User Guide for the Cisco Secure Access Control System 5.1

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

Text Part Number: OL-18995-01

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 of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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.

User Guide for the Cisco Secure Access Control System 5.1
© 2009 Cisco Systems, Inc. All rights reserved.

CONTENTS

Preface xxiii

Audience xxiii

Document Organization xxiii

Document Conventions xxiv

Documentation Updates xxv

Related Documentation xxvi

Notices xxvi

Obtaining Documentation and Submitting a Service Request xxviii

CHAPTER 1 **Introducing ACS 5.1** 1-1

Overview of ACS 1-1

ACS Distributed Deployment 1-2

ACS 4.x and 5.1 Replication 1-2

ACS Licensing Model 1-3

ACS Management Interfaces 1-3

ACS Web-Based Interface 1-3

ACS Command Line Interface 1-4

ACS Programmatic Interfaces 1-5

CHAPTER 2 **Migrating from ACS 4.x to ACS 5.1** 2-1

Overview of the Migration Process 2-1

Migration Requirements 2-2

Supported Migration Versions 2-2

Before You Begin 2-3

Downloading Migration Files 2-3

Migrating from ACS 4.x to ACS 5.1 2-3

Functionality Mapping from ACS 4.x to ACS 5.1 2-4

Common Scenarios in Migration 2-7

Migrating from ACS 4.2 on CSACS 1120 to ACS 5.1 2-7

Migrating from ACS 3.x to ACS 5.1 2-8

Migrating Data from Other AAA Servers to ACS 5.1 2-8

CHAPTER 3 **ACS 5.x Policy Model** 3-1

Overview of the ACS 5.x Policy Model 3-1
Policy Terminology 3-3
Simple Policies 3-4
Rule-Based Policies 3-4
Types of Policies 3-4
Access Services 3-5
Identity Policy 3-8
Group Mapping Policy 3-10
Authorization Policy for Device Administration 3-10
Processing Rules with Multiple Command Sets 3-10
Exception Authorization Policy Rules 3-11
Service Selection Policy 3-11
Simple Service Selection 3-12
Rules-Based Service Selection 3-12
Access Services and Service Selection Scenarios 3-12
First-Match Rule Tables 3-13
Policy Conditions 3-15
Policy Results 3-15
Authorization Profiles for Network Access 3-16
Processing Rules with Multiple Authorization Profiles 3-16
Policies and Identity Attributes 3-16
Policies and Network Device Groups 3-17
Example of a Rule-Based Policy 3-17
Flows for Configuring Services and Policies 3-18

CHAPTER 4 **Common Scenarios Using ACS** 4-1

Overview of Device Administration 4-2
Session Administration 4-3
Command Authorization 4-4
TACACS+ Custom Services and Attributes 4-4
Password-Based Network Access 4-5
Overview of Password-Based Network Access 4-5
Password-Based Network Access Configuration Flow 4-6
Certificate-Based Network Access 4-8
Overview of Certificate-Based Network Access 4-8
Using Certificates in ACS 4-9
Certificate-Based Network Access for EAP-TLS 4-9

Authorizing the ACS Web Interface from Your Browser Using a Certificate 4-10
Validating an LDAP Secure Authentication Connection 4-11
Agentless Network Access 4-11
Overview of Agentless Network Access 4-11
Host Lookup 4-12
Authentication with Call Check 4-13
Process Service-Type Call Check 4-14
PAP/EAP-MD5 Authentication 4-14
Agentless Network Access Flow 4-15
Configuring an Internal Identity Store for Host Lookup 4-16
Configuring an LDAP External Identity Store for Host Lookup 4-16
Configuring an Identity Group for Host Lookup Network Access Requests 4-17
Creating an Access Service for Host Lookup 4-17
Configuring an Identity Policy for Host Lookup Requests 4-18
Configuring an Authorization Policy for Host Lookup Requests 4-18
VPN Remote Network Access 4-19
Supported Authentication Protocols 4-19
Supported Identity Stores 4-20
Supported VPN Network Access Servers 4-20
Supported VPN Clients 4-21
Configuring VPN Remote Access Service 4-21
ACS and Cisco TrustSec 4-22
Adding Devices for TrustSec 4-22
Creating Security Groups 4-23
Creating SGACLs 4-23
Configuring an NDAC Policy 4-24
Configuring EAP-FAST Settings for TrustSec 4-24
Creating an Access Service for TrustSec 4-25
Creating an Endpoint Admission Control Policy 4-25
Creating an Egress Policy 4-26
Creating a Default Policy 4-27
RADIUS Proxy Requests 4-27
Supported Protocols 4-28
Supported RADIUS Attributes 4-29
Configuring RADIUS Proxy Service 4-29

CHAPTER 5 **Understanding My Workspace** 5-1
Welcome Page 5-1
Task Guides 5-2

My Account Page 5-2
Using the Web Interface 5-3
Accessing the Web Interface 5-3
Logging In 5-3
Logging Out 5-4
Understanding the Web Interface 5-5
Web Interface Design 5-5
Navigation Pane 5-6
Content Area 5-8
Importing and Exporting ACS Objects through the Web Interface 5-18
Supported ACS Objects 5-18
Creating Import Files 5-20
Downloading the Template from the Web Interface 5-20
Understanding the CSV Templates 5-21
Creating the Import File 5-22
Common Errors 5-25
Concurrency Conflict Errors 5-25
Deletion Errors 5-26
System Failure Errors 5-26
Accessibility 5-27
Display and Readability Features 5-27
Keyboard and Mouse Features 5-28
Obtaining Additional Accessibility Information 5-28

CHAPTER 6 **Post-Installation Configuration Tasks** 6-1
Configuring Minimal System Setup 6-1
Configuring ACS to Perform System Administration Tasks 6-2
Configuring ACS to Manage Access Policies 6-3
Configuring ACS to Monitor and Troubleshoot Problems in the Network 6-4

CHAPTER 7 **Managing Network Resources** 7-1
Network Device Groups 7-1
Creating, Duplicating, and Editing Network Device Groups 7-2
Deleting Network Device Groups 7-3
Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy 7-3
Deleting Network Device Groups from a Hierarchy 7-4
Network Devices and AAA Clients 7-5
Viewing and Performing Bulk Operations for Network Devices 7-5

Exporting Network Devices and AAA Clients 7-7
Performing Bulk Operations for Network Resources and Users 7-8
Exporting Network Resources and Users 7-9
Creating, Duplicating, and Editing Network Devices 7-10
Configuring Network Device and AAA Clients 7-11
Displaying Network Device Properties 7-13
Deleting Network Devices 7-16
Configuring a Default Network Device 7-16
Working with External RADIUS Servers 7-17
Creating, Duplicating, and Editing External RADIUS Servers 7-18
Deleting External RADIUS Servers 7-19

CHAPTER 8 **Managing Users and Identity Stores** 8-1
Overview 8-1
Internal Identity Stores 8-1
External Identity Stores 8-2
Identity Stores with Two-Factor Authentication 8-2
Identity Groups 8-3
Certificate-Based Authentication 8-3
Identity Sequences 8-3
Managing Internal Identity Stores 8-4
Authentication Information 8-5
Identity Groups 8-5
Creating Identity Groups 8-6
Deleting an Identity Group 8-7
Managing Identity Attributes 8-7
Standard Attributes 8-8
User Attributes 8-8
Host Attributes 8-9
Configuring Authentication Settings for Users 8-9
Creating Internal Users 8-11
Deleting Users from Internal Identity Stores 8-13
Viewing and Performing Bulk Operations for Internal Identity Store Users 8-14
Creating Hosts in Identity Stores 8-15
Deleting Internal Hosts 8-17
Viewing and Performing Bulk Operations for Internal Identity Store Hosts 8-17
Managing External Identity Stores 8-18
LDAP Overview 8-18
Directory Service 8-19

Authentication Using LDAP 8-19
Multiple LDAP Instances 8-20
Failover 8-20
LDAP Connection Management 8-20
Authenticating a User Using a Bind Connection 8-20
Group Membership Information Retrieval 8-21
Attributes Retrieval 8-22
Certificate Retrieval 8-22
Creating External LDAP Identity Stores 8-22
Configuring an External LDAP Server Connection 8-23
Configuring External LDAP Directory Organization 8-26
Deleting External LDAP Identity Stores 8-29
Configuring LDAP Groups 8-29
Viewing LDAP Attributes 8-30
Leveraging Cisco NAC Profiler as an External MAB Database 8-31
Enabling the LDAP Interface on Cisco NAC Profiler to Communicate with ACS 8-31
Configuring NAC Profile LDAP Definition in ACS for Use in Identity Policy 8-33
Troubleshooting MAB Authentication with Profiler Integration 8-37
Microsoft AD 8-38
Machine Authentication 8-39
Attribute Retrieval for Authorization 8-40
Group Retrieval for Authorization 8-40
Certificate Retrieval for EAP-TLS Authentication 8-40
Concurrent Connection Management 8-40
User and Machine Account Restrictions 8-40
Machine Access Restrictions 8-40
Joining ACS to an AD Domain 8-42
Configuring an AD Identity Store 8-42
Selecting an AD Group 8-44
Configuring AD Attributes 8-45
RSA SecurID Server 8-46
Configuring RSA SecurID Agents 8-47
Creating and Editing RSA SecurID Token Servers 8-47
RADIUS Identity Stores 8-52
Supported Authentication Protocols 8-52
Failover 8-53
Password Prompt 8-53
User Group Mapping 8-53
Groups and Attributes Mapping 8-53
RADIUS Identity Store in Identity Sequence 8-54

Authentication Failure Messages 8-54
Username Special Format with Safeword Server 8-54
User Attribute Cache 8-55
Creating, Duplicating, and Editing RADIUS Identity Servers 8-55
Configuring CA Certificates 8-60
Adding a Certificate Authority 8-60
Editing a Certificate Authority and Configuring Certificate Revocation Lists 8-61
Deleting a Certificate Authority 8-63
Exporting a Certificate Authority 8-63
Configuring Certificate Authentication Profiles 8-64
Configuring Identity Store Sequences 8-65
Creating, Duplicating, and Editing Identity Store Sequences 8-66
Deleting Identity Store Sequences 8-68

CHAPTER 9 **Managing Policy Elements** 9-1
Managing Policy Conditions 9-1
Creating, Duplicating, and Editing a Date and Time Condition 9-3
Creating, Duplicating, and Editing a Custom Session Condition 9-5
Deleting a Session Condition 9-6
Managing Network Conditions 9-7
Importing Network Conditions 9-8
Exporting Network Conditions 9-9
Creating, Duplicating, and Editing End Station Filters 9-10
Creating, Duplicating, and Editing Device Filters 9-12
Creating, Duplicating, and Editing Device Port Filters 9-15
Managing Authorizations and Permissions 9-18
Creating, Duplicating, and Editing Authorization Profiles for Network Access 9-18
Specifying Authorization Profiles 9-19
Specifying Common Attributes in Authorization Profiles 9-20
Specifying RADIUS Attributes in Authorization Profiles 9-22
Creating and Editing Security Groups 9-24
Creating, Duplicating, and Editing a Shell Profile for Device Administration 9-24
Defining General Shell Profile Properties 9-26
Defining Common Tasks 9-27
Defining Custom Attributes 9-28
Creating, Duplicating, and Editing Command Sets for Device Administration 9-29
Creating, Duplicating, and Editing Downloadable ACLs 9-32
Deleting an Authorizations and Permissions Policy Element 9-33
Configuring Security Group Access Control Lists 9-33

TACACS+ Command Sets 9-35
The TACACS+ Command Set Definition 9-35
Evaluation of Command Based Administration 9-35
Level 1: Match Logic for a Single Command Definition in a Command Set 9-36
Level 2: Match Logic for a Command Set 9-37
Level 3: Match Logic for the Combined Set of Command Sets 9-37

CHAPTER 10 **Managing Access Policies** 10-1
Policy Creation Flow 10-1
Network Definition and Policy Goals 10-2
Policy Elements in the Policy Creation Flow 10-3
Access Service Policy Creation 10-4
Service Selection Policy Creation 10-4
Customizing a Policy 10-5
Configuring the Service Selection Policy 10-6
Configuring a Simple Service Selection Policy 10-6
Service Selection Policy Page 10-6
Creating, Duplicating, and Editing Service Selection Rules 10-8
Displaying Hit Counts 10-10
Deleting Service Selection Rules 10-11
Configuring Access Services 10-11
Editing Default Access Services 10-12
Creating, Duplicating, and Editing Access Services 10-13
Configuring General Access Service Properties 10-14
Configuring Access Service Allowed Protocols 10-16
Configuring Access Services Templates 10-19
Deleting an Access Service 10-20
Configuring Access Service Policies 10-20
Viewing Identity Policies 10-21
Viewing Rules-Based Identity Policies 10-22
Configuring Identity Policy Rule Properties 10-24
Configuring a Group Mapping Policy 10-26
Configuring Group Mapping Policy Rule Properties 10-28
Configuring a Session Authorization Policy for Network Access 10-29
Configuring Network Access Authorization Rule Properties 10-32
Configuring Device Administration Authorization Policies 10-33
Configuring Device Administration Authorization Rule Properties 10-34
Configuring Device Administration Authorization Exception Policies 10-35
Configuring Shell/Command Authorization Policies for Device Administration 10-36

Configuring Authorization Exception Policies 10-36
Creating Policy Rules 10-39
Duplicating a Rule 10-40
Editing Policy Rules 10-40
Deleting Policy Rules 10-41
Configuring Compound Conditions 10-42
Compound Condition Building Blocks 10-42
Types of Compound Conditions 10-43
Using the Compound Expression Builder 10-45
TrustSec Access Control Pages 10-46
Egress Policy Matrix Page 10-47
Editing a Cell in the Egress Policy Matrix 10-47
Defining a Default Policy for Egress Policy Page 10-48
NDAC Policy Page 10-49
NDAC Policy Properties Page 10-51
Network Device Access EAP-FAST Settings Page 10-52

CHAPTER 11 **Monitoring and Reporting in ACS** 11-1
Authentication Records and Details 11-2
Dashboard Pages 11-3
Working with Portlets 11-4
Working with Authentication Lookup Portlet 11-5
Running Authentication Lookup Report 11-6
Configuring Tabs in the Dashboard 11-6
Adding Tabs to the Dashboard 11-6
Adding Applications to Tabs 11-7
Renaming Tabs in the Dashboard 11-7
Changing the Dashboard Layout 11-7
Deleting Tabs from the Dashboard 11-8

CHAPTER 12 **Managing Alarms** 12-1
Understanding Alarms 12-1
Evaluating Alarm Thresholds 12-2
Notifying Users of Events 12-3
Viewing and Editing Alarms in Your Inbox 12-3
Understanding Alarm Schedules 12-5
Creating and Editing Alarm Schedules 12-6
Assigning Alarm Schedules to Thresholds 12-7

Deleting Alarm Schedules 12-7
Creating, Editing, and Duplicating Alarm Thresholds 12-8
Configuring General Threshold Information 12-9
Configuring Threshold Criteria 12-9
Passed Authentications 12-10
Failed Authentications 12-12
Authentication Inactivity 12-14
TACACS Command Accounting 12-15
TACACS Command Authorization 12-16
ACS Configuration Changes 12-17
ACS System Diagnostics 12-18
ACS Process Status 12-19
ACS System Health 12-19
ACS AAA Health 12-20
RADIUS Sessions 12-22
Unknown NAD 12-22
External DB Unavailable 12-23
RBACL Drops 12-24
NAD-Reported AAA Downtime 12-26
Configuring Threshold Notifications 12-27
Deleting Alarm Thresholds 12-29
Configuring System Alarm Settings 12-29
Understanding Alarm Syslog Targets 12-30
Creating and Editing Alarm Syslog Targets 12-30
Deleting Alarm Syslog Targets 12-31

CHAPTER 13 **Managing Reports** 13-1
Working with Favorite Reports 13-3
Adding Reports to Your Favorites Page 13-3
Viewing Favorite-Report Parameters 13-4
Editing Favorite Reports 13-5
Running Favorite Reports 13-6
Deleting Reports from Favorites 13-7
Sharing Reports 13-7
Working with Catalog Reports 13-7
Available Reports in the Catalog 13-8
Running Catalog Reports 13-12
Deleting Catalog Reports 13-13
Running Named Reports 13-13

Understanding the Report_Name Page 13-15
Changing Authorization and Disconnecting Active RADIUS Sessions 13-17
Customizing Reports 13-19
Restoring Reports 13-19
Viewing Reports 13-20
About Standard Viewer 13-20
About Interactive Viewer 13-20
About Interactive Viewer's Context Menus 13-20
Navigating Reports 13-22
Using the Table of Contents 13-22
Exporting Report Data 13-23
Printing Reports 13-25
Saving Report Designs in Interactive Viewer 13-25
Formatting Reports in Interactive Viewer 13-26
Editing Labels 13-26
Formatting Labels 13-27
Formatting Data 13-27
Resizing Columns 13-28
Changing Column Data Alignment 13-28
Formatting Data in Columns 13-28
Formatting Data in Aggregate Rows 13-28
Formatting Data Types 13-29
Formatting Numeric Data 13-30
Formatting Fixed or Scientific Numbers or Percentages 13-31
Formatting Custom Numeric Data 13-31
Formatting String Data 13-32
Formatting Custom String Data 13-32
Formatting Date and Time 13-33
Formatting Custom Date and Time 13-34
Formatting Boolean Data 13-35
Applying Conditional Formats 13-35
Setting Conditional Formatting for Columns 13-36
Deleting Conditional Formatting 13-38
Setting and Removing Page Breaks in Detail Columns 13-39
Setting and Removing Page Breaks in a Group Column 13-39
Organizing Report Data 13-39
Displaying and Organizing Report Data 13-40
Reordering Columns in Interactive Viewer 13-40
Removing Columns 13-42

Hiding or Displaying Report Items 13-42
Hiding Columns 13-43
Displaying Hidden Columns 13-43
Merging Columns 13-43
Selecting a Column from a Merged Column 13-44
Sorting Data 13-45
Sorting a Single Column 13-45
Sorting Multiple Columns 13-45
Grouping Data 13-46
Adding Groups 13-48
Grouping Data Based on Date or Time 13-48
Removing an Inner Group 13-49
Creating Report Calculations 13-49
Understanding Supported Calculation Functions 13-50
Understanding Supported Operators 13-57
Using Numbers and Dates in an Expression 13-58
Using Multiply Values in Calculated Columns 13-58
Adding Days to an Existing Date Value 13-59
Subtracting Date Values in a Calculated Column 13-59
Working with Aggregate Data 13-60
Creating an Aggregate Data Row 13-61
Adding Additional Aggregate Rows 13-62
Deleting Aggregate Rows 13-62
Hiding and Filtering Report Data 13-63
Hiding or Displaying Column Data 13-63
Displaying Repeated Values 13-64
Hiding or Displaying Detail Rows in Groups or Sections 13-64
Working with Filters 13-65
Types of Filter Conditions 13-66
Setting Filter Values 13-67
Creating Filters 13-68
Modifying or Clearing a Filter 13-69
Creating a Filter with Multiple Conditions 13-69
Deleting One Filter Condition in a Filter that Contains Multiple Conditions 13-70
Filtering Highest or Lowest Values in Columns 13-71
Understanding Charts 13-71
Modifying Charts 13-72
Filtering Chart Data 13-72
Changing Chart Subtype 13-73
Changing Chart Formatting 13-73

CHAPTER 14 **Troubleshooting ACS with the Monitoring & Report Viewer** 14-1

Available Diagnostic and Troubleshooting Tools 14-1

Connectivity Tests 14-1

ACS Support Bundle 14-1

Expert Troubleshooter 14-2

Performing Connectivity Tests 14-3

Downloading ACS Support Bundles for Diagnostic Information 14-4

Working with Expert Troubleshooter 14-5

Troubleshooting RADIUS Authentications 14-6

Executing the Show Command on a Network Device 14-9

Evaluating the Configuration of a Network Device 14-10

Comparing SGACL Policy Between a Network Device and ACS 14-11

Comparing the SXP-IP Mappings Between a Device and its Peers 14-12

Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records 14-13

Comparing Device SGT with ACS-Assigned Device SGT 14-14

CHAPTER 15 **Managing System Operations and Configuration in the Monitoring & Report Viewer** 15-1

Configuring Data Purging and Incremental Backup 15-2

Restoring Data from a Backup 15-5

Viewing Log Collections 15-6

Log Collection Details Page 15-8

Viewing Scheduled Jobs 15-10

Viewing Process Status 15-10

Viewing Data Upgrade Status and Switching Database 15-11

Viewing Failure Reasons 15-12

Editing Failure Reasons 15-12

Specifying E-Mail Settings 15-13

Configuring SNMP Preferences 15-13

Understanding Collection Filters 15-14

Creating and Editing Collection Filters 15-14

Deleting Collection Filters 15-15

Configuring System Alarm Settings 15-16

Configuring Alarm Syslog Targets 15-16

Configuring Remote Database Settings 15-16

CHAPTER 16 **Managing System Administrators** 16-1

Understanding Administrator Roles and Accounts 16-2

Understanding Authentication 16-3
Configuring System Administrators and Accounts 16-3
Understanding Roles 16-3
Permissions 16-4
Predefined Roles 16-4
Changing Role Associations 16-5
Administrator Accounts and Role Association 16-6
Creating, Duplicating, Editing, and Deleting Administrator Accounts 16-6
Viewing Predefined Roles 16-8
Viewing Role Properties 16-8
Configuring Authentication Settings for Administrators 16-9
Configuring Session Idle Timeout 16-11
Configuring Administrator Access Settings 16-11
Resetting the Administrator Password 16-12
Changing the Administrator Password 16-13
Changing Your Own Administrator Password 16-13
Resetting Another Administrator's Password 16-13

CHAPTER 17 **Configuring System Operations** 17-1
Understanding Distributed Deployment 17-1
Activating Secondary Servers 17-2
Removing Secondary Servers 17-3
Promoting a Secondary Server 17-3
Understanding Local Mode 17-3
Understanding Full replication 17-4
Specifying a Hardware Replacement 17-4
Scheduled Backups 17-5
Creating, Duplicating, and Editing Scheduled Backups 17-5
Backing Up Primary and Secondary Instances 17-6
Synchronizing Primary and Secondary Instances After Backup and Restore 17-7
Editing Instances 17-8
Viewing and Editing a Primary Instance 17-8
Viewing and Editing a Secondary Instance 17-11
Deleting a Secondary Instance 17-12
Activating a Secondary Instance 17-13
Registering a Secondary Instance to a Primary Instance 17-13
Deregistering Secondary Instances from the Distributed System Management Page 17-16

Deregistering a Secondary Instance from the Deployment Operations Page 17-16
Promoting a Secondary Instance from the Distributed System Management Page 17-17
Promoting a Secondary Instance from the Deployment Operations Page 17-18
Replicating a Secondary Instance from a Primary Instance 17-19
Replicating a Secondary Instance from the Distributed System Management Page 17-19
Replicating a Secondary Instance from the Deployment Operations Page 17-20
Using the Deployment Operations Page to Create a Local Mode Instance 17-20
Understanding Software Updates 17-21
Creating, Duplicating, Editing, and Deleting Software Repositories 17-22
Creating, Duplicating, Editing, and Deleting a Software File or Patch 17-23
Applying Local Software Updates 17-25
Applying a Software Update to the ACS Instance 17-25
Managing Software Repositories from the Web Interface and CLI 17-26

