Protocols Without EAP, page E-2](#)

RADIUS-Based EAP Protocols

EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics:

Simple EAP Methods

- [Extensible Authentication Protocol-Message Digest 5, page E-6](#)
- [Lightweight Extensible Authentication Protocol, page E-7](#)

EAP Methods That Use Cisco ISE Server Certificate for 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](#)

Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)

RADIUS-Based EAP Authentication Flow

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.

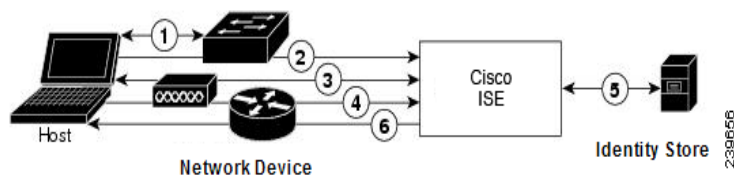
In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

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 E-2 shows a RADIUS-based authentication with EAP.

Figure E-2 RADIUS-Based Authentication with EAP



Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)

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 in a response by encrypting 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. Because no server authentication occurs, it is also vulnerable to spoofing. Cisco ISE supports EAP-MD5 authentication against the Cisco ISE internal identity store. Host Lookup is also supported when using the EAP-MD5 protocol. See the [Allowed Protocols Services Settings, page B-19](#) for more information on Host Lookup.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)

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.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)

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.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)

- [Advantages of Using PEAP, page E-8](#)
- [Supported Supplicants for the PEAP Protocol, page E-8](#)
- [PEAP Protocol Flow, page E-9](#)

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.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)
- [Protected Extensible Authentication Protocol, page E-7](#)
- [Supported Supplicants for the PEAP Protocol, page E-8](#)
- [PEAP Protocol Flow, page E-9](#)

Supported Supplicants for the PEAP Protocol

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

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)
- [Protected Extensible Authentication Protocol, page E-7](#)
- [Advantages of Using PEAP, page E-8](#)
- [PEAP Protocol Flow, page E-9](#)

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 Admin portal. 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 Admin portal. 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.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)
- [Protected Extensible Authentication Protocol, page E-7](#)
- [Advantages of Using PEAP, page E-8](#)
- [Supported Supplicants for the PEAP Protocol, page E-8](#)

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.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)
- [Benefits of EAP-FAST, page E-10](#)
- [EAP-FAST Flow, page E-11](#)

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.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)
- [Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling, page E-10](#)
- [EAP-FAST Flow, page E-11](#)

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.

Related Topics

- [Password-Based Authentication, page E-1](#)
- [RADIUS Protocol Support in Cisco ISE, page E-2](#)
- [RADIUS-Based EAP Protocols, page E-5](#)
- [RADIUS-Based EAP Authentication Flow, page E-6](#)
- [Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling, page E-10](#)
- [Benefits of EAP-FAST, page E-10](#)



Switch and Wireless LAN Controller 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. This appendix contains the following sections:

- [Enable Your Switch to Support Standard Web Authentication, page F-2](#)
- [Define a Local Username and Password for Synthetic RADIUS Transactions, page F-2](#)
- [Set the NTP Server to Ensure Accurate Log and Accounting Timestamps, page F-2](#)
- [Enable AAA Functions, page F-3](#)
- [Configure a RADIUS Server, page F-3](#)
- [Configure the Switch to Send RADIUS Accounting Start/Stop to Inline Posture Nodes, page F-4](#)
- [Enable RADIUS Change of Authorization \(CoA\), page F-4](#)
- [Enable Device Tracking and DHCP Snooping, page F-4](#)
- [Enable 802.1X Port-Based Authentication, page F-4](#)
- [Use EAP for Critical Authentications, page F-4](#)
- [Throttle AAA Requests Using Recovery Delay, page F-5](#)
- [Define VLANs Based on Enforcement States, page F-5](#)
- [Define Local \(Default\) ACLs on the Switch, page F-5](#)
- [Enable Cisco Security Group Access Switch Ports, page F-6](#)
- [Enable EPM Logging, page F-8](#)
- [Enable SNMP Traps, page F-8](#)
- [Enable SNMP v3 Query for Profiling, page F-8](#)
- [Enable MAC Notification Traps for Profiler to Collect, page F-9](#)
- [Configure the RADIUS Idle-Timeout, page F-9](#)
- [Set Up the Wireless LAN Controller for iOS Supplicant Provisioning, page F-9](#)
- [Configure the Wireless LAN Controller to Support Apple Devices, page F-9](#)
- [Configure ACLs on the Wireless LAN Controller for MDM Interoperability, page F-10](#)