CHAPTER 18 **Managing System Administration Configurations** 18-1
Configuring Global System Options 18-1
Configuring TACACS+ Settings 18-1
Configuring EAP-TLS Settings 18-2
Configuring PEAP Settings 18-3
Configuring EAP-FAST Settings 18-3
Generating EAP-FAST PAC 18-4
Configuring RSA SecurID Prompts 18-4
Managing Dictionaries 18-5
Viewing RADIUS and TACACS+ Attributes 18-5
Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes 18-6
Creating, Duplicating, and Editing RADIUS Vendor-Specific Subattributes 18-7
Viewing RADIUS Vendor-Specific Subattributes 18-9
Configuring Identity Dictionaries 18-10
Creating, Duplicating, and Editing an Internal User Identity Attribute 18-10
Configuring Internal Identity Attributes 18-11
Deleting an Internal User Identity Attribute 18-12
Creating, Duplicating, and Editing an Internal Host Identity Attribute 18-13
Deleting an Internal Host Identity Attribute 18-13
Configuring Local Server Certificates 18-14
Adding Local Server Certificates 18-14
Importing Server Certificates and Associating Certificates to Protocols 18-15
Generating Self-Signed Certificates 18-16
Generating a Certificate Signing Request 18-17

Binding CA Signed Certificates 18-18
Editing and Renewing Certificates 18-19
Deleting Certificates 18-20
Exporting Certificates 18-20
Viewing Outstanding Signing Requests 18-21
Configuring Logs 18-21
Configuring Remote Log Targets 18-22
Deleting a Remote Log Target 18-24
Configuring the Local Log 18-24
Deleting Local Log Data 18-25
Configuring Logging Categories 18-25
Configuring Global Logging Categories 18-25
Configuring Per-Instance Logging Categories 18-30
Configuring Per-Instance Security and Log Settings 18-31
Configuring Per-Instance Remote Syslog Targets 18-32
Displaying Logging Categories 18-33
Configuring the Log Collector 18-33
Viewing the Log Message Catalog 18-34
Licensing Overview 18-35
Types of Licenses 18-35
Installing a License File 18-36
Viewing the Base License 18-36
Upgrading the Base Server License 18-38
Viewing License Feature Options 18-39
Adding Deployment License Files 18-40
Deleting Deployment License Files 18-41
Available Downloads 18-42
Downloading Migration Utility Files 18-42
Downloading UCP WSDL Files 18-42
Downloading Sample Python Scripts 18-43

CHAPTER 19 **Understanding Logging** 19-1
About Logging 19-1
Using Log Targets 19-2
Logging Categories 19-2
Global and Per-Instance Logging Categories 19-4
Log Message Severity Levels 19-4
Local Store Target 19-5
Critical Log Target 19-7

Remote Syslog Server Target 19-8
Monitoring and Reports Server Target 19-10
Viewing Log Messages 19-10
Debug Logs 19-11
ACS 4.x Versus ACS 5.1 Logging 19-11

APPENDIX A **AAA Protocols** A-1
Typical Use Cases A-1
Device Administration (TACACS+) A-1
Session Access Requests (Device Administration [TACACS+]) A-1
Command Authorization Requests A-2
Network Access (RADIUS with and without EAP) A-2
RADIUS-Based Flow Without EAP Authentication A-3
RADIUS-Based Flows with EAP Authentication A-3
Access Protocols—TACACS+ and RADIUS A-4
Overview of TACACS+ A-5
Overview of RADIUS A-5
RADIUS VSAs A-6
ACS 5.1 as the AAA Server A-6
RADIUS Attribute Support in ACS 5.1 A-7
RADIUS Access Requests A-9

APPENDIX B **Authentication in ACS 5.1** B-1
Authentication Considerations B-1
Authentication and User Databases B-1
PAP B-2
RADIUS PAP Authentication B-3
EAP B-3
EAP-MD5 B-5
Overview of EAP-MD5 B-5
EAP- MD5 Flow in ACS 5.1 B-5
EAP-TLS B-5
Overview of EAP-TLS B-6
User Certificate Authentication B-6
PKI Authentication B-7
PKI Credentials B-8
PKI Usage B-8
Fixed Management Certificates B-8

Importing Trust Certificates B-9
Acquiring Local Certificates B-9
Importing the ACS Server Certificate B-9
Initial Self-Signed Certificate Generation B-10
Certificate Generation B-10
Exporting Credentials B-11
Credentials Distribution B-11
Hardware Replacement and Certificates B-11
Securing the Cryptographic Sensitive Material B-12
Private Keys and Passwords Backup B-12
EAP-TLS Flow in ACS 5.1 B-12
PEAPv0/1 B-14
Overview of PEAP B-14
Supported PEAP Features B-15
Server Authenticated and Unauthenticated Tunnel Establishment Modes B-15
Fast Reconnect B-15
Session Resume B-15
Protected Exchange of Arbitrary Parameters B-16
PEAP Flow in ACS 5.1 B-16
Creating the TLS Tunnel B-17
Authenticating with MSCHAPv2 B-17
EAP-FAST B-18
Overview of EAP-FAST B-18
EAP-FAST Benefits B-19
EAP-FAST in ACS 5.1 B-20
About Master-Keys B-20
About PACs B-20
Provisioning Modes B-21
Types of PACs B-21
ACS-Supported Features for PACs B-23
Master Key Generation and PAC TTLs B-25
EAP-FAST Flow in ACS 5.1. B-25
EAP-FAST PAC Management B-26
Key Distribution Algorithm B-27
EAP-FAST PAC-Opaque Packing and Unpacking B-27
Revocation Method B-27
PAC Migration from ACS 4.x B-27
EAP-MSCHAPv2 B-28
Overview of EAP-MSCHAPv2 B-28

MSCHAPv2 for User Authentication B-28
MSCHAPv2 for Change Password B-28
Windows Machine Authentication Against AD B-29
EAP- MSCHAPv2 Flow in ACS 5.1 B-29
CHAP B-29
LEAP B-29
Certificate Attributes B-30
Certificate Binary Comparison B-30
Rules Relating to Textual Attributes B-31
Certificate Revocation B-31
Machine Authentication B-32
Authentication Protocol and Identity Store Compatibility B-33

GLOSSARY

INDEX

Preface

Last Update: October 1, 2013

This guide describes how to use Cisco Secure Access Control System (ACS) 5.1.

Audience

This guide is for security administrators who use ACS, and who set up and maintain network and application security.

Document Organization

This guide contains the following chapters:

- Chapter 1, “Introducing ACS 5.1”
- Chapter 2, “Migrating from ACS 4.x to ACS 5.1”
- Chapter 3, “ACS 5.x Policy Model”
- Chapter 4, “Common Scenarios Using ACS”
- Chapter 5, “Understanding My Workspace”
- Chapter 6, “Post-Installation Configuration Tasks”
- Chapter 7, “Managing Network Resources”
- Chapter 8, “Managing Users and Identity Stores”
- Chapter 9, “Managing Policy Elements”
- Chapter 10, “Managing Access Policies”
- Chapter 11, “Monitoring and Reporting in ACS”
- Chapter 12, “Managing Alarms”
- Chapter 13, “Managing Reports”
- Chapter 14, “Troubleshooting ACS with the Monitoring & Report Viewer”
- Chapter 15, “Managing System Operations and Configuration in the Monitoring & Report Viewer”
- Chapter 16, “Managing System Administrators”
- Chapter 17, “Configuring System Operations”

- Chapter 18, “Managing System Administration Configurations”
- Chapter 19, “Understanding Logging”
- Appendix A, “AAA Protocols”
- Appendix B, “Authentication in ACS 5.1”

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

Document Conventions

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

Command descriptions use these conventions:

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

Examples use these conventions:

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

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

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

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

Documentation Updates

Table 1 lists the updates to the *User Guide for the Cisco Secure Access Control System 5.1*.

Table 1 Updates to the User Guide for the Cisco Secure Access Control System 5.1

Date	Description
10/01/2013	Fixed the following bugs: • CSCuh90646 • CSCuj24445
09/17/2012	Updated theViewing and Editing Alarms in Your Inbox, page 3 with list of all alarm messages.
02/02/2012	Fixed the bug CSCtw41634 by adding a note at the end of the section Configuring an AD Identity Store.
6/2/2011	Updated the "RSA SecurID Server" section on page 8-47.
1/19/2011	Added "TACACS+ Command Sets" section on page 9-35.
11/25/2010	Updated "Configuring an AD Identity Store" section on page 8-43 for the bug CSCtj62342.
11/24/2010	Updated "Manual PAC Provisioning" section on page B-23 for the bug CSCtj42714.
09/08/2010	Added "Machine Access Restrictions" section on page 8-41.
08/24/2010	Updated Chapter 11, "Monitoring and Reporting in ACS" with supported syslog messages.
08/20/2010	Updated the following sections: • Leveraging Cisco NAC Profiler as an External MAB Database, page 8-31. • Understanding Distributed Deployment, page 17-1.
08/16/2010	Updated the description of Username in Table 8-10.
07/01/2010	Updated the following sections: • Create an Agent Record (sdconf.rec), page 8-48 • Creating and Editing RSA SecurID Token Servers, page 8-49
06/14/2010	Added a note in the "Microsoft AD" section on page 8-38.
06/07/2010	Updated the document for the following bugs: • CSCth12870 • CSCth12958
06/03/2010	Updated the transport used for port numbers in "Understanding Distributed Deployment" section on page 17-1.
04/12/2010	Updated the description of Username in Table 8-10.
03/10/2010	Added a note on joining the AD domain in "Configuring an AD Identity Store" section on page 8-43.
02/22/2010	Added a note stating that no TAC support is available for modified python scrits in the "Downloading Sample Python Scripts" section on page 18-43.

Table 1 Updates to the User Guide for the Cisco Secure Access Control System 5.1

Date	Description
01/04/2010	Added information on ports that need to be opened in order to allow ACS to communicate with AD in Chapter 8, "Managing Users and Identity Stores."
11/30/2009	Added information on how to configure NADs to send syslog messages to the Monitoring & Report Viewer in Chapter 11, "Monitoring and Reporting in ACS".
11/11/2009	Cisco Secure Access Control System, Release 5.1.

Related Documentation

Table 1 lists a set of related technical documentation available on Cisco.com. To find end-user documentation for all products on Cisco.com, go to:

http://www.cisco.com/go/techdocs

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

Table 2 Related Documentation

Document	Location on Cisco.com
Supported and Interoperable Devices and Software Tables for the Cisco Secure Access Control System 5.1.	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/device_support/sdt51.html
Regulatory Compliance and Safety Information for Cisco 1121 Secure Access Control System 5.1 and Cisco NAC Appliance 4.7	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/regulatory/compliance/csacsrcsi.html
Release Notes for the Cisco Secure Access Control System 5.1	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/release/notes/acs_51_rn.html
Installation and Upgrade Guide for the Cisco Secure Access Control System 5.1	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/installation/guide/acs5_1_install_guide.html
Open Source Licensing Document for the Cisco Secure Access Control System 5.1	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/open_source_license/opn_src_lic_doc.html
CLI Reference Guide for the Cisco Secure Access Control System 5.1	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/command/reference/acs5_1_cli.html
Software Developer's Guide for the Cisco Secure Access Control System 5.1	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/sdkguide.html
Migration Guide for the Cisco Secure Access Control System 5.1	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/migration/guide/Migration_Book.html
License and Documentation Guide for the Cisco Secure Access Control System 5.1	http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/license_doc/guide/acs_51_lic_doc_gd.html

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually 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 a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Introducing ACS 5.1

This section contains the following topics:

- Overview of ACS, page 1-1
- ACS Distributed Deployment, page 1-2
- ACS Management Interfaces, page 1-3

Overview of ACS

ACS is a policy-based security server that provides standards-compliant Authentication, Authorization, and Accounting (AAA) services to your network. ACS facilitates the administrative management of Cisco and non-Cisco devices and applications. As a dominant enterprise network access control platform, ACS serves as an integration point for network access control and identity management.

ACS 5.x provides a rule-based policy model that allows you to control network access based on dynamic conditions and attributes. The rule-based policy is designed to meet complex access policy needs. For more information on the rule-based policy model in ACS, see Chapter 3, "ACS 5.x Policy Model."

Within the greater context of two major AAA protocols—RADIUS and TACACS+—ACS provides the following basic areas of functionality:

- Under the framework of the RADIUS protocol, ACS controls the wired and wireless access by users and host machines to the network and manages the accounting of the network resources used. ACS supports multiple RADIUS-based authentication methods that includes PAP, CHAP, MSCHAPv1, MSCHAPv2, and many members of the EAP family of protocols, such as EAP-MD5, LEAP, PEAP, EAP-FAST, and EAP-TLS. In association with PEAP or EAP-FAST, ACS also supports EAP-MSCHAPv2 and EAP-GTC. For more information on authentication methods, see Appendix B, "Authentication in ACS 5.1".
- Under the framework of the TACACS+ protocol, ACS facilitates the administrative management of Cisco and non-Cisco network devices such as switches, wireless access points, routers, and gateways, as well as of services and entities such as dialup, Virtual Private Network (VPN), and firewall.

ACS is the point in your network that identifies users and devices that try to connect to your network. This identity establishment can occur directly by using the ACS internal identity repository for local user authentication; or, by using external identity repositories. For example, ACS can use Active Directory as an external identity repository, to authenticate a user to grant the user access to the network. For more information about creating identities and supported identity services, see Chapter 8, "Managing Users and Identity Stores."

ACS provides advanced monitoring, reporting, and troubleshooting tools that help you administer and manage your ACS deployments. For more information on the monitoring, reporting, and troubleshooting capabilities of ACS, see Chapter 11, "Monitoring and Reporting in ACS.".

For more information about using ACS for device administration and network access scenarios, see Chapter 4, "Common Scenarios Using ACS."

Cisco Secure ACS:

- Enforces access policies for VPN and wireless users.
- Provides simplified device administration.
- Provides advanced monitoring, reporting, and troubleshooting tools.

ACS 5.1 offers several new features and enhancements compared to ACS 5.0. For a complete list of new and changed features, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/release/notes/acs_51_rn.html#wp71092.

Related Topics

- ACS Distributed Deployment, page 1-2
- ACS Management Interfaces, page 1-3

ACS Distributed Deployment

ACS 5.1 is delivered preinstalled on a standard Cisco Linux-based appliance, and supports a fully distributed deployment.

An ACS deployment can consist of a single instance, or multiple instances deployed in a distributed manner, where all instances in a system are managed centrally; one ACS instance becomes the *primary instance* and you can register additional ACS instances to the primary instance as *secondary instances*. All instances have the configuration for the entire deployment, which provides redundancy for configuration data.

The primary instance centralizes the configuration of the instances in the deployment. Configuration changes made in the primary instance are automatically replicated to the secondary instance. You can force a *full replication* to the secondary instance. Full replication is used when a new secondary instance is registered and in other cases when the replication gap between the secondary instance and the primary instance is significant.

Related Topic

- ACS 4.x and 5.1 Replication, page 1-2

ACS 4.x and 5.1 Replication

In ACS 4.x, you must select the database object types (or classes) you wish to replicate from primary instance to the secondary instance. When you replicate an object, a complete configuration copy is made on the secondary instance. In ACS 5.1, any configuration changes made in the primary instance are immediately replicated to the secondary instance. Only the configuration changes made *since the last replication* are propagated to the secondary instance. ACS 4.x did not provide incremental replication, only full replication, and there was service downtime for replication. ACS 5.1 provides incremental replications with no service downtime.

You can also *force* a full replication to the secondary instance if configuration changes do not replicate it. Full replication is used when a new secondary instance is registered and other cases when the replication gap between the secondary instance and the primary instance is significant.

Table 1-1 lists some of the differences between ACS 4.x and 5.1 replication.

Table 1-1 Differences Between ACS 4.x and 5.1 Replication

ACS 4.x	ACS 5.1
You can choose the data items to be replicated.	You cannot choose the data items to be replicated. All data items, by default are replicated.
Supports multi-level or cascading replication.	Supports only a fixed flat replication. Cascading replication is not supported.
Some data items such as, the external database configurations are not replicated.	All data items are replicated.

For more information about setting up a distributed deployment, see Configuring System Operations, page 17-1.

Note Network Address Translation (NAT) is not supported in ACS distributed deployment environment. That is, if a primary or secondary instance's network address is translated then the database replication may not work properly, and displays a shared secret mismatch error.

ACS Licensing Model

You must have a valid license to operate ACS; ACS prompts you to install a valid base license when you first access the web interface. Each server requires a unique base license in a distributed deployment. For information about the types of licenses you can install, see Types of Licenses, page 18-35. For more information about licenses, see Licensing Overview, page 18-35.

Related Topic

- ACS Distributed Deployment, page 1-2

ACS Management Interfaces

This section contains the following topics:

- ACS Web-Based Interface, page 1-4
- ACS Command Line Interface, page 1-4
- ACS Programmatic Interfaces, page 1-5

ACS Web-Based Interface

You can use the ACS web-based interface to fully configure your ACS deployment, and perform monitoring and reporting operations. The web interface provides a consistent user experience regardless of the particular area that you are configuring.

The ACS web interface is supported on HTTPS-enabled Microsoft Internet Explorer, versions 6 and 7, and Firefox version 3.x.

The new web interface design and organization:

- Reflects the new policy model, which is organized around the user's view of policy administration. The new policy model is easier to use, as it separates the complex interrelationships that previously existed among policy elements; for example, user groups, network device groups (NDGs), network access filters, network access profiles, and so on.
- Presents the configuration tasks in a logical order that you can follow for many common scenarios. For example, first you configure conditions and authorizations for policies in the Policy Elements drawer, and then you move on to the Policies drawer to configure the policies with the defined policy elements.
- Provides new page functionality, such as sorting and filtering lists of items.

See Chapter 5, "Using the Web Interface." for more information.

Related Topics

- ACS Command Line Interface, page 1-4

ACS Command Line Interface

You can use the ACS command-line interface (CLI), a text-based interface, to perform some configuration and operational tasks and monitoring. Access to the ACS-specific CLI requires administrator authentication by ACS 5.1. You do not need to be an ACS administrator or log into ACS 5.1 to use the non-ACS configuration mode. ACS configuration mode command sessions are logged to the diagnostics logs.

ACS 5.1 is shipped on the Cisco 1121 Secure Access Control System (CSACS 1121). The ADE-OS software supports these command modes:

- EXEC—Use these commands to perform system-level operation tasks (for example, install, start, and stop application; copy files and installations; restore backups; and display information). In addition, certain EXEC mode commands have ACS-specific abilities (for example, start an ACS instance, display and export ACS logs, and reset an ACS configuration to factory default settings). The documentation expressly calls out EXEC mode commands that provide this ability.
- ACS configuration—Use these commands to set the debug log level (enable or disable) for the ACS management and runtime components, and show system settings.
- Configuration—Use these commands to perform additional configuration tasks for the appliance server in an ADE-OS environment.

Note The CLI includes an option to reset the configuration that, when issued, resets all ACS configuration information, but retains the appliance settings such as network configuration.

For information about using the CLI, see the *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.0*.

Related Topic

- ACS Web-Based Interface, page 1-4

ACS Programmatic Interfaces

ACS 5.1 provides web services and command-line interface (CLI) commands that allow software developers and system integrators to programmatically access some ACS features and functions. ACS 5.1 also provides you access to the Monitoring & Report Viewer database that you can use to create custom applications to monitor and troubleshoot ACS.

You can use these web services and CLI commands to:

- Integrate external applications directly with ACS.
- View and modify the information stored in ACS.

The UCP web service allows users, defined in the ACS internal database, to first authenticate and then change their own password. ACS exposes the UCP web service to allow you to create custom web-based applications that you can deploy in your enterprise.

The Monitoring & Report Viewer web services allow you to create custom applications to track and troubleshoot events in ACS.

You can develop shell scripts using the CLI commands that ACS offers to perform create, read, update, and delete (CRUD) operations on ACS objects. You can also create an automated shell script to perform bulk operations.

For more information on how to access these web services and their functionalities, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/sdkguide.html.

CHAPTER 2

Migrating from ACS 4.x to ACS 5.1

ACS 4.x stores policy and authentication information, such as TACACS+ command sets, in the user and user group records. In ACS 5.1, policy and authentication information are independent shared components that you use as building blocks when you configure policies.

The most efficient way to make optimal use of the new policy model is to rebuild policies by using the building blocks, or policy elements, of the new policy model. This method entails creating appropriate identity groups, network device groups (NDGs), conditions, authorization profiles, and rules.

ACS 5.1 provides a migration utility to transfer data from migration-supported versions of ACS 4.x to an ACS 5.1 machine. The ACS 5.1 migration process requires, in some cases, administrative intervention to manually resolve data before you import it to ACS 5.1. This process is different from the process of upgrading from versions of ACS 3.x to ACS 4.x, where the ACS 4.x system works the same way as ACS 3.x and no administrative intervention is required.

The migration utility in ACS 5.1 supports multiple-instance migration that migrates all ACS 4.x servers in your deployment to ACS 5.1. For more information on multiple-instance migration, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/migration/guide/Migration_Book.html.

Upgrade refers to the process of transferring data from ACS 5.0 servers to ACS 5.1. For information on the upgrade process, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/installation/guide/csacs_upg.html.

This chapter contains the following sections:

- Overview of the Migration Process, page 2-1
- Before You Begin, page 2-3
- Downloading Migration Files, page 2-3
- Migrating from ACS 4.x to ACS 5.1, page 2-3
- Functionality Mapping from ACS 4.x to ACS 5.1, page 2-4
- Common Scenarios in Migration, page 2-7

Overview of the Migration Process

The Migration utility completes the data migration process in two phases:

- Analysis and Export
- Import

In the Analysis and Export phase, you identify the objects that you want to export into 5.1. The Migration utility analyses the objects, consolidates the data, and exports it. After the Analysis and Export phase is complete, the Migration utility generates a report that lists any data compatibility errors, which you can manually resolve to successfully import these objects into 5.1. The Analysis and Export phase is an iterative process that you can rerun many times to ensure that there are no errors in the data to be imported. After you complete the Analysis and Export phase, you can run the import phase to import data into ACS 5.1.

This section contains the following topics:

- Migration Requirements, page 2-2
- Supported Migration Versions, page 2-2

Migration Requirements

To run the Migration utility, you must deploy the following machines:

- The source ACS 4.x machine—The source machine can either be an ACS 4.x solution engine or a ACS for Windows 4.x machine. The source machine must be running a migration-supported version of ACS. See Supported Migration Versions, page 2-2 for more information.
- The migration machine—The migration machine must be a Windows platform that runs the same version of ACS (including the patch) as the source machine. The migration machine cannot be an ACS production machine or an ACS appliance machine. It has to be a Windows server running ACS for Windows. The migration machine requires 2 GB RAM.
- The target ACS 5.1 machine—Back up your ACS 5.1 configuration data and ensure that the migration interface is enabled on ACS 5.1 before you begin the import process. It is recommended that you import data into a fresh ACS 5.1 database. To enable the migration interface, from the ACS CLI, enter:

  ```
  acs config-web-interface migration enable
  ```

Supported Migration Versions

ACS 5.1 supports migration from the following ACS 4.x versions:

- ACS 4.1.1.24
- ACS 4.1.4
- ACS 4.2.0.124
- ACS 4.2.1

Note You must install the latest patch for the supported migration versions listed here. Also, if you have any other version of ACS 4.x installed, you must upgrade to one of the supported versions and install the latest patch for that version before you can migrate to ACS 5.1.

Before You Begin

Before you migrate data from ACS 4.x to ACS 5.1, ensure that you:

- Check for database corruption issues in the ACS 4.x source machine.
- Have the same ACS versions on the source and migration machines (including the patch).
- Have configured a single IP address on the migration machine.
- Take a backup of the source ACS 4.x data.
- Have full network connectivity between the migration machine and the ACS 5.1 server.
- Have enabled the migration interface on the ACS 5.1 server.
- Use only the default superadmin account for ACS 5.1, **acsadmin** while running the Migration utility.

Downloading Migration Files

To download migration application files and the migration guide for ACS 5.1:

Step 1 Select **System Administration > Downloads > Migration Utility**.

The Migration from 4.x page appears.

Step 2 Click **Migration application files**, to download the application file you want to use to run the migration utility.

Step 3 Click **Migration Guide**, to download *Migration Guide for the Cisco Secure Access Control System 5.1*.

Migrating from ACS 4.x to ACS 5.1

You can migrate data from any of the migration-supported versions of ACS 4.x to ACS 5.1. The migration utility migrates the following ACS 4.x data entities:

- Network Device Groups (NDGs)
- AAA Clients and Network Devices
- Internal Users
- User-Defined Fields (from the Interface Configuration section)
- User Groups
- Shared Shell Command Authorization Sets
- User TACACS+ Shell Exec Attributes (migrated to user attributes)
- Group TACACS+ Shell Exec Attributes (migrated to shell profiles)
- User TACACS+ Command Authorization Sets
- Group TACACS+ Command Authorization Sets
- Shared, Downloadable ACLs
- EAP-FAST Master Keys

- Shared RADIUS Authorization Components (RACs)
- RADIUS VSAs

Note The Migration utility does not migrate public key infrastructure (PKI) configuration data and does not support certificate migration.

To migrate data from ACS 4.x to ACS 5.1:

1. Upgrade the ACS 4.x version to a migration-supported version if your ACS 4.x server currently does not run one of the migration-supported versions. For a list of migration-supported ACS versions, see Supported Migration Versions, page 2-2.
2. Install the same migration-supported version of ACS on the migration machine, which is a Windows server.
3. Back up the ACS 4.x data and restore it on the migration machine.
4. Place the Migration utility on the migration machine. You can get the Migration utility from the Installation and Recovery DVD.
5. Run the Analyze and Export phase of the Migration utility on the migration machine.
6. Resolve any issues in the Analyze and Export phase.
7. Run the Import phase of the Migration utility on the migration machine.
8. The import phase imports data into the 5.1 server.

Note If you have a large internal database, then we recommend that you import the data into a standalone 5.x primary server and not to a server that is connected to several secondary servers. After data migration is complete, you can register the secondary servers to the standalone 5.x primary server.

For detailed information about using the migration utility, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/migration/guide/Migration_Book.html.

After you migrate the data, you can reconstruct your policies with the migrated objects.

Functionality Mapping from ACS 4.x to ACS 5.1

In ACS 5.1, you define authorizations, shell profiles, attributes, and other policy elements as independent, reusable objects, and not as part of the user or group definition.

Table 2-1 describes where you configure identities, network resources, and policy elements in ACS 5.1. Use this table to view and modify your migrated data identities. See Chapter 3, "ACS 5.x Policy Model" for an overview of the ACS 5.1 policy model.

Table 2-1 Functionality Mapping from ACS 4.x to ACS 5.1

To configure...	In ACS 4.x, choose...	In ACS 5.1, choose...	Additional information for 5.1
Network device groups	Network Configuration page	Network Resources > Network Device Groups See Creating, Duplicating, and Editing Network Device Groups, page 7-2.	You can use NDGs as conditions in policy rules. (ACS 5.1 does not support NDG shared password. After migration, member devices contain the NDG shared password information.)
Network devices and AAA clients	Network Configuration page	Network Resources > Network Devices and AAA Clients See Network Devices and AAA Clients, page 7-5.	—
User groups	Group Setup page	Users and Identity Stores > Identity Groups See Managing Identity Attributes, page 8-7.	You can use identity groups as conditions in policy rules.
Internal users	User Setup page	Users and Identity Stores > Internal Identity Stores > Users See Managing Internal Identity Stores, page 8-4.	ACS 5.1 authenticates internal users against the internal identity store only. Migrated users that used an external database for authentication have a default authentication password that they must change on first access.
Internal hosts	Network Access Profiles > Authentication	Users and Identity Stores > Internal Identity Stores > Hosts See Creating Hosts in Identity Stores, page 8-15.	You can use the internal hosts in identity policies for Host Lookup.
Identity attributes (user-defined fields)	Interface Configuration > User Data Configuration	System Administration > Configuration > Dictionaries > Identity > Internal Users See Managing Dictionaries, page 18-5.	Defined identity attribute fields appear in the User Properties page; you can use them as conditions in access service policies.
Command sets (command authorization sets)	One of the following: • Shared Profile Components > Command Authorization Set • User Setup page • Group Setup page	Policy Elements > Authorization and Permissions > Device Administration > Command Set See Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-29.	You can add command sets as results in authorization policy rules in a device administration access service.

Table 2-1 Functionality Mapping from ACS 4.x to ACS 5.1 (continued)

To configure...	In ACS 4.x, choose...	In ACS 5.1, choose...	Additional information for 5.1
Shell exec parameters	User Setup page	System Administration > Dictionaries > Identity > Internal Users See Managing Dictionaries, page 18-5.	Defined identity attribute fields appear in the User Properties page; you can use them as conditions in access service policies.
Shell profiles (shell exec parameters or shell command authorization sets)	Group Setup page	Policy Elements > Authorization and Permissions > Device Administration > Shell Profile See Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24.	You can add shell profiles as results in authorization policy rules in a device administration access service.
Date and time condition (Time of Day Access) **Note** You cannot migrate the date and time conditions. You have to recreate them in ACS 5.1.	Group Setup page	Policy Elements > Session Conditions > Date and Time See Creating, Duplicating, and Editing a Date and Time Condition, page 9-3.	You can add date and time conditions to a policy rule in the Service Selection policy or in an authorization policy in an access service.
RADIUS Attributes	One of the following: • Shared Profile Components > RADIUS Authorization Component • User Setup page • Group Setup page **Note** You cannot migrate the RADIUS attributes from user and group setups. You have to recreate them in ACS 5.1.	Policy Elements > Authorization and Permissions > Network Access > Authorization Profile > Common Tasks tab or Policy Elements > Authorization and Permissions > Network Access > Authorization Profile > RADIUS Attributes tab See Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18.	You configure RADIUS attributes as part of a network access authorization profile. You can add authorization profiles as results in an authorization policy in a network access service.

Table 2-1 Functionality Mapping from ACS 4.x to ACS 5.1 (continued)

To configure...	In ACS 4.x, choose...	In ACS 5.1, choose...	Additional information for 5.1
Downloadable ACLs	Shared Profile Components	Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs See Creating, Duplicating, and Editing Downloadable ACLs, page 9-32.	You can add downloadable ACLs (DACLs) to a network access authorization profile. After you create the authorization profile, you can add it as a result in an authorization policy in a network access service.
RADIUS VSA	Interface Configuration	System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA. See Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-6.	You configure RADIUS VSA attributes as part of a network access authorization profile. You can add authorization profiles as results in an authorization policy in a network access service.

Common Scenarios in Migration

The following are some of the common scenarios that you encounter while migrating to ACS 5.1:

- Migrating from ACS 4.2 on CSACS 1120 to ACS 5.1, page 2-7
- Migrating from ACS 3.x to ACS 5.1, page 2-8
- Migrating Data from Other AAA Servers to ACS 5.1, page 2-8

Migrating from ACS 4.2 on CSACS 1120 to ACS 5.1

In your deployment, if you have ACS 4.2 on CSACS 1120 and you would like to migrate to ACS 5.1, you must do the following:

1. Install Cisco Secure Access Control Server 4.2 for Windows on the migration machine.
2. Back up the ACS 4.2 data on CSACS 1120.
3. Restore the data in the migration machine.
4. Run the Analysis and Export phase of the Migration utility on the migration machine.
5. Install ACS 5.1 on CSACS 1120.
6. Import the data from the migration machine to the CSACS 1120 that has ACS 5.1 installed.

Refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/migration/guide/Migration_Book.html for a detailed description of each of these steps.

Migrating from ACS 3.x to ACS 5.1

If you have ACS 3.x deployed in your environment, you cannot directly migrate to ACS 5.1. You must do the following:

1. Upgrade to a migration-supported version of ACS 4.x. See Supported Migration Versions, page 2-2 for a list of supported migration versions.
2. Check the upgrade paths for ACS 3.x:

   For the ACS Solution Engine, refer to:
   http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.1/installation/guide/solution_engine/upgap.html#wp1120037

   For ACS for Windows, refer to:

   http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/install.html#wp1102849
3. Upgrade your ACS 3.x server to a migration-supported version of ACS 4.x.
4. After the upgrade, follow the steps that describe migrating from ACS 4.x to ACS 5.1. Refer to the *Migration Guide for the Cisco Secure Access Control System 5.1* for more information.

Migrating Data from Other AAA Servers to ACS 5.1

ACS 5.1 allows you to perform bulk import of various ACS objects through the ACS web interface and the CLI. You can import the following ACS objects:

- Users
- Hosts
- Network Devices
- Identity Groups
- NDGs
- Downloadable ACLs
- Command Sets

ACS allows you to perform bulk import of data with the use of a comma-separated values (.csv) file. You must input data in the .csv file in the format that ACS requires. ACS provides a .csv template for the various objects that you can import to ACS 5.1. You can download this template from the web interface.

To migrate data from other AAA servers to ACS 5.1:

1. Input data into .csv files. For more information on understanding .csv templates, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/cli_imp_exp.html#wp1055255.
2. Set up your ACS 5.1 appliance.
3. Perform bulk import of data into ACS 5.1.

   For more information on performing bulk import of ACS objects, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/cli_imp_exp.html#wp1052831.

The data from your other AAA servers is now available in ACS 5.1.

CHAPTER 3

ACS 5.x Policy Model

ACS 5.x is a policy-based access control system. The term *policy model* in ACS 5.x refers to the presentation of policy elements, objects, and rules to the policy administrator. ACS 5.x uses a rule-based policy model instead of the group-based model used in the 4.x versions.

This section contains the following topics:

- Overview of the ACS 5.x Policy Model, page 3-1
- Access Services, page 3-5
- Service Selection Policy, page 3-11
- Authorization Profiles for Network Access, page 3-16
- Policies and Identity Attributes, page 3-16
- Policies and Network Device Groups, page 3-17
- Example of a Rule-Based Policy, page 3-17
- Flows for Configuring Services and Policies, page 3-18

Note See Functionality Mapping from ACS 4.x to ACS 5.1, page 2-4 for a mapping of ACS 4.x concepts to ACS 5.0.

Overview of the ACS 5.x Policy Model

The ACS 5.x rule-based policy model provides more powerful and flexible access control than is possible with the older group-based approach.

In the older group-based model, a *group* defines policy because it contains and ties together three types of information:

- Identity information—This information can be based on membership in AD or LDAP groups or a static assignment for internal ACS users.
- Other restrictions or conditions—Time restrictions, device restrictions, and so on.
- Permissions—VLANs or Cisco IOS privilege levels.

The ACS 5.x policy model is based on *rules* of the form:

If <*condition*> then <*result*>

For example, we use the information described for the group-based model:

If <*identity-condition, restriction-condition*> then <*authorization-profile*>

In ACS 5.1, you define conditions and results as global, shared objects. You define them once and then reference them when you create rules. ACS 5.1 uses the term *policy elements* for these shared objects, and they are the building blocks for creating rules.

Table 3-1 shows how the various policy elements define all the information that the old group contained.

Table 3-1 Information in Policy Elements

Information in ACS 4.x Group	Information in ACS 5.1 Policy Element
Identity information	• AD group membership and attributes • LDAP group membership and attributes • ACS internal identity groups and attributes
Other policy conditions	• Time and date conditions • Custom conditions
Permissions	Authorization profiles

A *policy* is a set of rules that ACS 5.x uses to evaluate an access request and return a decision. For example, the set of rules in an:

- *Authorization policy* return the authorization decision for a given access request.
- *Identity policy* decide how to authenticate and acquire identity attributes for a given access request.

ACS 5.x organizes the sequence of independent policies (a policy workflow) into an *access service*, which it uses to process an access request. You can create multiple access services to process different kinds of access requests; for example, for device administration or network access. For more information, see Access Services, page 3-5.

You can define simple policies and rule-based policies. Rule-based policies are complex policies that test various conditions. Simple policies apply a single result to all requests without any conditions.

There are various types of policies:

For more information on the different types of policies, see Types of Policies, page 3-4.

For more information about policy model terminology, see Policy Terminology, page 3-3.

Related Topics

- Policies and Identity Attributes, page 3-16
- Flows for Configuring Services and Policies, page 3-18

Policy Terminology

Table 3-2 describes the rule-based policy terminology.

Table 3-2 Rule-Based Policy Terminology

Term	Description
Access service	A sequential set of policies used to process access requests. ACS 5.x allows you to define multiple access services to support multiple, independent, and isolated sets of policies on a single ACS system. There are two default access services: one for device administration (TACACS+ based access to the device shell or CLI) and one for network access (RADIUS-based access to network connectivity).
Policy element	Global, shared object that defines policy conditions (for example, time and date, or custom conditions based on user-selected attributes) and permissions (for example, authorization profiles). The policy elements are referenced when you create policy rules.
Authorization profile	The basic "permissions container" for a RADIUS-based network access service, which is where you define all permissions to be granted for a network access request. VLANs, ACLs, URL redirects, session timeout or reauthorization timers, or any other RADIUS attributes to be returned in a response, are defined in the authorization profile.
Shell profile	The basic "permissions container" for TACACS+ based device administration policy, which is where you define permissions to be granted for a shell access request. IOS privilege level, session timeout, and so on are defined in the shell profile.
Command set	Contains the set of permitted commands for TACACS+ based, per-command authorization.
Policy	A set of rules that are used to reach a specific policy decision (for example, how to authenticate and what authorization to grant). For those policies that have a default rule, a policy is a "first-match" rules table with a default rule for any request which does not match any user-created rules.
Identity policy	ACS 5.1 policy for choosing how to authenticate and acquire identity attributes for a given request. ACS 5.1 allows two types of identity policies: a simple, static policy, or a rules-based policy for more complex situations.
Identity group mapping policy	Optional policy for mapping identity information collected from identity stores (for example, group memberships and user attributes) to a single ACS identity group. This can help you "normalize" identity information and map requests to a single identity group, which is just a tag, an identity classification ("everyone like this"). The identity group can be used as a condition in authorization policy, if desired.
Authorization policy	ACS 5.1 policy for assigning authorization attributes for access requests. Authorization policy selects a single rule and populates the response with the contents of the authorization profiles referenced as the "result" of the rule.
Exception policy	A special option for authorization policy, which allows you to define separately the set of conditions and authorization results for authorization policy exceptions and waivers. If defined, the exception policy is checked before the main ("standard") authorization policy.
Default rule	A "catchall" rule in ACS 5.1 policies. You can edit this rule to specify a default result or authorization action, and it serves as the policy decision in cases where a given request fails to match the conditions specified in any user-created rule.

Simple Policies

You can configure all of your ACS policies as rule-based policies. However, in some cases, you can choose to configure a simple policy, which selects a single result to apply to all requests without conditions. For example, you can define a rule-based authentication policy with a set of rules for different conditions; or, if you want to use the internal database for all authentications, you can define a simple policy.

Table 3-3 helps you determine whether each policy type can be configured as a simple policy.

If you create and save a simple policy, and then change to a rule-based policy, the simple policy becomes the default rule of the rule-based policy. If you have saved a rule-based policy and then change to a simple policy, ACS automatically uses the default rule as the simple policy.

Related Topic

- Types of Policies, page 3-4

Rule-Based Policies

Rule-based policies have been introduced to overcome the challenges of identity-based policies. In earlier versions of ACS, although membership in a user group gives members access permissions, it also places certain restrictions on them. When a user requests access, the user's credentials are authenticated using an identity store, and the user is associated with the appropriate user group. Because authorization is tied to user group, all members of a user group have the same access restrictions and permissions at all times. With this type of policy (the simple policy), permissions are granted based on a user's association with a particular user group, which is useful in situations in which the user's identity is the only dominant condition. However, for users who need different permissions under different conditions, this policy does not work.

In ACS 5.x, you can create rules based on various conditions apart from identity. The user group no longer contains all of the information. For example, if you want to grant an employee full access while working on campus, and restricted access while working remotely, you can do so using the rule-based policies in ACS 5.1. You can base permissions on various conditions besides identity, and permissions are no longer associated with user groups. You can use session and environment attributes, such as access location, access type, health of the end station, date, time, and so on, to determine the type of access to be granted.

Authorization is now based on a set of rules:

If <conditions> then <apply the respective permissions>

With rule-based policies, conditions can consist of any combination of available session attributes, and permissions are defined in authorization profiles. You define these authorization profiles to include VLAN, downloadable ACLs, QoS settings, and RADIUS attributes.

Types of Policies

Table 3-3 describes the types of policies that you can configure in ACS.

The policies are listed in the order of their evaluation; any attributes that a policy retrieves can be used in any policy listed subsequently. The only exception is the Identity group mapping policy, which uses only attributes from identity stores.

Table 3-3 ACS Policy Types

Policy	Can Contain Exception Policy?	Simple[1] and Rule-Based?	Available Dictionaries for Conditions	Available Result Types	Attributes Retrieved
Service Selection Determines the access service to apply to an incoming request.	No	Yes	All except identity store related	Access Service	—
Identity Determines the identity source for authentication.	No	Yes	All except identity store related	Identity Source, Failure options	Identity Attributes; Identity Group for internal ID stores
Identity Group Mapping Defines mapping attributes and groups from external identity stores to ACS identity groups.	No	Yes	Only identity store dictionaries	Identity Group	Identity Group for external ID stores
Network Access Authorization Determines authorization and permissions for network access.	Yes	Rule-based only	All dictionaries	Authorization Profile, Security Group for TrustSec	—
Device Administration Authorization Determines authorization and permissions for device administration.	Yes	Rule-based only	All dictionaries	Shell Profile, Command Set	—

1. A simple policy specifies a single set of results that ACS applies to all requests; it is in effect a one-rule policy.

Access Services

Access services are fundamental constructs in ACS 5.x that allow you to configure access policies for users and devices that connect to the network and for network administrators who administer network devices. In ACS 5.x, authentication and authorization requests are processed by access services. An access service consists of the following elements:

- Identity Policy—Specifies how the user should be authenticated and includes the allowed authentication protocols and the user repository to use for password validation.
- Group Mapping Policy—Specifies if the user's ACS identity group should be dynamically established based on user attributes or group membership in external identity stores. The user's identity group can be used as part of their authorization.
- Authorization Policy—Specifies the authorization rules for the user.

The access service is an independent set of policies used to process an access request.

The ACS administrator might choose to create multiple access services to allow clean separation and isolation for processing different kinds of access requests. ACS provides two default access services:

- Default Device Admin—Used for TACACS+ based access to device CLI
- Default Network Access—Used for RADIUS-based access to network connectivity

You can use the access services as is, modify them, or delete them as needed. You can also create additional access services.

The TACACS+ protocol separates authentication from authorization; ACS processes TACACS+ authentication and authorization requests separately. Table 3-4 describes additional differences between RADIUS and TACACS+ access services.

Table 3-4 Differences Between RADIUS and TACACS+ Access Services

Policy Type	TACACS+	RADIUS
Identity	Optional[1]	Required
Group Mapping	Optional	Optional
Authorization	Optional[1]	Required

1. For TACACS+, you must select either Identity or Authorization.

For TACACS+, all policy types are optional; however, you must choose at least one policy type in a service. If you do not define an identity policy for TACACS+, ACS returns authentication failed for an authentication request. Similarly, if you do not define an authorization policy, if ACS receives a session or command authorization request, it fails. For both RADIUS and TACACS+ access services, you can modify the service to add policies after creation.

Note Access services do not contain the service selection policy. Service selection rules are defined independently.

You can maintain and manage multiple access services; for example, for different use cases, networks, regions, or administrative domains. You configure a service selection policy, which is a set of service selection rules to direct each new access request to the appropriate access service.

Table 3-5 describes an example of a set of access services.

Table 3-5 Access Service List

Access Service A for Device Administration	Access Service B for Access to 802.1X Agentless Hosts	Access Service C for Access from 802.1X Wired and Wireless Devices
Identity Policy A	Identity Policy B	Identity Policy C
Shell/Command Authorization Policy A	Session Authorization Policy B	Session Authorization Policy C

Table 3-6 describes a service selection policy.

Table 3-6 Service Selection Policy

Rule Name	Condition	Result
DevAdmin	protocol = TACACS+	Access Service A
Agentless	Host Lookup = True	Access Service C
Default	—	Access Service B

If ACS 5.1 receives a TACACS+ access request, it applies Access Service A, which authenticates the request according to Identity Policy A, and then applies authorizations and permissions according to the shell/command authorization policy. This service handles all TACACS+ requests.

If ACS 5.1 receives a RADIUS request that it determines is a host lookup (for example, the RADIUS service-type attribute is equal to *call-check*), it applies Access Service C, which authenticates according to Identity Policy C, and applies a session authorization profile according to Session Authorization Policy C. This service handles all host lookup requests (also known as MAC Auth Bypass requests).

Access Service B handles other RADIUS requests. This access service authenticates according to Identity Policy B and applies Session Authorization Policy B. This service handles all RADIUS requests except for host lookups, which are handled by the previous rule.

Access Service Templates

ACS contains predefined access services that you can use as a template when creating a new service. When you choose an access service template, ACS creates an access service that contains a set of policies, each with a customized set of conditions. You can change the structure of the access service by adding or removing a policy from the service, and you can change the structure of a policy by modifying the set of policy conditions. See Configuring Access Services Templates, page 10-19, for a list of the access service templates and descriptions.

RADIUS Proxy Services

ACS 5.1 can function both as a RADIUS and RADIUS proxy server. When it acts as a proxy server, ACS receives authentication and accounting requests from the NAS and forwards the requests to the external RADIUS server. ACS accepts the results of the requests and returns them to the NAS. You must configure the external RADIUS servers in ACS for ACS to forward requests to them. You can define the timeout period and the number of connection attempts.

The ACS proxy remote target is a list of remote RADIUS servers that contain the following parameters:

- IP
- Authentication port
- Accounting port
- Shared secret
- Reply timeout
- Number of retries

The following information is available in the proxy service:

- Remote RADIUS servers list
- Accounting proxy local/remote/both
- Strip username prefix/suffix

When a RADIUS proxy server receives a request, it forwards it to the first remote RADIUS server in the list. If the proxy server does not receive a response within the specified timeout interval and the specified number of retries, it forwards the request to the next RADIUS server in the list. When the first response arrives from any of the remote RADIUS servers in the list, the proxy service processes it. If the response is valid, ACS sends the response back to the NAS.

Table 3-7 lists the differences in RADIUS proxy service between ACS 4.2 and 5.1 releases.