Enable Your Switch to Support Standard Web Authentication

Ensure that you include the following commands 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 Username and Password for Synthetic RADIUS Transactions

Enter the following command 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

Ensure that you specify the same NTP server as you have set in Cisco ISE at **Administration > System > Settings > System Time** by entering the following command:

```
ntp server <IP_address>|<domain_name>
```

Enable AAA Functions

Enter the following commands 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 Cisco ISE to act as a AAA server when interacting with the client at IP address
10.0.56.17
```

Configure a RADIUS Server

Configure the switch to interoperate with Cisco ISE acting as the RADIUS source server by entering the following commands:

```
!
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.

Configure the Switch to Send RADIUS Accounting Start/Stop to Inline Posture Nodes

The network access device should be configured to send RADIUS accounting “Start” and “Stop” messages at the beginning and end of a session, respectively, with the remote device’s IP address in those messages to the Inline Posture nodes. The Inline Posture node associates the device IP address to any relevant authorization profiles downloaded over the life of a session. For example, a remote device may have an “unknown-compliance-state” authorization profile at initial login, then switch to a “compliant” authorization profile following CoA (assuming successful device posture assessment).

Enable RADIUS Change of Authorization (CoA)

Specify the settings to ensure the switch is able to appropriately handle RADIUS Change of Authorization behavior supporting Posture functions from Cisco ISE by entering the following commands:

```
aaa server radius dynamic-author
  client <ISE-IP> server-key 0 cisco123
```



Note

Cisco ISE uses port 1700 (Cisco IOS software 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 by entering the following commands:

```
! Optional
ip dhcp snooping
! Required!
ip device tracking
```

Enable 802.1X Port-Based Authentication

Enter the following commands to turn 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) by entering the following command:

```
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 by entering the following command:

```
authentication critical recovery delay 1000
```

Define VLANs Based on Enforcement States

Enter the following commands 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 Cisco IOS software releases earlier than 12.2(55)SE) to ensure Cisco ISE is able to perform the dynamic ACL updates required for authentication and authorization by entering the following commands:

```
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 that 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. We strongly recommend 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. Because 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 because we want complete visibility and do not want to 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 Cisco IOS software Release 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 Cisco IOS software Release 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 without any impact to 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 by choosing **Administration > Network Resources > Network Devices > Add | Edit > SNMP Settings**. See [“SNMP Settings” section on page A-38](#) 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 [Permissions for Authorization Profiles](#), page 20-10.

Set Up the Wireless LAN Controller for iOS Suppliant Provisioning

To support Apple iOS-based devices (iPhone/iPad) switching from one SSID to another on the same wireless access point, be sure to configure the Wireless LAN Controller (WLC) to enable the “FAST SSID change” function. This function helps ensure iOS-based devices are able to more quickly switch between SSIDs.

```
WLC (config)# FAST SSID change
```

Configure the Wireless LAN Controller to Support Apple Devices

Apple devices include the Apple Captive Network Assistant (CNA) feature, which detects captive networks (like the Cisco ISE WebAuth page), but it interferes with the portal redirection required to support guests and personal devices.

You can bypass this feature by enabling the **web-auth captive-bypass** command on the Wireless LAN Controller (WLC):

```
WLC > config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.
You must reset system for this setting to take effect.
WLC > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
WLC >
```

Configure ACLs on the Wireless LAN Controller for MDM Interoperability

You must configure ACLs on the wireless LAN controller for use in authorization policy to redirect nonregistered devices and certificate provisioning. Your ACLs should be in the following sequence.