Table 3-7 Differences in RADIUS Proxy Service Between ACS 4.2 and 5.1

Feature	ACS 5.1	ACS 4.2
Configurable timeout	Yes	No
Configurable retry count	Yes	No
Proxy cycles detection	Yes	No
Username stripping	Yes	Yes
Accounting proxy (local, remote, or both)	Yes	Yes
Account delay timeout support	No	No

ACS can simultaneously act as a proxy server to multiple external RADIUS servers. For ACS to act as a proxy server, you must configure a RADIUS proxy service in ACS. See Configuring General Access Service Properties, page 10-14 for information on how to configure a RADIUS proxy service.

For more information on proxying RADIUS requests, see RADIUS Proxy Requests, page 4-27.

Related Topics

- Policy Terminology, page 3-3
- Types of Policies, page 3-4
- Flows for Configuring Services and Policies, page 3-18

Identity Policy

Two primary mechanisms define the mechanism and source used to authenticate requests:

- Password-based—Authentication is performed against databases after the user enters a username and password. Hosts can bypass this authentication by specifying a MAC address. However, for identity policy authentication, host lookup is also considered to be password-based.
- Certificate-based—A client presents a certificate for authentication of the session. In ACS 5.1, certificate-based authentication occurs when the EAP-TLS protocol is selected.

In addition, databases can be used to retrieve attributes for the principal in the request.

The identity source is one result of the identity policy and can be one of the following types:

- Deny Access—Access to the user is denied and no authentication is performed.
- Identity Database—Single identity database. When a single identity database is selected as the result of the identity policy, either an external database (LDAP or AD) or an internal database (users or hosts) is selected as the result. The database selected is used to authenticate the user/host and to retrieve any defined attributes stored for the user/host in the database.

- Certificate Authentication Profile—Contains information about the structure and content of the certificate, and specifically maps certificate attribute to internal username. For certificate-based authentication, you must select a certificate authentication profile. For certificate based requests, the entity which identifies itself with a certificate holds the private key that correlates to the public key stored in the certificate. The certificate authentication profile extends the basic PKI processing by defining the following:
  - The certificate attribute used to define the username. You can select a subset of the certificate attributes to populate the *username* field for the context of the request. The username is then used to identify the user for the remainder of the request, including the identification used in the logs.
  - The LDAP or AD database to use to verify the revocation status of the certificate. When you select an LDAP or AD database, the certificate data is retrieved from the LDAP or AD database and compared against the data entered by the client in order to provide additional verification of the client certificate.
- Identity Sequence—Sequences of the identity databases. The sequence is used for authentication and, if specified, an additional sequence is used to retrieve attributes only. You can select multiple identity methods as the result of the identity policy. You define the identity methods in an identity sequence object, and the methods included within the sequence may be of any type.

  There are two components to an identity sequence: one for authentication, and one for attribute retrieval. The administrator can select to perform authentication based on a certificate or an identity database or both. If you choose to perform authentication based on a certificate, ACS selects a single certificate authentication profile. If you choose to perform authentication based on an identity database, you must define a list of databases to be accessed in sequence until authentication succeeds. When authentication succeeds, any defined attributes within the database are retrieved.

  In addition, you can define an optional list of databases from which additional attributes are retrieved. These additional databases can be accessed irrespective of whether password- or certificate-based authentication was used. When certificate-based authentication is used, the username field is populated from a certificate attribute and is used to retrieve attributes. All databases defined in the list are accessed and, in cases where a matching record for the user is found, the corresponding attributes, are retrieved.

  Attributes can be retrieved for a user even if the user's password is marked that it needs to be changed or if the user account is disabled. Even when you disable a user's account, the user's attributes are still available as a source of attributes, but not for authentication.

Failure Options

If a failure occurs while processing the identity policy, the failure can be one of three main types:

- Authentication failed—ACS received an explicit response that the authentication failed. For example, the wrong username or password was entered, or the user was disabled.
- User/host not found—No such user/host was found in any of the authentication databases.
- Process failed—There was a failure while accessing the defined databases.

All failures returned from an identity database are placed into one of the types above. For each type of failure, you can configure the following options:

- Reject—ACS sends a reject reply.
- Drop—No reply is returned.
- Continue—ACS continues processing to the next defined policy in the service.

The *Authentication Status* system attribute retains the result of the identity policy processing. If you select to continue policy processing in the case of a failure, this attribute can be referred to as a condition in subsequent policy processing to distinguish cases in which identity policy processing did not succeed.

Because of restrictions on the underlying protocol being used, there are cases in which it is not possible to continue processing even if you select the Continue option. This is the case for PEAP, LEAP, and EAP-FAST; even if you select the Continue option, the request is rejected.

The following default values are used for the failure options when you create rules:

- Authentication failed—The default is *reject*.
- User/host not found—The default is *reject*.
- Process failure—The default is *drop*.

Group Mapping Policy

The identity group mapping policy is a standard policy. Conditions can be based on attributes or groups retrieved from the external attribute stores only, or from certificates, and the result is an identity group within the identity group hierarchy.

If the identity policy accesses the internal user or host identity store, then the identity group is set directly from the corresponding user or host record. This processing is an implicit part of the group mapping policy. Therefore, as part of processing in the group mapping policy, the default rule is only applied if both of the following conditions are true:

- None of the rules in the group mapping table match.
- The identity group is not set from the internal user or host record.

The results of the group mapping policy are stored in the **IdentityGroup** attribute in the System Dictionary and you can include this attribute in policies by selecting the Identity Group condition.

Authorization Policy for Device Administration

Shell profiles determine access to the device CLI; command sets determine TACACS+ per command authorization. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets.

Processing Rules with Multiple Command Sets

It is important to understand how ACS processes the command in the access request when the authorization policy includes rules with multiple command sets. When a rule result contains multiple command sets, and the rule conditions match the access request, ACS processes the command in the access request against each command set in the rule:

1. If a command set contains a match for the command and its arguments, and the match has *Deny Always*, ACS designates the command set as *Commandset-DenyAlways*.
2. If there is no *Deny Always* for a command match in a command set, ACS checks all the commands in the command set sequentially for the first match. If the first match has *Permit*, ACS designates the command set as *Commandset-Permit*. If the first match has *Deny*, ACS designates the command set as *Commandset-Deny.*
3. If there is no match and "Permit any command that is not in the table below" is not checked (default,) ACS designates the command set as *Commandset-Deny.*

4. If there is no match and "Permit any command that is not in the table below" is checked, ACS designates the command set as *Commandset-Permit*.
5. After ACS has analyzed all the command sets, it authorizes the command:
   a. If ACS designated any command set as *Commandset-DenyAlways*, ACS denies the command.
   b. If there is no *Commandset-DenyAlways*, ACS permits the command if any command set is *Commandset-Permit*; otherwise, ACS denies the command.

Related Topics

- Policy Terminology, page 3-3
- Authorization Profiles for Network Access, page 3-16

Exception Authorization Policy Rules

A common real-world problem is that, in day-to-day operations, you often need to grant policy waivers or policy exceptions. A specific user might need special access for a short period of time; or, a user might require some additional user permissions to cover for someone else who is on vacation.

In ACS, you can define an exception policy for an authorization policy. The exception policy contains a separate set of rules for policy exception and waivers, which are typically ad hoc and temporary. The exception rules override the rules in the main rule table. The exception rules can use a different set of conditions and results from those in the main policy. For example, the main policy might use Identity Group and Location as its conditions, while its related exception policy might use different conditions; by default, exception policies use a compound condition and a time and date condition. The time and date condition is particularly valuable if you want to make sure your exception rules have a definite starting and ending time.

An exception policy takes priority over the main policy. The exception policy does not require its own default rule; if there is no match in the exception policy, the main policy applies, which has its own default rule.

You can use an exception to address a temporary change to a standard policy. For example, if an administrator, *John*, in one group is on vacation, and an administrator, *Bob*, from another group is covering for him, you can create an exception rule that will give *Bob* the same access permissions as *John* for the vacation period.

Related Topics

- Policy Terminology, page 3-3
- Policy Conditions, page 3-15
- Policy Results, page 3-15
- Policies and Identity Attributes, page 3-16

Service Selection Policy

When ACS receives various access requests, it uses a service selection policy to process the request. ACS provides you two modes of service selection:

- Simple Service Selection, page 3-12
- Rules-Based Service Selection, page 3-12

Simple Service Selection

In the simple service selection mode, ACS processes all AAA requests with just one access service and does not actually select a service.

Rules-Based Service Selection

In the rules-based service selection mode, ACS decides which access service to use based on various configurable options. Some of them are:

- AAA Protocol—The protocol used for the request, TACACS+ or RADIUS.
- Request Attributes—RADIUS or TACACS+ attributes in the request.
- Date and Time—The date and time ACS receives the request.
- Network Device Group—The network device group that the AAA client belongs to.
- ACS Server—The ACS server that receives this request.
- AAA Client—The AAA client that sent the request.
- Network condition objects—The network conditions can be based on
  - End Station—End stations that initiate and terminate connections.
  - Device—The AAA client that processes the request.
  - Device Port—In addition to the device, this condition also checks for the port to which the end station is associated with.

For more information on policy conditions, see Managing Policy Conditions, page 9-1.

ACS comes preconfigured with two default access services: Default Device Admin and Default Network Access. The rules-based service selection mode is configured to use the AAA protocol as the selection criterion and hence when a TACACS+ request comes in, the Default Device Admin service is used and when a RADIUS request comes in, the Default Network Access service is used.

Access Services and Service Selection Scenarios

ACS allows an organization to manage its identity and access control requirements for multiple scenarios, such as wired, wireless, remote VPN, and device administration. The access services play a major role in supporting these different scenarios. Access services allow the creation of distinct and separate network access policies to address the unique policy requirements of different network access scenarios. With distinct policies for different scenarios, you can better manage your organization's network.

For example, the default access services for device administration and network access reflect the typical distinction in policy that is required for network administrators accessing network devices and an organization's staff accessing the company’s network. However, you can create multiple access services to distinguish the different administrative domains. For example, wireless access in the Asia Pacific regions can be administered by a different team than the one that manages wireless access for European users. This situation calls for the following access services:

- APAC-wireless—Access service for wireless users in the Asia Pacific region.
- Europe-wireless—Access service for wireless users in the European countries.

You can create additional access services to reduce complexity in policies within a single access service by creating the complex policy among multiple access services. For example, if a large organization wishes to deploy 802.1x network access, it can have the following access services:

- 802.1x—For machine, user password, and certificate-based authentication for permanent staff.
- Agentless Devices—For devices that do not have an EAP supplicant, such as phones and printers.
- Guest Access—For users accessing guest wireless networks.

In this example, instead of creating the network access policy for 802.1x, agentless devices, and guest access in one access service, the policy is divided into three access services.

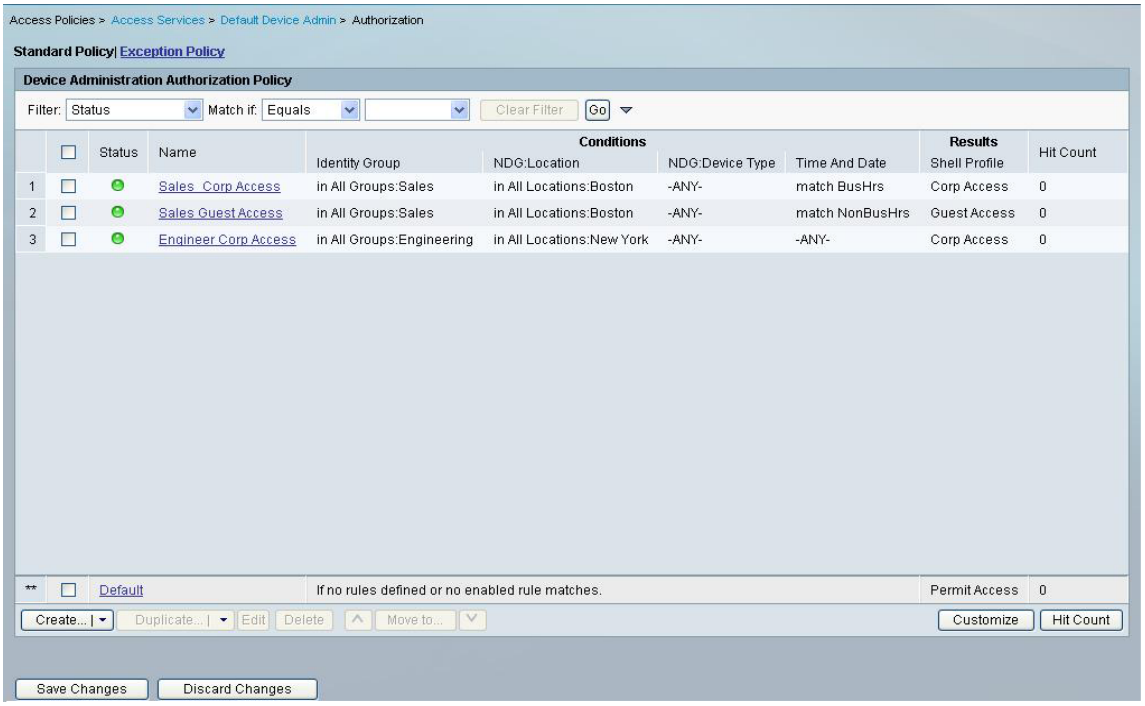
First-Match Rule Tables

ACS 5.1 provides policy decisions by using first-match rule tables to evaluate a set of rules. Rule tables contain conditions and results. Conditions can be either simple or compound. Simple conditions consist of attribute operator value and are either true or false. Compound conditions contain more complex conditions combined with AND or OR operators. See Policy Conditions, page 3-15 for more information.

The administrator selects simple conditions to be included in a policy. The conditions are displayed as columns in a rule table where the column headings are the condition name, which is usually the name of the attribute. The rules are displayed under the column headings, and each cell indicates the operator and value that are combined with the attribute to form the condition. If *ANY* appears in a cell, it indicates that no operations or comparisons are performed on that attribute.

Figure 3-1 shows a column-based rule table with defined condition types.

Figure 3-1 Example Policy Rule Table



Column	Description
Status	You can define the status of a rule as enabled, disabled, or monitored: • Enabled—ACS evaluates an enabled rule, and when the rule conditions match the access request, ACS applies the rule result. • Disabled—The rule appears in the rule table, but ACS skips this rule and does not evaluate it. • Monitor Only—ACS evaluates a monitored rule. If the rule conditions match the access request, ACS creates a log record with information relating to the match. ACS does not apply the result, and the processing continues to the following rules. Use this status during a running-in period for a rule to see whether it is needed.
Name	A descriptive name. You can specify any name that describes the rule's purpose. By default, ACS generates rule name strings <rule-number>.
Conditions	
Identity Group	In this example, this is matching against one of the internal identity groups.
NDG: Location	Location network device group. The two predefined NDGs are Location and Device Type.
Results	
Shell Profile	The shell profile is used for device administration-type policies and contains permissions for TACACS+ shell access request, such as Cisco IOS privilege level.
Hit Counts	Displays the number of times a rule matched an incoming request since the last reset of the policy's hit counters. ACS counts hits for any monitored or enabled rule whose conditions all matched an incoming request. Hit counts for: • Enabled rules reflect the matches that occur when ACS processes requests. • Monitored rules reflect the counts that would result for these rules if they were enabled when ACS processed the requests. The primary server in an ACS deployment displays the hit counts, which represent the total matches for each rule across all servers in the deployment. On a secondary server, all hit counts in policy tables appear as zeroes.

The default rule specifies the policy result that ACS uses when no other rules exist, or when the attribute values in the access request do not match any rules.

ACS evaluates a set of rules in the first-match rule table as follows:

1. ACS compares the values of the attributes associated with the current access request with a set of conditions expressed in a rule.
2. If the attribute values do not match the conditions, ACS proceeds to the next rule in the rule table.
3. If the attribute values match the conditions, ACS applies the result that is specified for that rule, and ignores all remaining rules.
4. If the attribute values do not match any of the conditions, ACS applies the result that is specified for the policy default rule.

Related Topics

- Policy Terminology, page 3-3
- Policy Conditions, page 3-15
- Policy Results, page 3-15
- Exception Authorization Policy Rules, page 3-11

Policy Conditions

You can define simple conditions in rule tables based on attributes in:

- Customizable conditions—You can create custom conditions based on protocol dictionaries and identity dictionaries that ACS knows about. You define custom conditions in a policy rule page; you cannot define them as separate condition objects.
- Standard conditions—You can use standard conditions, which are based on attributes that are always available, such as device IP address, protocol, and username-related fields.

Related Topics

- Policy Terminology, page 3-3
- Policy Results, page 3-15
- Exception Authorization Policy Rules, page 3-11
- Policies and Identity Attributes, page 3-16

Policy Results

Policy rules include result information depending on the type of policy. You define policy results as independent shared objects; they are not related to user or user group definitions.

For example, the policy elements that define authorization and permission results for authorization policies include:

- Identity source and failure options as results for identity policies. See Authorization Profiles for Network Access, page 3-16.
- Identity groups for group mapping. See Group Mapping Policy, page 3-10.
- Authorization Profiles for Network Access, page 3-16.
- Authorization Policy for Device Administration, page 3-10.
- Security groups and security group access control lists (ACLs) for Cisco TrustSec. See ACS and Cisco TrustSec, page 4-22.

For additional policy results, see Managing Authorizations and Permissions, page 9-18.

Related Topics

- Policy Terminology, page 3-3
- Policy Conditions, page 3-15
- Exception Authorization Policy Rules, page 3-11
- Policies and Identity Attributes, page 3-16

Authorization Profiles for Network Access

Authorization profiles define the set of RADIUS attributes that ACS returns to a user after successful authorization. The access authorization information includes authorization privileges and permissions, and other information such as downloadable ACLs.

You can define multiple authorization profiles as a network access policy result. In this way, you maintain a smaller number of authorization profiles, because you can use the authorization profiles in combination as rule results, rather than maintaining all the combinations themselves in individual profiles.

Processing Rules with Multiple Authorization Profiles

A session authorization policy can contain rules with multiple authorization profiles. The authorization profile contains general information (name and description) and RADIUS attributes only. When you use multiple authorization profiles, ACS merges these profiles into a single set of attributes. If a specific attribute appears:

- In only one of the resulting authorization profiles, it is included in the authorization result.
- Multiple times in the result profiles, ACS determines the attribute value for the authorization result based on the attribute value in the profile that appears first in the result set. For example, if a VLAN appears in the first profile, that takes precedence over a VLAN that appears in a 2nd or 3rd profile in the list.

Note If you are using multiple authorization profiles, make sure you order them in priority order.

The RADIUS attribute definitions in the protocol dictionary specify whether the attribute can appear only once in the response, or multiple times. In either case, ACS takes the values for any attribute from only one profile, irrespective of the number of times the values appear in the response. The only exception is the Cisco attribute value (AV) pair, which ACS takes from all profiles included in the result.

Related Topics

- Policy Terminology, page 3-3
- Authorization Policy for Device Administration, page 3-10

Policies and Identity Attributes

The identity stores contain identity attributes that you can use as part of policy conditions and in authorization results. When you create a policy, you can reference the identity attributes and user attributes. This gives you more flexibility in mapping groups directly to permissions in authorization rules. When ACS processes a request for a user or host, the identity attributes are retrieved and can then be used in authorization policy conditions.

For example, if you are using the ACS internal users identity store, you can reference the identity group of the internal user or you can reference attributes of the internal user. (Note that ACS allows you to create additional custom attributes for the internal identity store records.)

If you are using an external Active Directory (AD), you can reference AD groups directly in authorization rules, and you can also reference AD user attributes directly in authorization rules. User attributes might include a user's department or manager attribute.

Related Topics

- Managing Users and Identity Stores, page 8-1
- Policy Terminology, page 3-3
- Types of Policies, page 3-4

Policies and Network Device Groups

You can reference Network device groups (NDGs) as policy conditions. When the ACS receives a request for a device, the NDGs associated with that device are retrieved and compared against those in the policy table. With this method, you can group multiple devices and assign them the same policies. For example, you can group all devices in a specific location together and assign to them the same policy.

When ACS receives a request from a network device to access the network, it searches the network device repository to find an entry with a matching IP address. When a request arrives from a device that ACS identified using the IP address, ACS retrieves all NDGs associated with the device.

Related Topics

- Managing Users and Identity Stores, page 8-1
- Policy Terminology, page 3-3
- Types of Policies, page 3-4

Example of a Rule-Based Policy

The following example illustrates how you can use policy elements to create policy rules.

A company divides its network into two regions, East and West, with network operations engineers at each site. They want to create an access policy that allows engineers:

- Full access to the network devices in their region.
- Read-only access to devices outside their region.

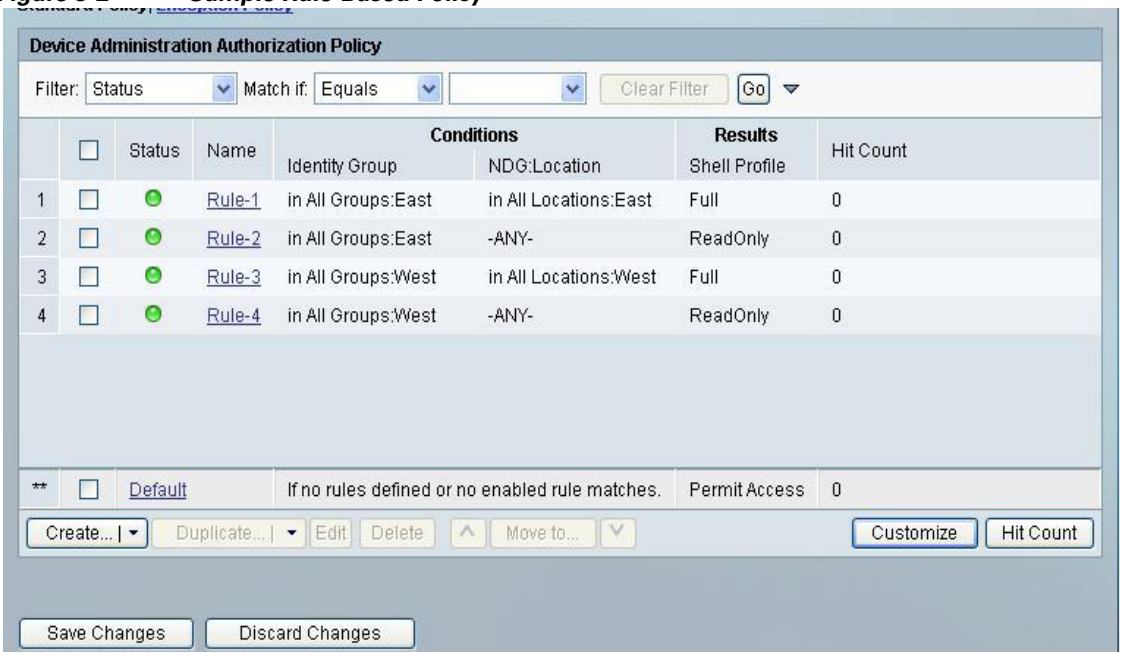
You can use the ACS 5.1 policy model to:

- Define East and West network device groups, and map network devices to the appropriate group.
- Define East and West identity groups, and map users (network engineers) to the appropriate group.
- Define Full Access and Read Only authorization profiles.
- Define Rules that allow each identity group full access or read-only access, depending on the network device group location.

Previously, you had to create two user groups, one for each location of engineers, each with separate definitions for permissions, and so on. This definition would not provide the same amount of flexibility and granularity as in the rule-based model.

Figure 3-2 illustrates what this policy rule table could look like.

Figure 3-2 Sample Rule-Based Policy



Each row in the policy table represents a single rule.

Each rule, except for the last Default rule, contains two conditions, ID Group and Location, and a result, Authorization Profile. ID Group is an identity-based classification and Location is a nonidentity condition. The authorization profiles contain permissions for a session.

The ID Group, Location, and Authorization Profile are the policy elements.

Related Topics

- Policy Terminology, page 3-3
- Types of Policies, page 3-4
- Access Services, page 3-5
- Flows for Configuring Services and Policies, page 3-18

Flows for Configuring Services and Policies

Table 3-8 describes the recommended basic flow for configuring services and policies; this flow does not include user-defined conditions and attribute configurations. With this flow, you can use NDGs, identity groups, and compound conditions in rules.

Prerequisites

Before you configure services and policies, it is assumed you have done the following:

- Added network resources to ACS and create network device groups. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 and Network Devices and AAA Clients, page 7-5.

- Added users to the internal ACS identity store or add external identity stores. See Creating Internal Users, page 8-11, Managing Identity Attributes, page 8-7, or Creating External LDAP Identity Stores, page 8-22.

Table 3-8 Steps to Configure Services and Policies

Step	Action	Drawer in Web Interface
Step 1	Define policy results: • Authorizations and permissions for device administration—Shell profiles or command sets. • Authorizations and permissions for network access—Authorization profile. See: • Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24 • Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-29 • Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18	Policy Elements
Step 2	(Optional) Define custom conditions to policy rules. You can complete this step before defining policy rules in Step 6, or you can define custom conditions while in the process of creating a rule. SeeCreating, Duplicating, and Editing a Custom Session Condition, page 9-5.	—
Step 3	Create Access Services—Define only the structure and allowed protocols; you do not need to define the policies yet. See Creating, Duplicating, and Editing Access Services, page 10-13.	Access Policies
Step 4	Add rules to Service Selection Policy to determine which access service to use for requests. See: • Customizing a Policy, page 10-5 • Creating, Duplicating, and Editing Service Selection Rules, page 10-8	Access Policies
Step 5	Define identity policy. Select the identity store or sequence you want to use to authenticate requests and obtain identity attributes. See Managing Users and Identity Stores.	Users and Identity Stores
Step 6	Create authorization rules: • Device administration—Shell/command authorization policy. • Network access—Session authorization policy. See: • Customizing a Policy, page 10-5 • Configuring Access Service Policies, page 10-20	Access Policies

Related Topics

- Policy Terminology, page 3-3
- Policy Conditions, page 3-15
- Policy Results, page 3-15
- Policies and Identity Attributes, page 3-16

CHAPTER 4

Common Scenarios Using ACS

Network control refers to the process of controlling access to a network. Traditionally a username and password was used to authenticate a user to a network. Now a days with the rapid technological advancements, the traditional method of managing network access with a username and a password is no longer sufficient. The ways in which the users can access the network and what they can access has changed considerably. Hence, you must define complex and dynamic policies to control access to your network.

For example, earlier, a user was granted access to a network and authorized to perform certain actions based on the group that he belonged to. Now, in addition to the group that the user belongs to, you must also consider other factors, such as whether:

- The user is trying to gain access within or outside of work hours.
- The user is attempting to gain access remotely.
- The user has full or restricted access to the services and resources.

Apart from users, you also have devices that attempt to connect to your network.

When users and devices try to connect to your network through network access servers, such as wireless access points, 802.1x switches, and VPN servers, ACS authenticates and authorizes the request before a connection is established.

Authentication is the process of verifying the identity of the user or device that attempts to connect to a network. ACS receives identity proof from the user or device in the form of credentials. There are two different authentication methods:

- Password-based authentication—A simpler and easier way of authenticating users. The user enters a username and password. The server checks for the username and password in its internal or external databases and if found, grants access to the user. The level of access (authorization) is defined by the rules and conditions that you have created.
- Certificate-based authentication—ACS supports certificate-based authentication with the use of the Extensible Authentication Protocol-Transport Level Security (EAP-TLS), which uses certificates for server authentication by the client and for client authentication by the server. Certificate-based authentication methods provide stronger security and are recommended when compared to password-based authentication methods.

Authorization determines the level of access that is granted to the user or device. The rule-based policy model in ACS 5.x allows you to define complex conditions in rules. ACS uses a set of rules (policy) to evaluate an access request and to return a decision. ACS organizes a sequence of independent policies into an access service, which is used to process an access request. You can create multiple access services to process different kinds of access requests; for example, for device administration or network access.

Cisco Secure Access Control System (ACS) allows you to centrally manage access to your network services and resources (including devices, such as IP phones, printers, and so on). ACS 5.1 is a policy-based access control system that allows you to create complex policy conditions and helps you to comply with the various Governmental regulations.

When you deploy ACS in your network, you must choose an appropriate authentication method that determines access to your network.

This chapter provides guidelines for some of the common scenarios. This chapter contains:

- Overview of Device Administration, page 4-2
- Password-Based Network Access, page 4-5
- Certificate-Based Network Access, page 4-8
- Agentless Network Access, page 4-11
- VPN Remote Network Access, page 4-19
- ACS and Cisco TrustSec, page 4-22
- RADIUS Proxy Requests, page 4-27

Overview of Device Administration

Device administration allows ACS to control and audit the administration operations performed on network devices, by using these methods:

- Session administration—A session authorization request to a network device elicits an ACS response. The response includes a token that is interpreted by the network device which limits the commands that may be executed for the duration of a session. See Session Administration, page 4-3.
- Command authorization—When an administrator issues operational commands on a network device, ACS is queried to determine whether the administrator is authorized to issue the command. See Command Authorization, page 4-4.

Device administration results can be shell profiles or command sets.

Shell profiles allow a selection of attributes to be returned in the response to the authorization request for a session, with privilege level as the most commonly used attribute. Shell profiles contain common attributes that are used for shell access sessions and user-defined attributes that are used for other types of sessions.

ACS 5.1 allows you to create custom TACACS+ authorization services and attributes. You can define:

- Any A-V pairs for these attributes.
- The attributes as either optional or mandatory.
- Multiple A-V pairs with the same name (multipart attributes).

ACS also supports task-specific predefined shell attributes. Using the TACACS+ shell profile, you can specify custom attributes to be returned in the shell authorization response. See TACACS+ Custom Services and Attributes, page 4-4.

Command sets define the set of commands, and command arguments, that are permitted or denied. The received command, for which authorization is requested, is compared against commands in the available command sets that are contained in the authorization results.

If a command is matched to a command set, the corresponding permit or deny setting for the command is retrieved. If multiple results are found in the rules that are matched, they are consolidated and a single permit or deny result for the command is returned, as described in these conditions:

- If an explicit deny-always setting exists in any command set, the command is denied.
- If no explicit deny-always setting exists in a command set, and any command set returns a permit result, the command is permitted.
- If either of the previous two conditions are not met, the command is denied.

You configure the permit and deny settings in the device administration rule table. You configure policy elements within a device administration rule table as conditions that are or not met. The rule table maps specific request conditions to device administration results through a matching process. The result of rule table processing is a shell profile or a command set, dependent on the type of request.

Session administration requests have a shell profile result, which contains values of attributes that are used in session provisioning. Command authorization requests have a command authorization result, which contains a list of command sets that are used to validate commands and arguments.

This model allows you to configure the administrator levels to have specific device administration capabilities. For example, you can assign a user the Network Device Administrator role which provides full access to device administration functions, while a Read Only Admin cannot perform administrative functions.

Session Administration

The following steps describe the flow for an administrator to establish a session (the ability to communicate) with a network device:

1. An administrator accesses a network device.
2. The network device sends a RADIUS or TACACS+ access request to ACS.
3. ACS uses an identity store (external LDAP, Active Directory, RSA, RADIUS Identity Server, or internal ACS identity store) to validate the administrator's credentials.
4. The RADIUS or TACACS+ response (accept or reject) is sent to the network device. The accept response also contains the administrator's maximum privilege level, which determines the level of administrator access for the duration of the session.

To configure a session administration policy (device administration rule table) to permit communication:

1. Configure the TACACS+ protocol global settings and user authentication option. See Configuring TACACS+ Settings, page 18-1.
2. Configure network resources. See Network Devices and AAA Clients, page 7-5.
3. Configure the users and identity stores. See Managing Internal Identity Stores, page 8-4 or Managing External Identity Stores, page 8-18.
4. Configure shell profiles according to your needs. See Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24.
5. Configure an access service policy. See Access Service Policy Creation, page 10-4.
6. Configure a service selection policy. See Service Selection Policy Creation, page 10-4.
7. Configure an authorization policy (rule table). See Configuring a Session Authorization Policy for Network Access, page 10-29.

Command Authorization

This topic describes the flow for an administrator to issue a command to a network device.

Note The device administration command flow is available for the TACACS+ protocol only.

1. An administrator issues a command to a network device.
2. The network device sends an access request to ACS.
3. ACS optionally uses an identity store (external Lightweight Directory Access Protocol [LDAP], Active Directory, RADIUS Identity Server, or internal ACS identity store) to retrieve user attributes which are included in policy processing.
4. The response indicates whether the administrator is authorized to issue the command.

To configure a command authorization policy (device administration rule table) to allow an administrator to issue commands to a network device:

1. Configure the TACACS+ protocol global settings and user authentication option. See Configuring TACACS+ Settings, page 18-1.
2. Configure network resources. See Network Devices and AAA Clients, page 7-5.
3. Configure the users and identity stores. See Managing Internal Identity Stores, page 8-4 or Managing External Identity Stores, page 8-18.
4. Configure command sets according to your needs. See Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-29.
5. Configure an access service policy. See Access Service Policy Creation, page 10-4.
6. Configure a service selection policy. See Service Selection Policy Creation, page 10-4.
7. Configure an authorization policy (rule table). See Configuring Shell/Command Authorization Policies for Device Administration, page 10-36.

Related Topics

- Network Devices and AAA Clients, page 7-5
- Configuring System Administrators and Accounts, page 16-3
- Managing Users and Identity Stores, page 8-1
- Managing External Identity Stores, page 8-18
- Managing Policy Conditions, page 9-1
- Managing Access Policies, page 10-1

TACACS+ Custom Services and Attributes

This topic describes the configuration flow to define TACACS+ custom attributes and services.

1. Create a custom TACACS+ condition to move to TACACS+ service on request. To do this:
   a. Go to **Policy Elements > Session Conditions > Custom** and click **Create**.
   b. Create a custom TACACS+ condition. See Creating, Duplicating, and Editing a Custom Session Condition, page 9-5.

2. Create an access service for Device Administration with the TACACS+ shell profile as the result. See Configuring Shell/Command Authorization Policies for Device Administration, page 10-36.
3. Create custom TACACS+ attributes. See Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24.

Password-Based Network Access

This section contains the following topics:

- Overview of Password-Based Network Access, page 4-5
- Password-Based Network Access Configuration Flow, page 4-6

For more information about password-based protocols, see Appendix B, "Authentication in ACS 5.1."

Overview of Password-Based Network Access

The use of a simple, unencrypted username and password is not considered a strong authentication mechanism but can be sufficient for low authorization or privilege levels such as Internet access.

Encryption reduces 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 AAA client and ACS. Before this point in the authentication process, unauthorized persons can obtain clear-text passwords, in these scenarios:

- The communication between an end-user client dialing up over a phone line
- An ISDN line terminating at a network-access server
- Over a Telnet session between an end-user client and the hosting device

ACS supports various authentication methods for authentication against the various identity stores that ACS supports. For more information about authentication protocol identity store compatibility, see Authentication Protocol and Identity Store Compatibility, page B-33.

Passwords can be processed by using these password-authentication protocols based on the version and type of security-control protocol used (for example, RADIUS), and the configuration of the AAA client and end-user client.

You can use different levels of security with ACS concurrently, for different requirements. Password Authentication Protocol (PAP) provides a basic security level. PAP provides a very basic level of security, but is simple and convenient for the client. MSCHAPv2 allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client.

Note During password-based access (or certificate-based access), the user is not only authenticated but also *authorized* according to the ACS configuration. And if NAS sends accounting requests, the user is also accounted.

ACS supports the following password-based authentication methods:

- Plain RADIUS password authentication methods
  - RADIUS-PAP
  - RADIUS-CHAP

  - RADIUS-MSCHAPv1
  - RADIUS-MSCHAPv2
- RADIUS EAP-based password authentication methods
  - PEAP-MSCHAPv2
  - PEAP-GTC
  - EAP-FAST-MSCHAPv2
  - EAP-FAST-GTC
  - EAP-MD5
  - LEAP

You must choose the authentication method based on the following factors:

- The network access server—Wireless access points, 802.1X authenticating switches, VPN servers, and so on.
- The client computer and software—EAP supplicant, VPN client, and so on.
- The identity store that is used to authenticate the user—Internal or External (AD, LDAP, RSA token server, or RADIUS identity server).

Related Topics

- Authentication in ACS 5.1, page B-1
- Password-Based Network Access Configuration Flow, page 4-6
- Network Devices and AAA Clients, page 7-5
- Managing Access Policies, page 10-1

Password-Based Network Access Configuration Flow

This topic describes the end-to-end flow for password-based network access and lists the tasks that you must perform. The information about how to configure the tasks is located in the relevant task chapters.

To configure password-based network access:

1. Configure network devices and AAA clients.
   a. In the Network Devices and AAA Clients, page 7-5, configure the **Authentication Setting** as RADIUS.
   b. Enter the Shared Secret.

   See Network Devices and AAA Clients, page 7-5, for more information.
2. Configure the users and identity stores. For more information, see Chapter 8, "Managing Users and Identity Stores."
3. Define policy conditions and authorization profiles. For more information, see Chapter 9, "Managing Policy Elements."
4. Define an access service. For more information, see Creating, Duplicating, and Editing Access Services, page 10-13.
   a. Set the Access Service Type to Network Access.
   b. Select one of the ACS-supported protocols in the Allowed Protocols Page and follow the steps in the Action column in Table 4-1.

5. Add the access service to your service selection policy. For more information, see Creating, Duplicating, and Editing Service Selection Rules, page 10-8.
6. Return to the service that you created and in the Authorization Policy Page, define authorization rules. For more information, see Configuring Access Service Policies, page 10-20.

Table 4-1 Network Access Authentication Protocols

Protocol	Action
Process Host Lookup (MAB)	In the Allowed Protocols Page, choose Process Host Lookup.
RADIUS PAP	In the Allowed Protocols Page, choose Allow PAP/ASCII.
RADIUS CHAP	In the Allowed Protocols Page, choose Allow CHAP.
RADIUS MSCHAPv1	In the Allowed Protocols Page, choose Allow MS-CHAPv1.
RADIUS MSCHAPv2	In the Allowed Protocols Page, choose Allow MS-CHAPv2.
EAP-MD5	In the Allowed Protocols Page, choose Allow EAP-MD5.
LEAP	In the Allowed Protocols Page, choose Allow LEAP.
PEAP	In the Allowed Protocols Page, choose PEAP. For the PEAP inner method, choose EAP-MSCHAPv2 or EAP-GTC or both.
EAP-FAST	1. In the Allowed Protocols Page, choose Allow EAP-FAST to enable the EAP-FAST settings. 2. For the EAP-FAST inner method, choose EAP-MSCHAPv2 or EAP-GTC or both. 3. Select Allow Anonymous In-Band PAC Provisioning or Allow Authenticated In-Band PAC Provisioning or both. For Windows machine authentication against Microsoft AD and for the change password feature: 1. Click the Use PACS radio button. For details about PACs, see About PACs, page B-20. 2. Check Allow Authenticated In-Band PAC Provisioning. 3. Check Allow Machine Authentication. 4. Enter the Machine PAC Time to Live.

For RADIUS, non-EAP authentication methods (RADIUS/PAP, RADIUS/CHAP, RADIUS/MS-CHAPv1, RADIUS/MSCHAPv2), and simple EAP methods (EAP-MD5 and LEAP), you need to configure only the protocol in the Allowed Protocols page as defined in Table 4-1.

Some of the complex EAP protocols require additional configuration:

- For EAP-TLS, you must also configure:
  - The EAP-TLS settings under **System Administration > Configuration > EAP-TLS Settings**.
  - A local server certificate under **System Administration > Configuration > Local Server Certificates > Local Certificates**.
  - A CA certificate under **Users and Identity Stores > Certificate Authorities**.
- For PEAP, you must also configure:
  - The inner method in the Allowed Protocols page and specify whether password change is allowed.

  - The PEAP settings under **System Administration > Configuration > PEAP Settings**.
  - Local server certificates under **System Administration > Configuration > Local Server Certificates > Local Certificates**.
- For EAP-FAST, you must also configure:
  - The inner method in the Allowed Protocols page and specify whether password change is allowed.
  - Whether or not to use PACs and if you choose to use PACs, you must also specify how to allow in-band PAC provisioning.
  - The EAP-FAST settings under **System Administration > Configuration > EAP-FAST > Settings**.
  - A local server certificate under **System Administration > Configuration > Local Server Certificates > Local Certificates** (Only if you enable authenticated PAC provisioning).

Related Topics

- Authentication in ACS 5.1, page B-1
- Network Devices and AAA Clients, page 7-5
- Managing Access Policies, page 10-1
- Creating, Duplicating, and Editing Access Services, page 10-13
- About PACs, page B-20

Certificate-Based Network Access

This section contains the following topics:

- Overview of Certificate-Based Network Access, page 4-8
- Using Certificates in ACS, page 4-9
- Certificate-Based Network Access for EAP-TLS, page 4-9

For more information about certificate-based protocols, see Appendix B, "Authentication in ACS 5.1."

Overview of Certificate-Based Network Access

Before using EAP-TLS, you must install a computer certificate on ACS. The installed computer certificate must be issued from a CA that can follow a certificate chain to a root CA that the access client trusts. Additionally, in order for ACS to validate the user or computer certificate of the access client, you must install the certificate of the root CA that issued the user or computer certificate to the access clients.

ACS supports certificate-based network access through the EAP-TLS protocol, which uses certificates for server authentication by the client and for client authentication by the server. Other protocols, such as PEAP or the authenticated-provisioning mode of EAP-FAST also make use of certificates for server authentication by the client, but they cannot be considered certificate-based network access because the server does not use the certificates for client authentication.

ACS Public Key Infrastructure (PKI) certificate-based authentication is based on X509 certificate identification. The entity which identifies itself with a certificate holds a private-key that correlates to the public key stored in the certificate.

A certificate can be self-signed or signed by another CA. A hierarchy of certificates can be made to form trust relations of each entity to its CA. The trusted root CA is the entity that signs the certificate of all other CAs and eventually signs each certificate in its hierarchy.

ACS identifies itself with its own certificate. ACS supports a certificate trust list (CTL) for authorizing connection certificates. ACS also supports complex hierarchies that authorize an identity certificate when all of the chain certificates are presented to it.

ACS supports several RSA key sizes used in the certificate that are 512, 1024, 2048, or 4096 bits. Other key sizes may be used. ACS 5.1 supports RSA. ACS does not support the Digital Signature Algorithm (DSA), however, in some use cases, ACS will not prevent DSA cipher suites from being used for certificate-based authentication.

All certificates that are used for network access authentication must meet the requirements for X.509 certificates and work for connections that use SSL/TLS. After this minimum requirement is met, the client and server certificates have additional requirements.

You can configure two types of certificates in ACS:

- Trust certificate—Also known as CA certificate. Used to form CTL trust hierarchy for verification of remote certificates.
- Local certificate—Also known as local server certificate. The client uses the local certificate with various protocols to authenticate the ACS server. This certificate is maintained in association with its private key, which is used to prove possession of the certificate.

Note During certificate-based access (or password-based access), the user is not only authenticated but also *authorized* according to the ACS configuration. And if NAS sends accounting requests, the user is also accounted.

Related Topics

- Configuring CA Certificates, page 8-61
- Configuring Local Server Certificates, page 18-14
- Using Certificates in ACS, page 4-9

Using Certificates in ACS

The four use cases for certificates in ACS 5.1 are:

- Certificate-Based Network Access for EAP-TLS, page 4-9
- Authorizing the ACS Web Interface from Your Browser Using a Certificate, page 4-10
- Validating an LDAP Secure Authentication Connection, page 4-11

Certificate-Based Network Access for EAP-TLS

For TLS- related EAP protocols, you must set up a server certificate from the local certificate store and a trust list certificate to authenticate the client. You can choose the trust certificate from any of the certificates in the local certificate store.

To use EAP-TLS, you must obtain and install trust certificates. The information about how to perform the tasks is located in the relevant task chapters.

Before you Begin:

Set up the server by configuring:

- EAP-TLS.
- The local certificate. See Configuring Local Server Certificates, page 18-14.

To configure certificate-based network access for EAP-TLS:

1. Configure the trust certificate list. See Configuring CA Certificates, page 8-61, for more information.
2. Configure the LDAP external identity store. You might want to do this to verify the certificate against a certificate stored in LDAP. See Creating External LDAP Identity Stores, page 8-22, for details.
3. Set up the Certificate Authentication Profile. See Configuring Certificate Authentication Profiles, page 8-66, for details.
4. Configure policy elements. See Managing Policy Conditions, page 9-1, for more information.

Note You can create custom conditions to use the certificate's attributes as a policy condition. See Creating, Duplicating, and Editing a Custom Session Condition, page 9-5, for details.

5. Create an access service. See Configuring Access Services, page 10-11, for more information.
6. In the Allowed Protocols Page, choose **EAP-TLS**.
7. Configure identity and authorization policies for the access service. See Configuring Access Service Policies, page 10-20, for details.

Note When you create rules for the identity policy, the result may be the Certificate Authentication Profile or an Identity Sequence. See Viewing Identity Policies, page 10-21, for more information.

8. Configure the Authorization Policies. See Configuring a Session Authorization Policy for Network Access, page 10-29.
9. Configure the Service Selection Policy. See Configuring the Service Selection Policy, page 10-6.

Related Topics

- Configuring Local Server Certificates, page 18-14
- Configuring CA Certificates, page 8-61
- Authentication in ACS 5.1, page B-1
- Overview of EAP-TLS, page B-6

Authorizing the ACS Web Interface from Your Browser Using a Certificate

You use the HTTPS certificate-based authentication to connect to ACS with your browser. The Local Server Certificate in ACS is used to authorize the ACS web interface from your browser. ACS does not support browser authentication (mutual authentication is not supported).

A default Local Server Certificate is installed on ACS so that you can connect to ACS with your browser. The default certificate is a self-signed certificate and cannot be modified during installation.

Related Topics

- Using Certificates in ACS, page 4-9
- Configuring Local Server Certificates, page 18-14

Validating an LDAP Secure Authentication Connection

You can define a secure authentication connection for the LDAP external identity store, by using a CA certificate to validate the connection.

To validate an LDAP secure authentication connection using a certificate:

Step 1 Configure an LDAP external identity store. See Creating External LDAP Identity Stores, page 8-22.

Step 2 In the LDAP Server Connection page, check **Use Secure Authentication**.

Step 3 Select **Root CA** from the drop-down menu and continue with the LDAP configuration for ACS.