-
Step 1	Allow all outbound traffic from server to client.
Step 2	(Optional) Allow ICMP inbound traffic from client to server for troubleshooting.
Step 3	Allow access to MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.
Step 4	Allow all inbound traffic from client to server to ISE for Web Portal and supplicant, and certificate provisioning flows.
Step 5	Allow inbound DNS traffic from client to server for name resolution.
Step 6	Allow inbound DHCP traffic from client to server for IP addresses.
Step 7	Deny all inbound traffic from client to server to corporate resources for redirection to ISE (as per your company policy).
Step 8	(Optional) Permit the rest of the traffic.
-

Figure F-1 shows the ACLs for redirecting a nonregistered device to the BYOD flow. In this example, the Cisco ISE ip address is 10.35.50.165, the internal corporate network ip address is 192.168.0.0 and 172.16.0.0 (to redirect), and the MDM server subnet is 204.8.168.0.

Figure F-1 *ACLs for Redirecting Nonregistered Devices*

General										
Access List Name		NSP-ACL								
Deny Counters		0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 0.0.0.0 0.0.0.0	Any	Any	Any	Any	Outbound	150720	
2	Permit	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 0.0.0.0 204.8.168.0	ICMP	Any	Any	Any	Inbound	7227	
3	Permit	0.0.0.0 / 0.0.0.0 0.0.0.0	255.255.255.0 / 10.35.50.165 255.255.255.255	Any	Any	Any	Any	Any	17626	
4	Permit	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 0.0.0.0 0.0.0.0	Any	Any	Any	Any	Inbound	7505	
5	Permit	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 0.0.0.0 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864	
6	Permit	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 0.0.0.0 192.168.0.0	UDP	Any	DHCP Server	Any	Inbound	0	
7	Deny	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 255.255.0.0 172.16.0.0	Any	Any	Any	Any	Inbound	0	
8	Deny	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 255.240.0.0 10.0.0.0	Any	Any	Any	Any	Inbound	4	
9	Deny	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 255.0.0.0 173.194.0.0	Any	Any	Any	Any	Inbound	457	
10	Deny	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 255.255.0.0 171.68.0.0	Any	Any	Any	Any	Inbound	1256	
11	Deny	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 255.252.0.0 171.71.181.0	Any	Any	Any	Any	Inbound	11310	
12	Deny	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 255.255.255.0 0.0.0.0	Any	Any	Any	Any	Any	0	
13	Permit	0.0.0.0 / 0.0.0.0 0.0.0.0	0.0.0.0 / 0.0.0.0 0.0.0.0	Any	Any	Any	Any	Any	71819	

■ Configure ACLs on the Wireless LAN Controller for MDM Interoperability



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 G-2](#)
- [Licensing and Administrator Access, page G-11](#)
- [Configuration and Operation \(Including High Availability\), page G-12](#)
- [External Authentication Sources, page G-16](#)
- [Client Access, Authentication, and Authorization, page G-21](#)
- [Error Messages, page G-35](#)
- [Configure NADs for ISE Monitoring, page G-39](#)
- [Troubleshooting APIs, page G-40](#)
- [Contacting the Cisco Technical Assistance Center, page G-41](#)



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 1.2, however, we recommend using the stand-alone [Cisco Identity Services Engine Troubleshooting Guide, Release 1.2](#).

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 1.2](#).

**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 **Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator**.

Current Installation and Network Connection Troubleshooting Topics

- [Unknown Network Device, page G-3](#)
- [CoA Not Initiating on Client Machine, page G-3](#)
- [Users Are Assigned to Incorrect VLAN During Network Access Sessions, page G-4](#)
- [Client Machine URL Redirection Function Not Working, page G-5](#)
- [Cisco ISE Profiler is Not Able to Collect Data for Endpoints, page G-5](#)
- [RADIUS Accounting Packets \(Attributes\) Not Coming from Switch, page G-6](#)
- [Policy Service Node Not Passing Traffic, page G-7](#)
- [Registered Nodes in Cisco ISE-Managed List Following Standalone Reinstallation, page G-7](#)
- [Primary and Secondary Inline Posture Nodes Heartbeat Link Not Working, page G-8](#)
- [Cisco SNS-3415 Appliance RAID Configuration Cleared Inadvertently, page G-8](#)
- [Cisco SNS-3495 Appliance RAID Configuration Cleared Inadvertently, page G-9](#)