Related Topics

- Using Certificates in ACS, page 4-9
- Configuring Local Server Certificates, page 18-14
- Managing External Identity Stores, page 8-18

Agentless Network Access

This section contains the following topics:

- Overview of Agentless Network Access, page 4-11
- Host Lookup, page 4-12
- Agentless Network Access Flow, page 4-15

For more information about protocols used for network access, see Authentication in ACS 5.1, page B-1.

Overview of Agentless Network Access

Agentless network access refers to the mechanisms used to perform port-based authentication and authorization in cases where the host device does not have the appropriate agent software. For example, a host device, where there is no 802.1x supplicant or a host device, where the supplicant is disabled.

802.1x must be enabled on the host device and on the switch to which the device connects. If a host/device without an 802.1x supplicant attempts to connect to a port that is enabled for 802.1x, it will be subjected to the default security policy. The default security policy says that 802.1x authentication must succeed before access to the network is granted. Therefore, by default, non-802.1x-capable devices cannot get access to an 802.1x-protected network.

Although many devices increasingly support 802.1x, there will always be devices that require network connectivity, but do not, or cannot, support 802.1x. Examples of such devices include network printers, badge readers, and legacy servers. You must make some provision for these devices.

Cisco provides two features to accommodate non-802.1x devices. For example, MAC Authentication Bypass (Host Lookup) and the Guest VLAN access by using web authentication. ACS 5.1 supports the Host Lookup fallback mechanism when there is no 802.1x supplicant. After 802.1x times out on a port, the port can move to an open state if Host Lookup is configured and succeeds.

Related Topics

- Host Lookup, page 4-12
- Agentless Network Access Flow, page 4-15

Host Lookup

ACS uses Host Lookup as the validation method when an identity cannot be authenticated according to credentials (for example, password or certificate), and ACS needs to validate the identity by doing a lookup in the identity stores.

An example for using host lookup is when a network device is configured to request MAC Authentication Bypass (MAB). This can happen after 802.1x times out on a port or if the port is explicitly configured to perform authentication bypass. When MAB is implemented, the host connects to the network access device. The device detects the absence of the appropriate software agent on the host and determines that it must identify the host according to its MAC address. The device sends a RADIUS request with *service-type=10* and the MAC address of the host to ACS in the calling-station-id attribute. (Some devices might be configured to implement the MAB request by sending PAP or EAP-MD5 authentication with the MAC address of the host in the user name, user password, and CallingStationID attributes, but without the *service-type=10* attribute.)

While most use cases for host lookup are to obtain a MAC address, there are other scenarios where a device requests to validate a different parameter, and the calling-station-id attribute contains this value instead of the MAC address (for example, IP address in layer 3 use cases).

Table 4-2 describes the RADIUS parameters required for host lookup use cases.

Table 4-2 RADIUS Attributes for Host Lookup Use Cases

	Use Cases		
Attribute	**PAP**	**802.1x**	**EAP-MD5**
RADIUS::ServiceType	—	Call check (with PAP or EAP-MD5)	—
RADIUS::UserName	MAC address	Any value (usually the MAC address)	MAC address
RADIUS::UserPassword	MAC address	Any value (usually the MAC address)	MAC address
RADIUS::CallingStationID	MAC address	MAC address	MAC address

ACS supports host lookup for the following identity stores:

- Internal hosts
- External LDAP
- Internal users

You can access the Active Directory via the LDAP API.

You can use the Internal Users identity store for Host Lookup in cases where the relevant host is already listed in the Internal Users identity store, and you prefer not to move the data to the Internal Hosts identity store. ACS uses the MAC format (XX-XX-XX-XX-XX-XX) and no other conversions are possible. To search the Internal Users identity store using the User-Name attribute (for example, xx:xx:xx:xx:xx:xx) you should leave the Process Host Lookup option unchecked. ACS will handle the request as a PAP request.

When MAC address authentication over PAP or EAP-MD5 is not detected according to the Host Lookup configuration, authentication and authorization occur like regular user authentication over PAP or EAP-MD5. You can use any identity store that supports these authentication protocols. ACS uses the MAC address format as presented in the RADIUS User-Name attribute.

Related Topics

- Creating an Access Service for Host Lookup, page 4-17
- Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17
- Managing Users and Identity Stores, page 8-1
- Authentication with Call Check, page 4-13

Authentication with Call Check

When ACS identifies a network access request with the call check attribute as Host Lookup (RADIUS::ServiceType = 10), ACS authenticates (validates) and authorizes the host by looking up the value in the Calling-Station-ID attribute (for example, the MAC address) in the configured identity store according to the authentication policy.

When ACS receives a RADIUS message, it performs basic parsing and validation, and then checks if the Call Check attribute, RADIUS ServiceType(6), is equal to the value 10. If the RADIUS ServiceType is equal to 10, ACS sets the system dictionary attribute UseCase to a value of Host Lookup.

In the ACS packet processing flow, the detection of Host Lookup according to Call Check service-type is done before the service selection policy. It is possible to use the condition *UseCase equals Host Lookup* in the service selection policy.

Initially, when RADIUS requests are processed, the RADIUS User-Name attribute is copied to the System UserName attribute. When the RADIUS Service-Type equals 10, the RADIUS Calling-Station-ID attribute is copied to the System User-Name attribute, and it overrides the RADIUS User-Name attribute value.

ACS supports four MAC address formats:

- Six groups of two hexadecimal digits, separated by hyphens—01-23-45-67-89-AB
- Six groups of two hexadecimal digits, separated by colons—01:23:45:67:89:AB
- Three groups of four hexadecimal digits, separated by dots—0123.4567.89AB
- Twelve consecutive hexadecimal digits without any separators—0123456789AB

If the Calling-Station-ID attribute is one of the four supported MAC address formats above, ACS copies it to the User-Name attribute with the format of XX-XX-XX-XX-XX-XX. If the MAC address is in a format other than one of the four above, ACS copies the string as is.

Process Service-Type Call Check

You may not want to copy the CallingStationID attribute value to the System UserName attribute value. When the Process Host Lookup option is checked, ACS uses the System UserName attribute that was copied from the RADIUS User-Name attribute. When the Process Host Lookup option is not checked, ACS ignores the HostLookup field and uses the original value of the System UserName attribute for authentication and authorization. The request processing continues according to the message protocol; for example, according to the RADIUS User-Name and User-Password attributes for PAP.

PAP/EAP-MD5 Authentication

When a device is configured to use PAP or EAP-MD5 for MAC address authentication, you can configure ACS to detect the request as a Host Lookup request, within the network access service. The device sends the request with the host's MAC address in the User-Name, User-Password, and Calling-Station-ID attributes.

If you do not configure ACS to detect Host Lookup, the access request is handled as a regular PAP, or EAP-MD5 authentication request.

If you check the Process HostLookup field and select PAP or EAP-MD5, ACS places the HostLookup value in the ACS::UseCase attribute. The User-Password attribute is ignored for the detection algorithm. ACS follows the authentication process as if the request is using the call check attribute, and processes it as a Host Lookup (Service-Type=10) request. The RADIUS dictionary attribute ACS::UseCase is set to the value of HostLookup.

The Detect Host Lookup option for PAP and EAP-MD5 MAC authentication is done after the service selection policy. If a service selection rule is configured to match ACS::UseCase = Host Lookup, the request falls into the Host Lookup category.

If ACS is not configured to detect PAP or EAP-MD5 authentications as MAC authentication flows, ACS will not consider the Detect Host Lookup option. These requests are handled like a regular user request for authentication, and looks for the username and password in the selected identity store.

Related Topics

- Creating an Access Service for Host Lookup, page 4-17
- Managing Access Policies, page 10-1
- Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17
- Managing Users and Identity Stores, page 8-1

Agentless Network Access Flow

This topic describes the end-to-end flow for agentless network access and lists the tasks that you must perform. The information about how to configure the tasks is located in the relevant task chapters.

Perform these tasks in the order listed to configure agentless network access in ACS:

1. Configure network devices and AAA clients.

   This is the general task to configure network devices and AAA clients in ACS and is not specific to agentless network access. Select **Network Resources > Network Devices and AAA Clients** and click **Create**. See Network Devices and AAA Clients, page 7-5.

2. Configure an identity store for internal hosts.

   Configure an internal identity store. See Configuring an Internal Identity Store for Host Lookup, page 4-16

   or

   Configure an external identity store. See Configuring an LDAP External Identity Store for Host Lookup, page 4-16.

   For more information, see Chapter 8, “Managing Users and Identity Stores.”

3. Configure the identity group. See Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17.

   For more information, see Chapter 8, “Managing Users and Identity Stores.”

4. Define policy elements and authorization profiles for Host Lookup requests.

   For more information, see Chapter 9, “Managing Policy Elements.”

5. Define an access service for Host Lookup. For more information, see Creating, Duplicating, and Editing Access Services, page 10-13.

6. Return to the service that you created:

   a. Define an identity policy. For more information, see Configuring an Identity Policy for Host Lookup Requests, page 4-18.

      ACS has the option to look for host MAC addresses in multiple identity stores. For example, MAC addresses can be in the Internal Hosts identity store, in one of the configured LDAP identity stores, or in the Internal Users identity store. The MAC address lookup may be in one of the configured identity stores, and the MAC attributes may be fetched from a different identity store that you configured in the identity sequence.

      You can configure ACS to continue processing a Host Lookup request even if the MAC address was not found in the identity store. An administrator can define an authorization policy based on the event, regardless of whether or not the MAC address was found.

      The ACS::UseCase attribute is available for selection in the Authentication Policy, but is not mandatory for Host Lookup support.

   b. Return to the service that you created.

   c. Define an authorization policy. For more information, see Configuring an Authorization Policy for Host Lookup Requests, page 4-18.

7. Define the service selection. Add the access service to your service selection policy. For more information, see Creating, Duplicating, and Editing Service Selection Rules, page 10-8.

Related Topics

- Managing Users and Identity Stores, page 8-1
- Managing Access Policies, page 10-1

Configuring an Internal Identity Store for Host Lookup

To configure an internal identity store for Host Lookup:

Step 1 Choose **Users and Identity Store > Internal Identity Stores > Hosts** and click **Create**. See Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17, or more information.

Step 2 Fill in the fields as described in the **Users and Identity Stores > Internal Identity Store > Hosts > Create** Page.

Step 3 Click **Submit**.

Previous Step:

Network Devices and AAA Clients, page 7-5

Next Step:

Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17

Configuring an LDAP External Identity Store for Host Lookup

To configure an LDAP external identity store for Host Lookup:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP** and click **Create**. See Creating External LDAP Identity Stores, page 8-22, for more information.

Step 2 Follow the steps for creating an LDAP database.

In the LDAP: Directory Organization page, choose the MAC address format.

The format you choose represents the way MAC addresses are stored in the LDAP external identity store.

Step 3 Click **Finish.**

Previous Step:

Network Devices and AAA Clients, page 7-5

Next Step:

Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17

Related Topics

- Creating External LDAP Identity Stores, page 8-22
- Deleting External LDAP Identity Stores, page 8-29

Configuring an Identity Group for Host Lookup Network Access Requests

To configure an identity group for Host Lookup network access requests:

Step 1 Choose **Users and Identity Store > Identity Groups>** and click **Create**. See Managing Identity Attributes, page 8-7, for more information.

Step 2 Fill in the fields as required.

The identity group may be any agentless device, such as a printer or phone.

Step 3 Click **Submit**.

Previous Steps:

- Configuring an Internal Identity Store for Host Lookup, page 4-16
- Configuring an LDAP External Identity Store for Host Lookup, page 4-16

Next Step:

- Creating an Access Service for Host Lookup, page 4-17

Related Topic

- Managing Identity Attributes, page 8-7

Creating an Access Service for Host Lookup

You create an access service and then enable agentless host processing.

To create an access service for Host Lookup:

Step 1 Choose **Access Policies > Access Service**, and click **Create**. See Configuring Access Services, page 10-11, for more information.

Step 2 Fill in the fields as described in the Access Service Properties—General page:

a. In the Service Structure section, choose **User Selected Policy Structure.**

b. Set the Access Service Type to **Network Access** and define the policy structure.

c. Select **Network Access**, and check **Identity** and **Authorization**. The group mapping and External Policy options are optional.

d. Make sure you select Process Host Lookup.

If you want ACS to detect PAP or EAP-MD5 authentications for MAC addresses (see PAP/EAP-MD5 Authentication, page 4-14), and process it like it is a Host Lookup request (for example, MAB requests), complete the following steps:

e. Select one of the ACS supported protocols for MAB in the Allowed Protocols Page (EAP-MD5 or PAP).

f. Check **Detect PAP/EAP-MD5** as Host Lookup.

Related Topics

- Managing Access Policies, page 10-1
- Authentication in ACS 5.1, page B-1
- Authentication with Call Check, page 4-13
- Process Service-Type Call Check, page 4-14

Configuring an Identity Policy for Host Lookup Requests

To configure an identity policy for Host Lookup requests:

Step 1 Choose **Access Policies > Access Services > <access_servicename> Identity**. See Viewing Identity Policies, page 10-21, for details.

Step 2 Select **Customize** to customize the authorization policy conditions. A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions. See Customizing a Policy, page 10-5, for more information.

Step 3 Select **Use Case** from the **Available** customized conditions and move it to the **Selected** conditions. In the Identity Policy Page, click **Create.**

a. Enter a **Name** for the rule.

b. In the Conditions area, check **Use Case**, then check whether the value should or should not match.

c. Select **Host Lookup** and click **OK.**

This attribute selection ensures that while processing the access request, ACS will look for the host and not for an IP address.

d. Select any of the identity stores that support host lookup as your Identity Source.

e. Click **OK**.

Step 4 Click **Save Changes**.

Related Topic

- Managing Access Policies, page 10-1

Configuring an Authorization Policy for Host Lookup Requests

To configure an authorization policy for Host Lookup requests:

Step 1 Choose **Access Policies > Access Services > <access_servicename> Authorization**. See Configuring a Session Authorization Policy for Network Access, page 10-29, for details.

Step 2 Select **Customize** to customize the authorization policy conditions. A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions. See Customizing a Policy, page 10-5, for more information.

Step 3 Select **Use Case** from the **Available** customized conditions and move it to the **Selected** conditions.

Step 4 Select **Authorization Profiles** from the customized results and move it to the **Selected** conditions and click **OK.**

Step 5 In the Authorization Policy Page, click **Create.**

a. Enter a **Name** for the rule.

b. In the Conditions area, check **Use Case**, then check whether the value should or should not match.

c. Select **Host Lookup and** click **OK.**

This attribute selection ensures that while processing the access request, ACS will look for the host and not for an IP address.

d. Select an **Authorization Profile** from the authorization profiles and move it to the **Selected** results column and click **OK.**

Step 6 Click **Save Changes.**

Related Topic

- Managing Access Policies, page 10-1

VPN Remote Network Access

A remote access Virtual Private Network (VPN) allows you to connect securely to a private company network from a public Internet. You could be accessing your company's network from home or elsewhere. The VPN is connected to your company's perimeter network (DMZ). A VPN gateway can manage simultaneous VPN connections.

Related Topics

- Supported Authentication Protocols, page 4-19
- Supported Identity Stores, page 4-20
- Supported VPN Network Access Servers, page 4-20
- Supported VPN Clients, page 4-21
- Configuring VPN Remote Access Service, page 4-21

Supported Authentication Protocols

ACS 5.1 supports the following protocols for inner authentication inside the VPN tunnel:

- RADIUS/PAP
- RADIUS/CHAP
- RADIUS/MS-CHAPv1
- RADIUS/MS-CHAPv2

With the use of MS-CHAPv1 or MS-CHAPv2 protocols, ACS can generate MPPE keys that is used for encryption of the tunnel that is created.

Related Topics

- VPN Remote Network Access, page 4-19
- Supported Identity Stores, page 4-20

- Supported VPN Network Access Servers, page 4-20
- Supported VPN Clients, page 4-21
- Configuring VPN Remote Access Service, page 4-21

Supported Identity Stores

ACS can perform VPN authentication against the following identity stores:

- ACS internal identity store—RADIUS/PAP, RADIUS/CHAP, RADIUS/MS-CHAP-v1, and RADIUS/MS-CHAP-v2
- Active Directory—RADIUS/PAP, RADIUS/MS-CHAP-v1, and RADIUS/MS-CHAP-v2
- LDAP—RADIUS/PAP
- RSA SecurID Server—RADIUS/PAP
- RADIUS Token Server—RADIUS/PAP (dynamic OTP)

Related Topics

- VPN Remote Network Access, page 4-19
- Supported Authentication Protocols, page 4-19
- Supported VPN Network Access Servers, page 4-20
- Supported VPN Clients, page 4-21
- Configuring VPN Remote Access Service, page 4-21

Supported VPN Network Access Servers

ACS 5.1 supports the following VPN network access servers:

- Cisco ASA 5500 Series
- Cisco VPN 3000 Series

Related Topics

- VPN Remote Network Access, page 4-19
- Supported Authentication Protocols, page 4-19
- Supported Identity Stores, page 4-20
- Supported VPN Clients, page 4-21
- Configuring VPN Remote Access Service, page 4-21

Supported VPN Clients

- ACS 5.1 supports the following VPN clients:
- Cisco VPN Client 5.0 Series
- Cisco Clientless SSL VPN (WEBVPN)
- Cisco AnyConnect VPN client 2.3 Series
- MS VPN client

Related Topics

- VPN Remote Network Access, page 4-19
- Supported Authentication Protocols, page 4-19
- Supported Identity Stores, page 4-20
- Supported VPN Network Access Servers, page 4-20
- Configuring VPN Remote Access Service, page 4-21

Configuring VPN Remote Access Service

To configure a VPN remote access service:

Step 1 Configure the VPN protocols in the Allowed Protocols page of the default network access service. For more information, see Configuring Access Service Allowed Protocols, page 10-16.

Step 2 Create an authorization profile for VPN by selecting the dictionary type, and the Tunneling-Protocols attribute type and value. For more information, see Specifying RADIUS Attributes in Authorization Profiles, page 9-22.

Step 3 Click **Submit** to create the VPN authorization profile.

Related Topics

- VPN Remote Network Access, page 4-19
- Supported Authentication Protocols, page 4-19
- Supported Identity Stores, page 4-20
- Supported VPN Network Access Servers, page 4-20
- Supported VPN Clients, page 4-21
- Configuring VPN Remote Access Service, page 4-21

ACS and Cisco TrustSec

Note ACS requires an additional feature license to enable TrustSec capabilities.

Cisco TrustSec, hereafter referred to as TrustSec, is a new security architecture for Cisco products. You can use TrustSec to create a trustworthy network fabric that provides confidentiality, message authentication, integrity, and antireplay protection on network traffic.

TrustSec requires that all network devices have an established identity, and must be authenticated and authorized before they start operating in the network. This precaution prevents the attachment of rogue network devices in a secure network. Until now, ACS authenticated only users and hosts to grant them access to the network. With TrustSec, ACS also authenticates devices such as routers and switches by using a name and password. Any device with a Network Interface Card (NIC) must authenticate itself or stay out of the trusted network. Security is improved and device management is simplified since devices can be identified by their name rather than IP address.

Note The Cisco Catalyst 6500 running Cisco IOS 12.2(33) SXI and DataCenter 3.0 (Nexus 7000) NX-OS 4.0.3 devices support TrustSec. The Cisco Catalyst 6500 supports Security Group Tags (SGTs); however, it does not support Security Group Access Control Lists (SGACLs) in this release.

To configure ACS for TrustSec:

1. Add users.

   This is the general task to add users in ACS and is not specific to TrustSec. Choose **Users and Identity Stores > Internal Identity Store > Users** and click **Create**. See Creating Internal Users, page 8-11, for more information.
2. Adding Devices for TrustSec.
3. Creating Security Groups.
4. Creating SGACLs.
5. Configuring an NDAC Policy.
6. Configuring EAP-FAST Settings for TrustSec.
7. Creating an Access Service for TrustSec.
8. Creating an Endpoint Admission Control Policy.
9. Creating an Egress Policy.
10. Creating a Default Policy.

Adding Devices for TrustSec

The RADIUS protocol requires a shared secret between the AAA client and the server. In ACS, RADIUS requests are processed only if they arrive from a known AAA client. You must configure the AAA client in ACS with a shared secret. The TrustSec device should be configured with the same shared secret. In TrustSec, every device must be able to act as a AAA client for new devices that join the secured network.

All the TrustSec devices possess a Protected Access Credential (PAC) as part of the EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol. A PAC is used to identify the AAA client. The RADIUS shared secret can be derived from the PAC.

To add a network device:

Step 1 Choose **Network Resources > Network Devices and AAA Client** and click **Create**. See Network Devices and AAA Clients, page 7-5, for more information.

Step 2 Fill in the fields in the Network Devices and AAA clients pages:

- To add a device as a seed TrustSec device, check **RADIUS** and **TrustSec**, or to add a device as a TrustSec client, check **TrustSec** only.

  If you add the device as a RADIUS client, enter the **IP Address** and the **RADIUS/Shared Secret**.

  If you add the device as a TrustSec device, fill in the fields in the TrustSec section.

- (Optional) Check **Advanced Settings** to display advanced settings for the TrustSec device configuration and modify the default settings.

The location or device type can be used as a condition to configure an NDAC policy rule.

Step 3 Click **Submit**.

Creating Security Groups

TrustSec uses security groups for tagging packets at ingress to allow filtering later on at Egress. The product of the security group is the security group tag, a 4-byte string ID that is sent to the network device. The web interface displays the decimal and hexadecimal representation. The SGT is unique. When you edit a security group you can modify the name, however, you cannot modify the SGT ID.

The security group names *Unknown* and *Any* are reserved. The reserved names are used in the Egress policy matrix. The generation ID changes when the Egress policy is modified.

Devices consider only the SGT value; the name and description of a security group are a management convenience and are not conveyed to the devices. Therefore, changing the name or description of the security group does not affect the generation ID of an SGT.

To create a security group:

Step 1 Choose **Policy Elements > Authorizations and Permissions > Network Access > Security Groups** and click **Create**.

Step 2 Fill in the fields as described in the Configuring Security Group Access Control Lists, page 9-33.

Tip When you edit a security group, the security group tag and the generation ID are visible.

Step 3 Click **Submit**.

Creating SGACLs

Security Group Access Control Lists (SGACLs) are similar to standard IP-based ACLs, in that you can specify whether to allow or deny communications down to the transport protocol; for example, TCP, User Datagram Protocol (UDP), and the ports; FTP; or Secure Shell Protocol (SSH). You can create

SGACLs that can be applied to communications between security groups. You apply TrustSec policy administration in ACS by configuring these SGACLs to the intersection of source and destination security groups through a customizable Egress matrix view, or individual source and destination security group pairs.

To create an SGACL:

Step 1 Choose **Policy Elements > Authorizations and Permissions > Named Permissions Objects > Security Group ACLs**. then click **Create**.

Step 2 Fill in the fields as described in the Configuring Security Group Access Control Lists, page 9-33.

Step 3 Click **Submit**.

Configuring an NDAC Policy

The Network Device Admission Control (NDAC) policy defines which security group is sent to the device. When you configure the NDAC policy, you create rules with previously defined conditions, for example, NDGs. The NDAC policy is a single service, and it contains a single policy with one or more rules. Since the same policy is used for setting responses for authentication, peer authorization, and environment requests, the same SGT is returned for all request types when they apply to the same device.

Note You cannot add the NDAC policy as a service in the service selection policy; however, the NDAC policy is automatically applied to TrustSec devices.