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 (for example, 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 (required on switch to activate CoA and configure the switch): <pre>aaa server radius dynamic-author client <Monitoring_node_IP_address> server-key <radius_key></pre>

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 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 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 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 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 the accounting events shows that audit-session-id fields are blank because the VSA¹ 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 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 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 portal 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 Admin portal displays the Policy Service 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 nodes.
Possible Causes	If the Policy Service 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 nodes from the Cisco ISE node, reconfigure the Policy Service nodes so that it sends syslog messages to itself, rather than the Cisco ISE node and restart the Policy Service node. Note If you deregister any associated Policy Service nodes before reinstalling the Cisco ISE software and reconfiguring the Administration persona, the Policy Service 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.

Cisco SNS-3415 Appliance RAID Configuration Cleared Inadvertently

Symptoms or Issue	RAID configuration does not exist on the Cisco SNS-3415 series appliance. This RAID configuration needs to be re-configured.
Conditions	Configuration of RAID on the Cisco SNS-3415 series appliance is done at manufacturing time and you are not required to perform it again. The only reason to re-configure RAID would be if someone inadvertently deletes the RAID configuration.
Possible Causes	The RAID configuration on the Cisco SNS-3415 series appliance is deleted accidentally.
Resolution	1. Reboot the Cisco SNS-3415 appliance. 2. When the appliance is in the process of booting, press Ctrl+M. The LSI Software RAID Configuration Utility opens displaying the Main Setup Utility window. 3. On the Management Menu screen, , select Configure > Clear Configuration. The Configuration Menu screen appears. 4. At the prompt, select Yes to confirm and press Enter. The virtual drive is deleted from the configuration. 5. On the Management Menu screen, choose Configure with your cursor, and press Enter. The Configuration Menu screen appears. 6. Use your cursor to highlight Easy Configuration and press Enter. The Easy Configuration - Array Selection Menu appears. 7. Press the space bar to select <i>ONLIN AOO-xx</i> and add it to the drive group.

	8. Press F10 to continue configuration. The Select Configurable Array(s) dialog box appears. 9. Press the space bar to select the drive group. 10. Press F10 to continue configuration. The Virtual Drive(s) Configured dialog box appears. This dialog box shows the virtual drive number, RAID level, drive group size, number of stripes, stripe size and drive status. 11. Change the virtual drive options from the defaults listed in the dialogbox as needed. Use the cursor keys to navigate between the virtual drive parameters and choose 557.8Gb, and RAID 0. 12. Highlight Accept and press Enter after you select your virtual drive parameters. The virtual drive configuration appears. 13. Press Esc to continue. 14. Click Yes at the prompt to save the configuration. The LSI Software RAID Configuration Utility begins a background initialization of the virtual drives. New RAID 5 virtual drives require a minimum number of drives for a background initialization to start. If there are fewer drives than the minimum, the background initialization will not start. 15. Press Esc 3 times to exit all menus. 16. The system displays an Exit prompt. Use the arrow keys to choose Yes and press Enter. The system prompts you to press CTRL+ALT+DEL to reboot appliance. 17. Restart the Cisco SNS-3415 appliance.

Cisco SNS-3495 Appliance RAID Configuration Cleared Inadvertently

Symptoms or Issue	RAID configuration does not exist on the Cisco SNS-3495 series appliance. This RAID configuration needs to be re-configured.
Conditions	Configuring RAID on the Cisco SNS-3495 series appliance is done at manufacturing time and you are not required to perform it again. The only reason to reconfigure the RAID would be if someone inadvertently deletes the RAID configuration.
Possible Causes	The RAID configuration on the Cisco SNS-3495 series appliance is deleted accidentally.

Resolution	1. Reboot the Cisco SNS-3495 appliance. 2. When the Cisco SNS-3495 appliance is in the process of booting, press Ctrl+H to enter the WebBIOS. The Controller Selection window appears. 3. Click Start to continue. The main WebBIOS CU window appears. 4. Click Configuration Wizard in the left pane of the WebBIOS main window. The first Configuration Wizard window opens. 5. Click the Clear Configuration radio button to clear the existing configuration. 6. Click Next. WebBIOS prompts you indicating that all the existing configuration data will be deleted. 7. Click Yes to continue. 8. Click Configuration Wizard in the left pane of the WebBIOS main window. The first Configuration Wizard window opens. 9. Click the New Configuration radio button and click Next. WebBIOS prompts you indicating whether you are sure to continue. 10. Click Yes. The WebBIOS Configuration Method window opens. 11. Click the Automatic Configuration radio button 12. Click Next. 13. From the drop-down list, Choose Redundancy When Possible. 14. Click Next. The WebBIOS displays the proposed new configuration, review the information in the window. 15. Click Accept. WebBIOS prompts you to save the configuration. 16. Click Yes. WebBIOS begins a background initialization of the RAID volumes and a screen appears that enables you to re-initialize the RAID volumes. 17. Click the Home button. 18. Click the Exit button on the main WebBIOS screen. 19. Reboot the Cisco SNS-3495 appliance.

Licensing and Administrator Access

- [Certificate Expired, page G-11](#)

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)

This section contains the following topics:

- [Client Machines Are Unable to Authenticate](#), page G-12
- [Users Are Not Appropriately Redirected to URL](#), page G-13
- [Cannot Download Remote Client Provisioning Resources](#), page G-13
- [Lost Monitoring and Troubleshooting Data After Registering Policy Service Node to Administration Node](#), page G-13
- [Cisco ISE Monitoring Dashlets Not Visible with Internet Explorer 8](#), page G-14
- [Data Out of Sync Between Primary And Secondary ISE Nodes](#), page G-14

Client Machines Are Unable 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 the magnifying glass icon in Authentications to launch the Authentication Details. The session event section of the authentication report should have the following entry: <pre>%EPM-4-POLICY_APP_FAILURE: IP 0.0.0.0 MAC 0002.b3e9.c926 AuditSessionID 0A0002010000239039837B18 AUTHTYPE DOT1X POLICY_TYPE Named ACL POLICY_NAME xACSACLx-IP-acl_access-4918c248 RESULT FAILURE REASON Interface ACL not configured</pre>
Possible Causes	• The DACL syntax may be incorrect or not configured in Cisco ISE. • When Cisco ISE enforces the DACL and there is no preauthentication 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 preauthentication 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 Node to Administration Node

Symptoms or Issue	The known collection of profiled endpoints is not visible on the secondary Policy Service 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 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 <i>prior to</i> registering the new Policy Service 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 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 Cisco 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

This section contains the following topics:

- [User Authentication Failed, page G-16](#)
- [Missing User for RADIUS-Server Test Username in Cisco ISE Identities, page G-16](#)
- [Connectivity Issues Between the Network Access Device \(Switch\) and Cisco ISE, page G-17](#)
- [Active Directory Disconnected, page G-17](#)
- [Cisco ISE Node Not Authenticating with Active Directory, page G-18](#)
- [RADIUS Server Error Message Entries Appearing in Cisco ISE, page G-18](#)
- [RADIUS Server Connectivity Issues \(No Error Message Entries Appearing in Cisco ISE\), page G-19](#)

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 of entries 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 is 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 NTP¹ on VMware. This issue can also arise if the Cisco ISE FQDN² 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 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 AAA¹ 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 CLI² 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 node IP address • Correct server key • Recognized username or password • Connectivity between the NAD and Policy Service 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 <i>know</i> 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 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 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 node to see if there are any indications.