To configure an NDAC policy for a device:

Step 1 Choose **Access Policies > TrustSec Access Control > Network Device Access > Authorization Policy**.

Step 2 Click **Customize** to select which conditions to use in the NDAC policy rules.

Note The Default Rule provides a default rule when no rules match or there are no rules defined. The default security group tag for the Default Rule result is Unknown.

Step 3 Click **Create** to create a new rule.

Step 4 Fill in the fields in the NDAC Policy Properties page.

Step 5 Click **Save Changes**.

Configuring EAP-FAST Settings for TrustSec

Since RADIUS information is retrieved from the PAC, you must define the amount of time for the EAP-FAST tunnel PAC to live. You can also refresh the time to live for an active PAC.

To configure the EAP-FAST settings for the tunnel PAC:

Step 1 Choose **Access Policies > TrustSec Access Control > > Network Device Access**.

Step 2 Fill in the fields in the Network Device Access EAP-FAST Settings page.

Step 3 Click **Submit**.

Creating an Access Service for TrustSec

You create an access service for endpoint admission control policies for endpoint devices, and then you add the service to the service selection policy.

Note The NDAC policy is a service that is automatically applied to TrustSec devices. You do not need to create an access service for TrustSec devices.

To create an access service:

Step 1 Choose **Access Policies > Access Service**, and click **Create**. See Configuring Access Services, page 10-11, for more information.

Step 2 Fill in the fields in the Access Service Properties—General page as required.

Step 3 In the Service Structure section, choose **User selected policy structure**.

Step 4 Select **Network Access**, and check **Identity** and **Authorization**.

Step 5 Click **Next**.

The Access Services Properties page appears.

Step 6 In the Authentication Protocols area, check the relevant protocols for your access service.

Step 7 Click **Finish**.

Creating an Endpoint Admission Control Policy

After you create a service, you configure the endpoint admission control policy. The endpoint admission control policy returns an SGT to the endpoint and an authorization profile. You can create multiple policies and configure the Default Rule policy. The defaults are Deny Access and the Unknown security group.

To add a session authorization policy for an access service:

Step 1 Choose **Access Policies > Access Services > <*service*> > Authorization**.

Step 2 Configure an Authorization Policy. See Configuring a Session Authorization Policy for Network Access, page 10-29.

Step 3 Fill in the fields in the Network Access Authorization Rule Properties page.

Note The Default Rule provides a default rule when no rules match or there are no rules defined. The default for the Default Rule result is Deny Access, which denies access to the network. The security group tag is Unknown.

Note You can modify the security group when creating the session authorization policy for TrustSec.

Step 4 Click **OK**.

Step 5 Choose **Access Policies > Service Selection Policy** to choose which services to include in the endpoint policy. See Configuring the Service Selection Policy, page 10-6, for more information.

Step 6 Fill in the fields in the Service Select Policy pages.

Step 7 Click **Save Changes**.

Creating an Egress Policy

The Egress policy (sometimes called SGACL policy) determines which SGACL to apply at the Egress points of the network based on the source and destination SGT. The Egress policy is represented in a matrix, where the X and Y axes represent the destination and source SGT, respectively, and each cell contains the set of SGACLs to apply at the intersection of these two SGTs. Any security group can take the role of a source SGT, if an endpoint (or TrustSec device) that carries this SGT sends the packet. Any security group can take the role of a destination SGT, if the packet is targeting an endpoint (or TrustSec device) that carries this SGT. Therefore, the Egress matrix lists all of the existing security groups on both axes, making it a Cartesian product of the SGT set with itself (SGT x SGT).

The first row (topmost) of the matrix contains the column headers, which display the destination SGT. The first column (far left) contains the row titles, with the source SG displayed. At the intersection of these axes lies the origin cell (top left) that contains the titles of the axes, namely, Destination and Source. All other cells are internal matrix cells that contain the defined SGACL. The rows and columns are ordered alphabetically according to the SGT names.

Initially, the matrix contains the cell for the unknown source and unknown destination SG. *Unknown* refers to the preconfigured SG, which is not modifiable. When you add an SG, ACS adds a new row and new column to the matrix with empty content for the newly added cell.

To add an Egress policy and populate the Egress matrix:

Step 1 Choose **Access Policies > TrustSec Access Control > Egress Policy**.

The Egress matrix is visible. The security groups appear in the order in which you defined them.

Step 2 Click on a cell and then click **Edit**.

Step 3 Fill in the fields as required.

Step 4 Select the set of SGACLs to apply to the cell and move the selected set to the Selected column.

The ACLS are used at the Egress point of the SGT of the source and destination that match the coordinates of the cell. The SGACLs are applied in the order in which they appear.

Step 5 Use the Up and Down arrows to change the order. The device applies the policies in the order in which they are configured. The SGACL are applied to packets for the selected security groups.

Step 6 Click **Submit**.

Creating a Default Policy

After you configure the Egress policies for the source and destination SG in the Egress matrix, Cisco recommends that you configure the Default Egress Policy. The default policy refers to devices that have not been assigned an SGT. The default policy is added by the network devices to the specific policies defined in the cells. The initial setting for the default policy is *Permit All*.

The term *default policy* refers to the ANY security group to ANY security group policy. TrustSec network devices concatenate the default policy to the end of the specific cell policy. If the cell is empty, only the default policy is applied. If the cell contains a policy, the resultant policy is the combination of the cell-specific policy which precedes the default policy.

Note The way the specific cell policy and the default policy are combined depends on the algorithm running on the device. The result is the same as concatenating the two policies. The packet is analyzed first to see if it matches the ACEs defined by the SGACLs of the cell. If there is no match, the packet falls through to be matched by the ACEs of the default policy.

Combining the cell-specific policy and the default policy is done not by ACS, but by the TrustSec network device. From the ACS perspective, the cell-specific and the default policy are two separate sets of SGACLs, which are sent to devices in response to two separate policy queries.

To create a default policy:

Step 1 Choose **Access Policies > TrustSec Access Control > Egress Policy** then choose **Default Policy**.

Step 2 Fill in the fields as in the Default Policy for Egress Policy page.

Step 3 Click **Submit**.

RADIUS Proxy Requests

You can use ACS to act as a proxy server that receives authentication and accounting RADIUS requests from a Network Access Server (NAS) and forwards them to a remote server. ACS then receives the replies for each forwarded request from the remote RADIUS server and sends it back to the client.

ACS uses the service selection policy to differentiate between incoming authentication and accounting requests that must be handled locally and those that must be forwarded to a remote RADIUS server.

When ACS receives a proxy request from the NAS, it forwards the request to the first remote RADIUS server in its list. ACS processes the first valid or invalid response from the remote RADIUS server and does the following:

- If the response is valid, such as an Access-Challenge, Access-Accept, Access-Reject, or Accounting-Response, ACS returns the response back to the NAS.

- If ACS does not receive a response within the specified time period, after the specified number of retries, it forwards the request to the next remote RADIUS server in the list.
- If the response is invalid, ACS drops the request and does not send any response to the NAS.

You can configure ACS to strip the prefix, suffix, and both from a username. For example, from a username acme\smith@acme.com, you can configure ACS to extract only the name of the user, smith by specifying \ and @ as the prefix and suffix separators respectively.

ACS can perform local accounting, remote accounting, or both. If you choose both, ACS performs local accounting and then moves on to remote accounting. If there are any errors in local accounting, ACS ignores them and moves on to remote accounting.

During proxying, ACS:

1. Receives the following packets from the NAS and forwards them to the remote RADIUS server:
- Access-Request
- Accounting-Request packets
2. Receives the following packets from the remote RADIUS server and returns them back to the NAS:
- Access-Accept
- Access-Reject
- Access-Challenge
- Accounting-Response

Note An unresponsive external RADIUS server waits for about <*timeout*> * <*number of retries*> seconds before failover to move to the next server. There could be several unresponsive servers in the list before the first responsive server is reached. In such cases, each request that is forwarded to a responsive external RADIUS server is delayed for <*number of previous unresponsive servers*> * <*timeout*> * <*number of retries*>. This delay can sometimes be longer than the external RADIUS server timeout between two messages in EAP or RADIUS conversation. In such a situation, the external RADIUS server would drop the request.

Related Topics

- Supported Protocols, page 4-28
- Supported RADIUS Attributes, page 4-29
- Configuring RADIUS Proxy Service, page 4-29

Supported Protocols

The RADIUS proxy feature in ACS supports the following protocols:

- Supports forwarding for all RADIUS protocols
- All EAP protocols (including protocols that are not supported by ACS).

Related Topics

- RADIUS Proxy Requests, page 4-27
- Supported RADIUS Attributes, page 4-29
- Configuring RADIUS Proxy Service, page 4-29

Supported RADIUS Attributes

The following supported RADIUS attributes are encrypted:

- User-Password
- CHAP-Password
- Message-Authenticator
- MPPE-Send-Key and MPPE-Recv-Key
- Tunnel-Password
- LEAP Session Key Cisco AV-Pair

Related Topics

- RADIUS Proxy Requests, page 4-27
- Supported Protocols, page 4-28
- Configuring RADIUS Proxy Service, page 4-29

Configuring RADIUS Proxy Service

To configure RADIUS proxy:

Step 1 Configure a set of remote RADIUS servers. For information on how to configure remote RADIUS servers, see Creating, Duplicating, and Editing External RADIUS Servers, page 7-18.

Step 2 Configure a RADIUS proxy service. For information on how to configure a RADIUS proxy service, see Configuring General Access Service Properties, page 10-14.

Note You must select the User Selected Service Type option and choose RADIUS proxy as the Access Service Policy Structure in the Access Service Properties - General page.

Step 3 After you configure the allowed protocols, click finish to complete your RADIUS proxy service configuration.

Related Topics

- RADIUS Proxy Requests, page 4-27
- Supported Protocols, page 4-28
- Supported RADIUS Attributes, page 4-29

CHAPTER 5

Understanding My Workspace

The Cisco Secure ACS web interface is designed to be viewed using Microsoft Internet Explorer 6.x and 7.x, and Mozilla Firefox 3.x. The web interface not only makes viewing and administering ACS possible, but it also allows you to monitor and report on any event in the network. These reports track connection activity, show which users are currently logged in, list the failed authentication and authorization attempts, and so on.

The My Workspace drawer contains:

- Welcome Page, page 5-1
- Task Guides, page 5-2
- My Account Page, page 5-2
- Using the Web Interface, page 5-3
- Importing and Exporting ACS Objects through the Web Interface, page 5-18
- Common Errors, page 5-25
- Accessibility, page 5-27

Welcome Page

The Welcome page appears when you start ACS, and provides shortcuts to common ACS tasks, and links to information.

You can return to the Welcome page at any time during your ACS session. To return to this page, choose **My Workspace > Welcome**.

Table 5-1 Welcome Page

Field	Description
Before You Begin	This section contains a link to a section that describes the ACS policy model and associated terminology.
Getting Started	The links in this section launch the ACS Task Guides, which provide step-by-step instructions on how to accomplish ACS tasks.
Quick Start	Opens the Task Guide for the Quick Start scenario. These steps guide you through a minimal system setup to get ACS going quickly in a lab, evaluation, or demonstration environment.
Initial System Setup	Opens the Task Guide for initial system setup. This scenario guides you through the steps that are required to set up ACS for operation as needed; many steps are optional.

Table 5-1 Welcome Page (continued)

Field	Description
Policy Setup Steps	Opens the Task Guide for policy setup. This scenario guides you through the steps that are required to set up ACS policies.
New in ACS 5	The options in this section link to topics in the ACS online help. Click an option to open the online help window, which displays information for the selected topic. Use the links in the online help topics and in the Contents pane of the online help to view more information about ACS features and tasks.
Tutorials & Other Resources	Provides links to: • Introduction Overview video. • Configuration guide that provides step-by-step instructions for common ACS scenarios.

Task Guides

From the My Workspace drawer, you can access Tasks Guides. Clicking any of the task guides opens a frame on the right side of the web interface. This frame contains step-by-step instructions as well as links to additional information. ACS provides the following task guides:

- Quick Start—Lists the minimal steps required to get ACS up and running quickly.
- Initial System Setup—Lists the required steps to set up ACS for basic operations, including information about optional steps.
- Policy Setup Steps—Lists the required steps to define ACS access control policies.

My Account Page

Use the My Account page to update and change the administrator password for the administrator that is currently logged in to ACS.

To display this page, select **My Workspace > My Account**.

Table 5-2 My Account Page

Field	Description
General	Read-only fields that display information about the currently logged-in administrator: • Administrator name • Description • E-mail address, if it is available
Change Password	Displays rules for password definition according to the password policy. To change your password: 1. In the Password field, enter your current password. 2. In the New Password field, enter a new password. 3. In the Confirm Password field, enter your new password again.
Assigned Roles	Displays the roles that are assigned to the currently logged-in administrator.

Related Topics

- Configuring Authentication Settings for Administrators, page 16-9
- Changing the Administrator Password, page 16-13

Using the Web Interface

You can configure and administer ACS through the ACS web interface, in which you can access pages, perform configuration tasks, and view interface configuration errors. This section describes:

- Accessing the Web Interface, page 5-3
- Understanding the Web Interface, page 5-5
- Common Errors, page 5-25
- Accessibility, page 5-27

Accessing the Web Interface

The ACS web interface is supported on HTTPS-enabled Microsoft Internet Explorer versions 6 and 7, and Firefox version 3.x.

This section contains:

- Logging In, page 5-3
- Logging Out, page 5-4

Logging In

To log in to the ACS web interface for the first time after installation:

Step 1 Enter the ACS URL in your browser, for example **https://*<acs_host>*/acsadmin**, where <acs_host> is the IP address or Domain Name System (DNS) hostname.

The login page appears.

Step 2 Enter **ACSAdmin** in the Username field; the value is not case-sensitive.

Step 3 Enter **default** in the Password field; the value is case-sensitive.

Note This password (default) is valid only when you log in for the first time after installation. Click **Reset** to clear the Username and Password fields and start over, if needed.

Step 4 Click **Login** or press **Enter**.

The login page reappears, prompting you to change your password.

Note ACS prompts you to change your password the first time you log in to the web interface after installation and in other situations based on the authentication settings that is configured in ACS.

Step 5 Enter **default** in the Old Password field, then enter a new password in the New Password and the Confirm Password fields.

Note If you forget your username or password, use the **acs reset-password** command to reset your username to ACSAdmin and your password to default. You are prompted to change your password after a reset. See *Command Line Reference for ACS 5.1* for more information.

Step 6 Click **Login** or press **Enter**.

You are prompted to install a valid license:

Note The license page only appears the first time that you log in to ACS.

Step 7 See Installing a License File, page 18-36 to install a valid license.

If your login is successful, the main page of the ACS web interface appears.

If your login is unsuccessful, the following error message appears:

```
Invalid username or password specified.
```

The Username and Password fields are cleared.

Step 8 Re-enter the valid username and password, and click **Login**.

Logging Out

Click **Logout** in the ACS web interface header to end your administrative session. A dialog box appears asking if you are sure you want to log out of ACS. Click **OK**.

Caution For security reasons, Cisco recommends that you log out of the ACS when you complete your administrative session. If you do not log out, the ACS web interface logs you out if your session remains inactive for a configurable period of time, and does not save any unsubmitted configuration data.

Understanding the Web Interface

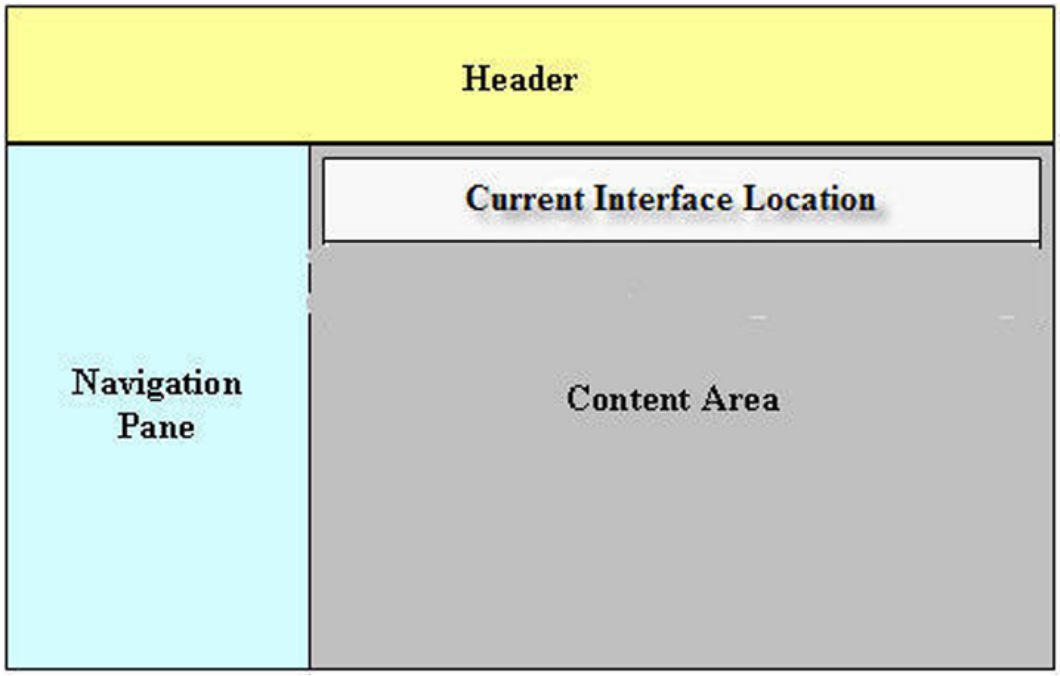
The following sections explain the ACS web interface:

- Web Interface Design, page 5-5
- Header, page 5-5
- Navigation Pane, page 5-6
- Content Area, page 5-8

Web Interface Design

Figure 5-1 shows the overall design of the ACS web interface.

Figure 5-1 ACS Web Interface



The interface contains:

- Header, page 5-5
- Navigation Pane, page 5-6
- Content Area, page 5-8

Header

Use the header to:

- Identify the current user (your username)
- Access the online help

- Log out
- Access the About information, where you can find information about which ACS web interface version is installed.

These items appear on the right side of the header (see Figure 5-2).

Figure 5-2 Header

Related Topics

- Navigation Pane, page 5-6
- Content Area, page 5-8

Navigation Pane

Use the navigation pane to navigate through the drawers of the web interface (see Figure 5-3).

Figure 5-3 Navigation Pane

Table 5-3 describes the function of each drawer.

Table 5-3 Navigation Pane Drawers

Drawer	Function
My Workspace	Access the Task Guide and Welcome page with shortcuts to common tasks and links to more information. See Chapter 5, "Understanding My Workspace" for more information.
Network Resources	Configure network devices, AAA clients, and network device groups. See Chapter 7, "Managing Network Resources" for more information.
Users and Identity Stores	Configure internal users and identity stores. See Chapter 8, "Managing Users and Identity Stores" for more information.
Policy Elements	Configure policy conditions and results. See Chapter 9, "Managing Policy Elements" for more information.

Table 5-3 Navigation Pane Drawers (continued)

Drawer	Function
Access Policies	Configure access policies. See Chapter 10, "Managing Access Policies" for more information.
Monitoring and Reports	View log messages. See Chapter 11, "Monitoring and Reporting in ACS" for more information.
System Administration	Administer and maintain your ACS. See Chapter 16, "Managing System Administrators" for more information.

To open a drawer, click it. A list of options for that drawer appears. You can view the contents of only one drawer at a time. When you open a drawer, any previously open drawer automatically closes. Click an option to view the hierarchy of items and the current configuration, and perform configuration tasks associated with that option in the content area. See Content Area, page 5-8 for more information about the content area.

To hide the navigation pane and expand the content area, click the collapse arrow, which is centered vertically between the navigation pane and content area. Click the collapse arrow again to reveal the navigation pane.

The options listed beneath drawers in the navigation pane are organized in a tree structure, where appropriate. The options in the tree structure are dynamic and can change based on administrator actions. Creating, deleting, or renaming objects in the content area can change the option display in the navigation pane. For example, beneath the **Network Resources > Network Device Groups** option, there are two preconfigured network device groups (options)—Location and Device Type. Figure 5-4 shows that the administrator has used the Network Device Groups option page to create an additional network device group called Business, which appears in the tree structure in the navigation pane.

Figure 5-4 Navigation Pane—Dynamic Tree Structure

Related Topics

- Header, page 5-5
- Content Area, page 5-8

Content Area

Use the content area to view your current location in the interface, view your configuration, configure AAA services, and administer your ACS.

The content area can contain:

- Web Interface Location, page 5-8
- List Pages, page 5-8
- Secondary Windows, page 5-13
- Rule Table Pages, page 5-16

Web Interface Location

Your current location in the interface appears at the top of the content area. Figure 5-5 shows that the location is the Policy Elements drawer and the Network Devices and AAA Clients page. Using this location as an example, ACS documentation uses this convention to indicate interface locations—**Policy Elements > Policy Conditions > Network Devices and AAA Clients > Location**. The remainder of the content area shows the content of the chosen page.

The interface location also displays the action that you are configuring. For example, if you are in the **Users and Identity Stores > Internal Identity Stores > Users** page and you attempt to duplicate a specific user, the interface location is stated as:

Users and Identity Stores > Internal Identity Stores > Users > Duplicate: <*user_name*>, where <*user_name*> is the name of the user you chose to duplicate. ACS documentation also uses this convention.

List Pages

List pages contain a list of items (see Figure 5-5).

You can use list pages to delete one or more items from an option that you chose in the navigation pane.

Figure 5-5 List Page

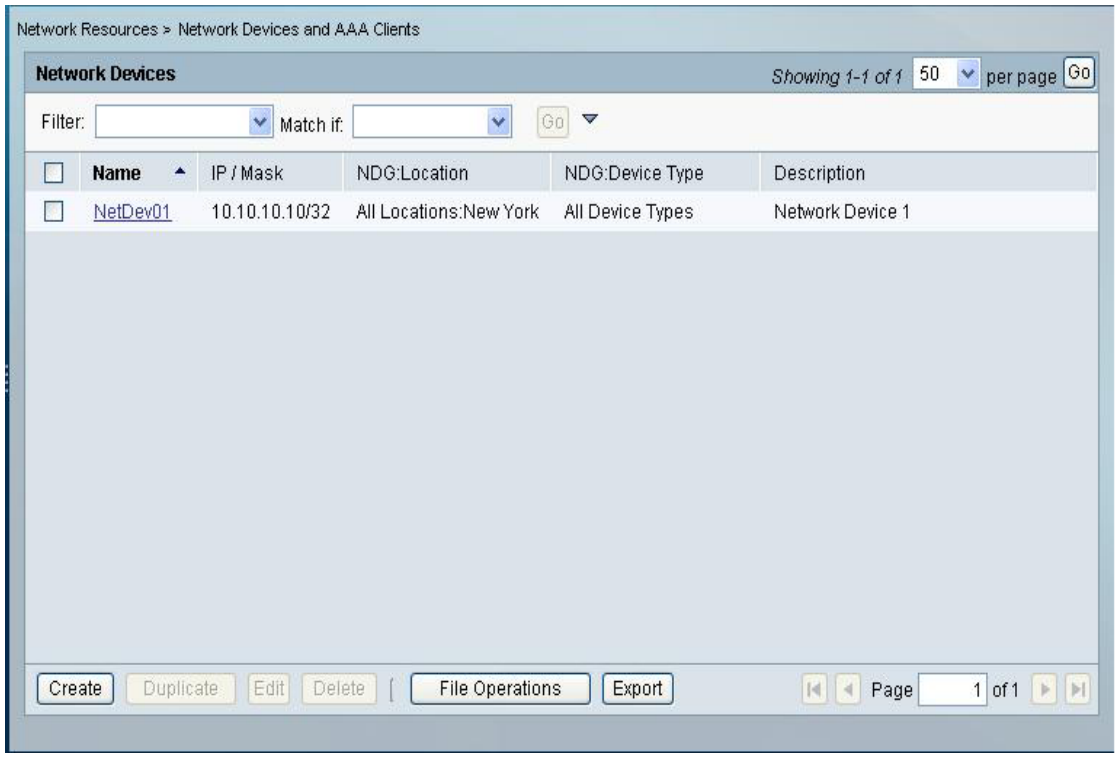


Table 5-4 describes the content area buttons and fields that list pages have in common.