Client Access, Authentication, and Authorization

This section contains the following topics:

- [Cannot Authenticate on Profiled Endpoint, page G-21](#)
- [Quarantined Endpoints Do Not Renew Authentication Following Policy Change, page G-22](#)
- [Endpoint Does Not Align to the Expected Profile, page G-23](#)
- [User is Unable to Authenticate Against the Local Cisco ISE Identity Store, page G-24](#)
- [Sponsor Users Cannot Log in to Sponsor Portal, page G-24](#)
- [Certificate-Based User Authentication via Supplicant Failing, page G-25](#)
- [802.1X Authentication Fails, page G-26](#)
- [Users Are Reporting Unexpected Network Access Issues, page G-26](#)
- [Authorization Policy Not Working, page G-27](#)
- [Switch is Dropping Active AAA Sessions, page G-28](#)
- [URL Redirection on Client Machine Fails, page G-29](#)
- [Agent Download Issues on Client Machine, page G-31](#)
- [Agent Login Dialog Not Appearing, page G-32](#)
- [Agent Fails to Initiate Posture Assessment, page G-32](#)
- [Agent Displays “Temporary Access”, page G-33](#)
- [Cisco ISE Does Not Issue CoA Following Authentication, page G-33](#)
- [Non-Guest Users Do Not Go Through Guest Flow for Network Access, page G-34](#)
- [Guest Devices Keep Losing Network Access, page G-34](#)

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 MAB¹ 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 > Configurations and choose Allowed Protocol Services to create a Protocol Policy. MAC authentications use PAP²/ASCII and EAP-MD5³ 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**

Because CoA requires a MAC address or session ID, we recommend 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.

Sponsor Users Cannot Log in to Sponsor Portal

Symptoms or Issue	Sponsor users (internal or AD) are unable to log in to the sponsor portal. The following error message appears: "Invalid username or password. Please try again."
Conditions	This issue occurs when a sponsor user tries to log in to the sponsor portal.
Possible Causes	The possible causes are: - User is not valid, which means, the user record is not present in the database (internal or AD) or the user has entered invalid credentials. - Any sponsor group policy that is created by the administrator is disabled.
Resolution	Enable the sponsor group policies.

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 reusing 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 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 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 the show vlan command 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: <pre> 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 </pre> - Ensure the session is created on the switch by entering the show epm session summary command. If the IP address of the session shown is “not available,” ensure that the following configuration lines appear on the switch: <pre> ip dhcp snooping vlan 30-100 ip device tracking </pre>

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): <pre>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</pre>

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 following example. (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=0A000A720000A45A2444BFC2&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 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: <pre>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</pre> - Ensure that the HTTP and HTTPS servers are running on the switch: <pre>ip http server ip http secure-server</pre> - 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 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 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: <pre> 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 </pre> - 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, and so on).

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 reestablish 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: <pre>aaa server radius dynamic-author client 80.0.80.2 server-key cisco456 --> ISE ip. server-key cisco456</pre>

Non-Guest Users Do Not Go Through Guest Flow for Network Access

Symptoms or Issue	Active Directory users do not go through the guest flow for network access.
Conditions	This issue is specific only to non-guest users when the self-provisioning flow is enabled.
Possible Causes	Active Directory, LDAP, and internal Cisco ISE users are considered to be non-guest users. Thus, when you enable the self-provisioning flow for employees (to support personal devices, or BYOD), they are directed to that flow rather than the guest flow for network access.
Resolution	If you prefer to have non-guest users to access the network using the guest flow, you must disable the self-provisioning flow by choosing Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations > Operations and uncheck Enable Self-Provisioning Flow .

Guest Devices Keep Losing Network Access

Symptoms or Issue	Guests repeatedly lose network connectivity on device requiring them to reconnect.
Conditions	This issue is specific the configuration scenario in which you have set the Guest portal policy to limit guests to one active network session, and guest users: • have connected more than one device to the network • are activated guests.
Possible Causes	The user credentials in the supplicant are cached on the devices, allowing the devices to maintain network connectivity. However, because the guest is limited to only one network session, the devices are continually connecting on one device and disconnecting on the other device.
Resolution	Guests should force the unused device to forget the network.

Error Messages

This section contains the following topics:

- [ACTIVE_DIRECTORY_USER_INVALID_CREDENTIALS](#), page G-35
- [ACTIVE_DIRECTORY_USER_AUTH_FAILED](#), page G-35
- [ACTIVE_DIRECTORY_USER_PASSWORD_EXPIRED](#), page G-36
- [ACTIVE_DIRECTORY_USER_WRONG_PASSWORD](#), page G-36
- [ACTIVE_DIRECTORY_USER_ACCOUNT_DISABLED](#), page G-36
- [ACTIVE_DIRECTORY_USER_RESTRICTED_LOGON_HOURS](#), page G-36
- [ACTIVE_DIRECTORY_USER_NON_COMPLIANT_PASSWORD](#), page G-36
- [ACTIVE_DIRECTORY_USER_UNKNOWN_DOMAIN](#), page G-37
- [ACTIVE_DIRECTORY_USER_ACCOUNT_EXPIRED](#), page G-37
- [ACTIVE_DIRECTORY_USER_ACCOUNT_LOCKED_OUT](#), page G-37
- [ACTIVE_DIRECTORY_GROUP_RETRIEVAL_FAILED](#), page G-37
- [ACTIVE_DIRECTORY_MACHINE_AUTHENTICATION_DISABLED](#), page G-37
- [ACTIVE_DIRECTORY_ATTRIBUTE_RETRIEVAL_FAILED](#), page G-38
- [ACTIVE_DIRECTORY_PASSWORD_CHANGE_DISABLED](#), page G-38
- [ACTIVE_DIRECTORY_USER_UNKNOWN](#), page G-38
- [ACTIVE_DIRECTORY_CONNECTION_FAILED](#), page G-38
- [ACTIVE_DIRECTORY_BAD_PARAMETER](#), page G-38
- [ACTIVE_DIRECTORY_TIMEOUT](#), page G-38

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 Admin portal 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 Admin portal 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 Admin portal 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 Admin portal 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 Admin portal 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 Admin portal 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 G-39](#).

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 1.2](#).



Note

The [Cisco Identity Services Engine API Reference Guide, Release 1.2](#), 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 SNS 3400 Series appliance after your initial installation.



Supported Management Information Bases in Cisco ISE

This chapter lists Objects and Object Identifiers (OIDs) for the Management Information Bases (MIBs) supported by Cisco ISE.

- [IF-MIB](#)
- [SNMPv2-MIB](#)
- [IP-MIB](#)
- [CISCO-CDP-MIB](#)
- [CISCO-VTP-MIB](#)
- [CISCO-STACK-MIB](#)
- [BRIDGE-MIB](#)
- [OLD-CISCO-INTERFACE-MIB](#)
- [CISCO-LWAPP-AP-MIB](#)
- [CISCO-LWAPP-DOT11-CLIENT-MIB](#)
- [CISCO-AUTH-FRAMEWORK-MIB](#)
- [EEE8021-PAE-MIB: RFC IEEE 802.1X](#)
- [HOST-RESOURCES-MIB](#)
- [LLDP-MIB](#)

Table H-1 **IF-MIB**

Object	OID
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

Table H-2 *SNMPv2-MIB*

Object	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

Table H-3 *IP-MIB*

Object	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2

Table H-4 *CISCO-CDP-MIB*

Object	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13

Table H-4 CISCO-CDP-MIB

Object	OID
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

Table H-5 CISCO-VTP-MIB

Object	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

Table H-6 CISCO-STACK-MIB

Object	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

Table H-7 BRIDGE-MIB

Object	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

Table H-8 OLD-CISCO-INTERFACE-MIB

Object	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

Table H-9 CISCO-LWAPP-AP-MIB

Object	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

Table H-10 CISCO-LWAPP-DOT11-CLIENT-MIB

Object	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

Table H-11 CISCO-AUTH-FRAMEWORK-MIB

Object	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

Table H-12 **EEE8021-PAE-MIB: RFC IEEE 802.1X**

Object	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

Table H-13 **HOST-RESOURCES-MIB**

Object	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

Table H-14 **LLDP-MIB**

Object	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
lldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12