Table 5-4 Common Content Area Buttons and Fields for List Pages

Button or Field	Description
Rows per page	Use the drop-down list to specify the number of items to display on this page. Options: • 10—Up to 10. • 25—Up to 25. • 50—Up to 50. • 100—Up to 100.
Go	Click to display the number of items you specify in the Rows per page field.
Check box or radio button	Chooses or does not choose items in a list, for edit, duplicate, or delete actions. Options: • Check (a check box) or click (a radio button)—Chooses an item. Check the check box in the header row to choose all items in the list. Check the individual check boxes to choose specific items in the list. • Uncheck (a check box) or unclick (a radio button)—Does not choose an item.
List column	A tabular or hierarchical view of items associated with a specific configuration task. Figure 5-5 shows the list column as a list of configured network device names; the heading of this list column is Name.

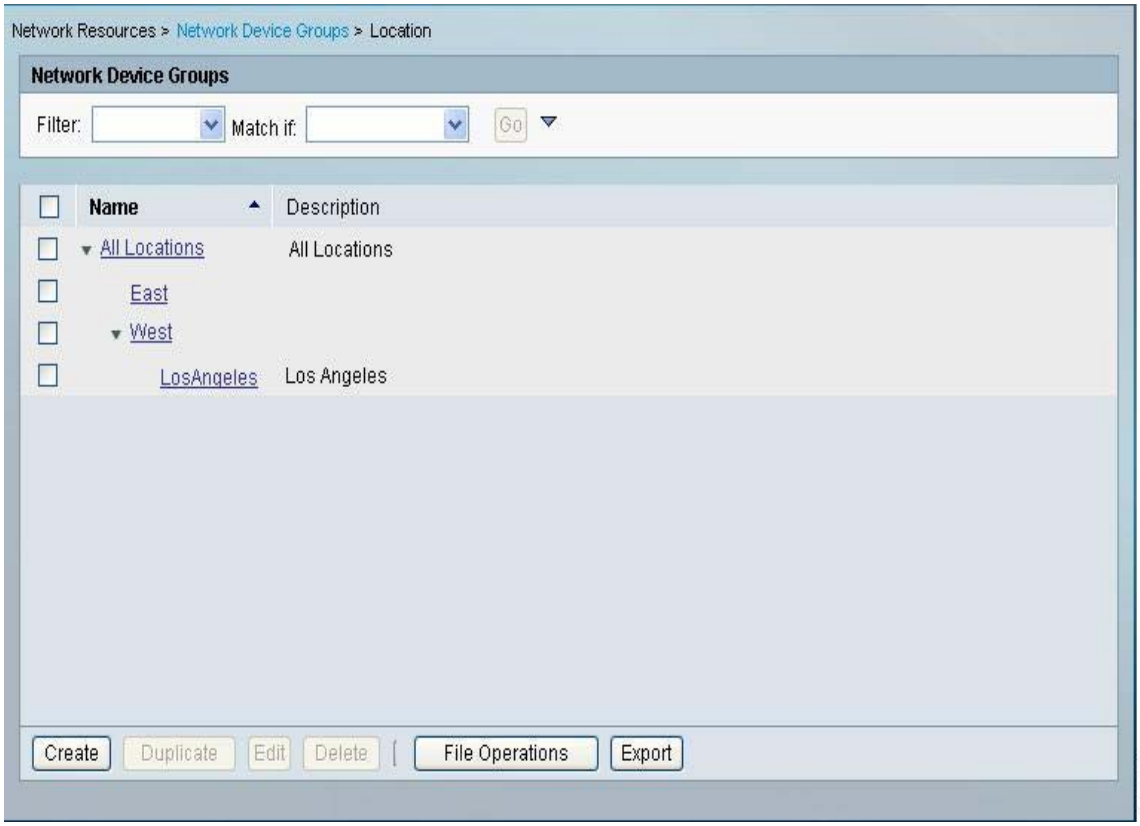
Table 5-4 Common Content Area Buttons and Fields for List Pages (continued)

Button or Field	Description
Scroll bar	Use the content area scroll bar to view all the data in a page, if needed.
Create	Click to create a new item. A wizard or single page appears in the content area. **Note** When you click Create, any selections that you made in the content area are ignored and the content area displays an Edit page with page-specific default values, if any.
Duplicate	Click to duplicate a selected item. A single page or a tabbed page appears in the content area.
Edit	Click to edit a selected item. A single page or a tabbed page appears in the content area.
Delete	Click to delete one or more selected items. A dialog box that queries `Are you sure you want to delete item/items?` appears for the item, or items, you chose to delete. The confirmation dialog box contains OK and Cancel. Click: • OK—Deletes the selected item or items. The list page appears without the deleted item. • Cancel—Cancels the delete operation. The list page appears with no changes. **Note** You can only delete items that you can view on a page, including the content of a page that you can view by using the scroll bar. For tables that span more than one page, your selections of rows to delete for pages that you cannot view are ignored and those selections are not deleted.
Page <*num*> of n	Enter the number of the page you want to display in the content area of the list page, where <*num*> is the page you want to display, then click **Go**. **Note** Not available for tree table pages.
Direction arrows	Click the arrows on the lower right side of the content area to access the first page, previous page, next page, or last page. The arrows are active when required. **Note** Not available for tree table pages.

Tree table pages are a variation of list pages (see Figure 5-6). You can perform the same operations on tree table pages that you can on list pages, except for paging. In addition, with tree table pages:

- A darker background color in a row indicates the top level of a tree.
- If the first folder of a tree contains fewer than 50 items, the first folder is expanded and all others are collapsed. You must use the expanding icon (+) to view the contents of the collapsed folders.
- If the first folder of a tree contains 50 or more items, all folders in the tree are collapsed. You must click the expanding icon (+) to view the contents of the folders.
- If you check the check box for a folder (a parent), it chooses all children of that folder.
- If you check the check box of a folder (a parent), and then uncheck any of the children, the parent folder is unchecked automatically.

Figure 5-6 Tree Table Page



Filtering

Large lists in a content area window or a secondary window (see Figure 5-9) can be difficult to navigate through and select the data that you want. You can use the web interface to filter data in these windows to reduce the data that appears in a list, based on criteria and conditions that you choose. Table 5-5 describes the filtering options.

Note Not all filtering options are available in all fields.

Table 5-5 Filtering in the Content Area Window and Secondary Windows

Button or Field	Description
Filter (drop-down list box)	Select the name of the column from the drop-down list box on which to filter.
Match if (drop-down list box)	Select the condition you want to apply to your filter action: • Contains • Doesn't Contain • Ends With • Equals • Is Empty • Not Empty • Not Equals • Starts With The condition is applied to the column you select in the Filter drop-down list box.
v (down arrow)	Click to add an additional filter row on which to choose conditions to narrow or expand your filter action. The text `And:` precedes the additional filter row.
^ (up arrow)	Click to remove an extraneous filter row.
Go	Click to execute your filter action.
Clear Filter	Click to clear any current filter options.
OK	Click to add the selected data to your configuration and close the secondary window. **Note** This button is only available in secondary windows (see Figure 5-9).

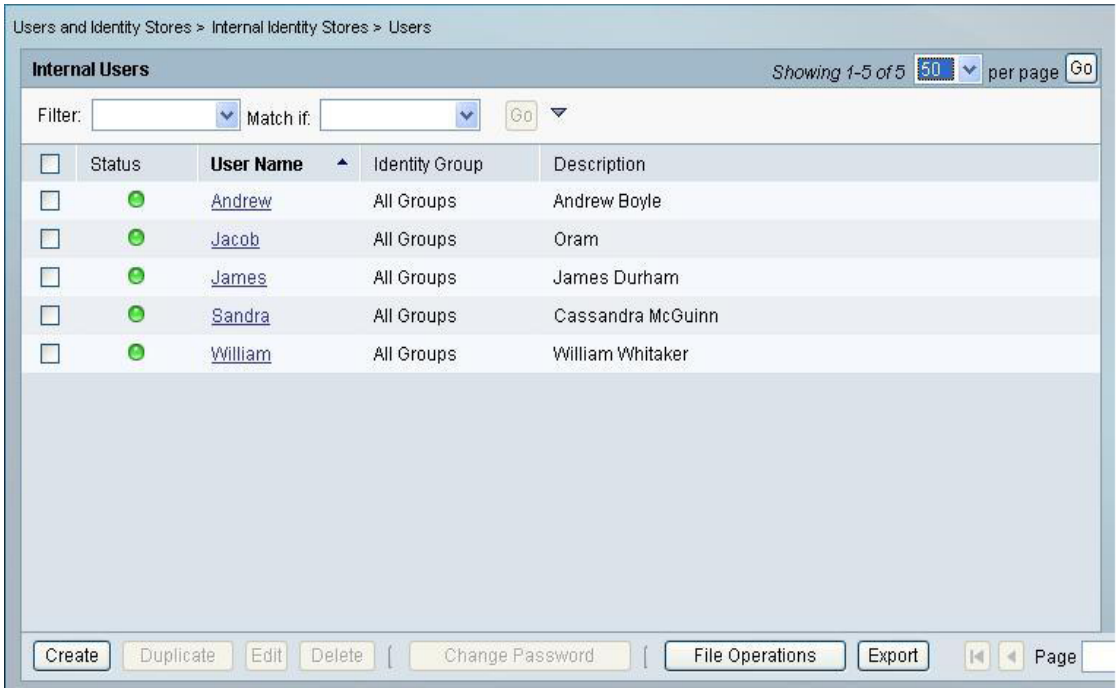
Note For tree table pages, you can only perform filtering on a root node, the top-most parent.

Sorting

Most nontree list pages support sorting by the Name column or the Description column, when available. You can sort pages in an ascending or descending manner. For pages that do not have a Name or Description column, the sorting mechanism may be supported in the left-most column of the page, or the Description column. Place your cursor over a column heading to determine if sorting is available for a column. If sorting is available, the cursor turns into a hand and the text `Click to sort` appears.

When a table is sorted, the column heading text darkens and an up arrow or down arrow appears next to the text (see Figure 5-7). Click the arrow to resort in the opposing manner.

Figure 5-7 Sorting Example



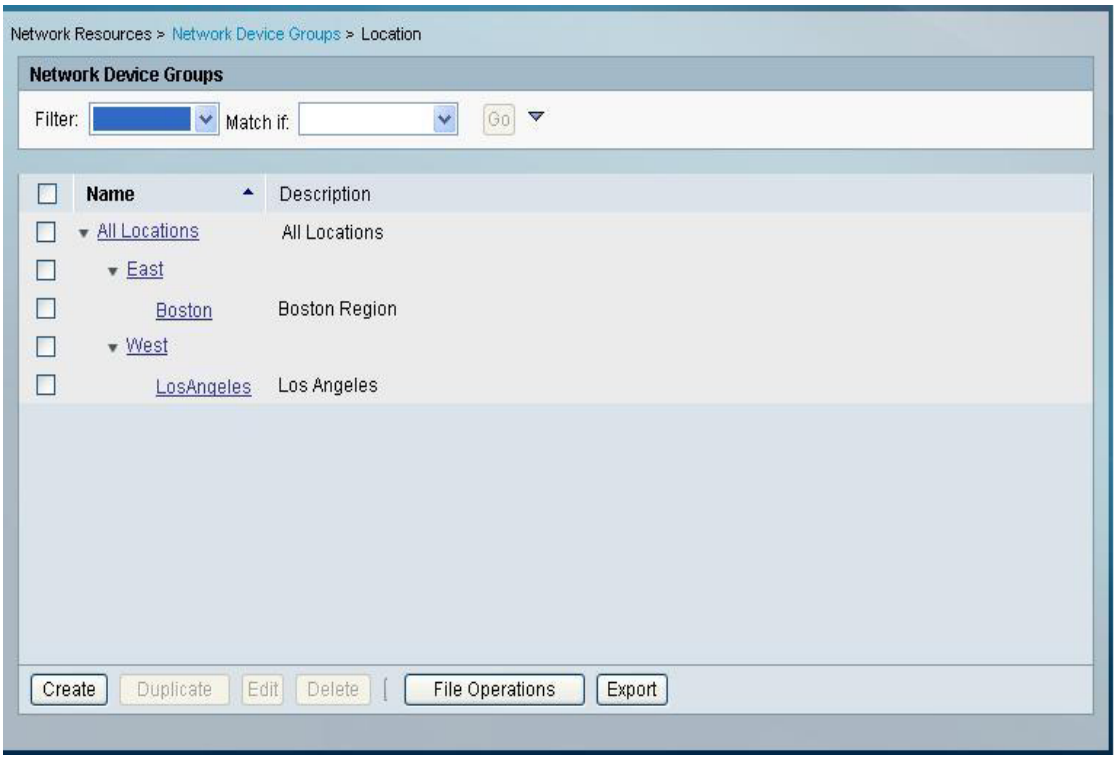
Secondary Windows

The content area serves as the launching place for any secondary (popup) windows that you access by clicking Select (see Figure 5-8) from single, tabbed, or wizard pages. You use these secondary windows to filter and select data that you want to use in your configuration (see Figure 5-9 and Table 5-5).

You can select one or more items from a secondary window to include in your configuration, dependent upon the selection option—items listed in a secondary window with radio buttons allow you to select one item to include in your configuration and items listed with check boxes allow you to select multiple items.

Figure 5-8 Select Button—Accesses Secondary Windows

Figure 5-9 Secondary Window



In addition to selecting and filtering data, you can create a selectable object within a secondary window. For example, if you attempt to create a users internal identity store, and click **Select** to assign the store to an identity group (a selectable object), but the identity group you want to associate it with is not available for selection, you can click **Create** within the secondary window to create the object you want. After you have created the object and clicked Submit, the secondary window is refreshed with the newly created object, which you can then select for your configuration. In our example, you can select the newly created identity group to assign it to the users internal identity store.

Transfer Boxes

Transfer boxes are a common element in content area pages (see Figure 5-10). You use these boxes to select and remove items for use in your configuration and order them according to your needs. Figure 5-10 shows the transfer box options. Table 5-6 describes the transfer box options.

Figure 5-10 Transfer Box

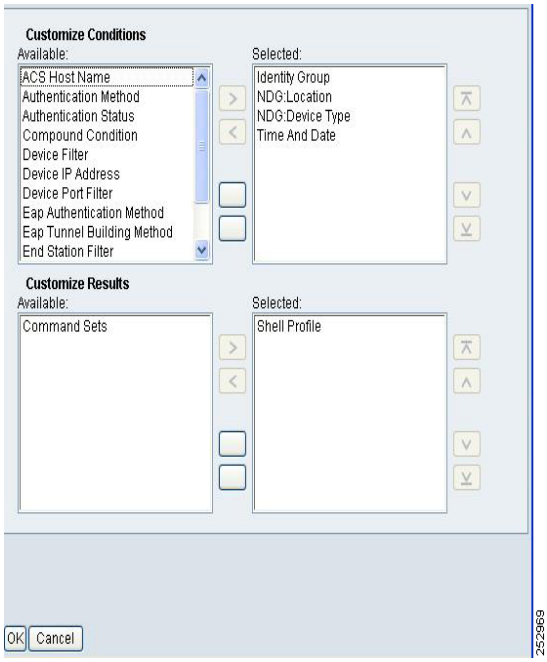


Table 5-6 Transfer Box Fields and Buttons

Field or Button	Description
Available	List of available items for selection.
Selected	Ordered list of selected items.
Right arrow (>)	Click to move one selected item from the Available list to the Selected list.
Left arrow (<)	Click to move one selected item from the Selected list to the Available list.
Double right arrow (>>)	Click to move all items from the Available list to the Selected list.
Double left arrow (<<)	Click to move all items from the Selected list to the Available list.
Up arrow with above score	Click to move one selected item to the top of the ordered Selected items list.
Up arrow	Click to move one selected item up one position in the ordered Selected items list.
Down arrow	Click to move one selected item down one position in the ordered Selected items list.
Down arrow with underscore	Click to move one selected item to the bottom of the ordered Selected items list.

Schedule Boxes

Schedule boxes are a common element in content area pages (see Figure 5-10). You use them to select active times for a policy element from a grid, where each row represents a day of the week and each square in a row represents an hour in a day. Click one square to make one hour active. Table 5-7 describes the Schedule box options.

Figure 5-11 Schedule Box

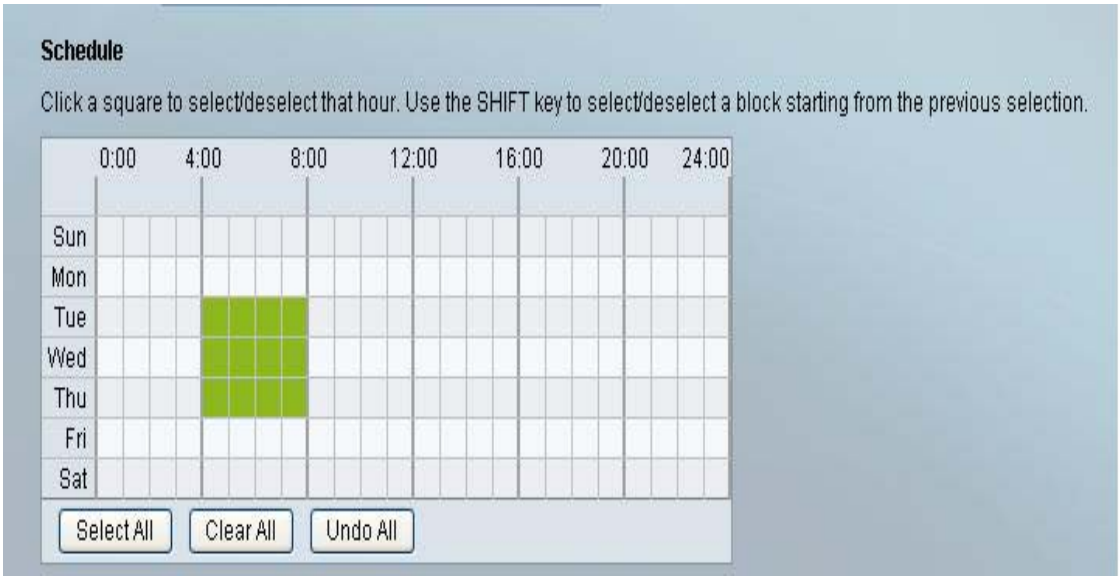


Table 5-7 Schedule Box Fields and Buttons

Field or Button	Description
Mon	A row that indicates Monday of every week of every year.
Tue	A row that indicates Tuesday of every week of every year.
Wed	A row that indicates Wednesday of every week of every year.
Thu	A row that indicates Thursday of every week of every year.
Fri	A row that indicates Friday of every week of every year.
Sat	A row that indicates Saturday of every week of every year.
Sun	A row that indicates Sunday of every week of every year.
0:00 to 24:00	Indicates the hours of a day in columns, where 0:00 = the hour that begins the second after midnight Eastern Standard Time (EST), and 24:00 = midnight to 1:00 a.m., in the time zone in which your ACS instance is located.
Square (of the grid)	Click one square to make one hour active.
Set All	Click to select all squares (hours).
Clear All	Click to deselect all squares (hours).
Undo All	Click to remove your most recent selections.

Rule Table Pages

Rule table pages display the rules that comprise policies. You can reorder rules within a rule table page and submit the policy that is associated with a table. You can access properties and customization pages from rule tables to configure your policies. For more information on specific rule table pages, and properties and customization pages, see Managing Access Policies.

Directly above the rule table are two display options:

- Standard Policy—Click to display the standard policy rule table.

- Exception Policy—Click to display the exception policy rule table, which takes precedence over the standard policy rule table content.

Table 5-8 describe the common options of standard and exception rule table pages:

Table 5-8 Rule Table Page Options

Option	Description
#	The ordered column of rules within the rule table. You can renumber the rules by reordering, adding, or deleting rules and then clicking **Save Changes** to complete the renumbering. New rules are added to the end of the ordered column, so you must reorder them if you want to move a new rule to a different position within the ordered list. **Note** You cannot reorder the default (catch-all) rule, which remains at the bottom of the rule table.
Check box	Click one or more check boxes to select associated rules on which to perform actions.
Status	(*Display only.*) Indicates the status of rules within the rule table. The status can be: • Enabled—Indicated by a green (or light colored) circle with a white check mark. • Disabled—Indicated by a red (or dark colored circle) with a white x. • Monitor-only—Indicated by a gray circle with a black i.
Name	A unique name for each rule (except the default, catch-all rule). Click a name to edit the associated rule. When you add a new rule, it is given a name in the format `Rule-<num>`, where <*num*> is the next available consecutive integer. You can edit the name to make it more descriptive. Cisco recommends that you name rules with concatenation of the rule name and the service and policy names.
Conditions	A variable number of condition types are listed, possibly in subcolumns, dependent upon the policy type.
Results	A variable number of result types are listed, possibly in subcolumns, dependent upon the policy type.
Hit Counts column	View the hits counts for rules, where hits indicate which policy rules are invoked.
Rules scroll bar	Use the scroll bar at the right of the rules rows to scroll up and down the rules list.
Conditions and results scroll bar	Use the scroll bar beneath the Conditions and Results columns to scroll left and right through the conditions and results information.
Default rule	Click to configure the catch-all rule. This option is not available for exception policy rule tables.
Customize	Click to open a secondary window where you can determine the set and order of conditions and results used by the rule table.
Hit Counts button	Click to open a secondary window where you can: • View when the hit counters were last reset or refreshed. • View the collection period. • Request a reset or refresh of the hit counts. See Displaying Hit Counts, page 10-10 for more information.
Move to...	Use the ^ and v buttons to reorder selected rules within the rule table.
Save Changes	Click to submit your configuration changes.
Discard Changes	Click to discard your configuration changes prior to saving them.

Related Topic

- ACS 5.x Policy Model

Importing and Exporting ACS Objects through the Web Interface

You can use the import functionality in ACS to add, update, or delete multiple ACS objects at the same time. ACS uses a comma-separated values (CSV) file to perform these bulk operations. This *.csv* file is called an import file. ACS provides a separate *.csv* template for add, update, and delete operations for each ACS object. The first record in the .csv file is the header record from the template that contains column (field) names. You must download these templates from the ACS web interface. The header record from the template must be included in the first row of any .csv file that you import.

Note You cannot use the same template to import all the ACS objects. You must download the template that is designed for each ACS object and use the corresponding template while importing the objects. However, you can use the export file of a particular object, retain the header and update the data, and use it as the import file of the same object.

You can use the export functionality to create a *.csv* file that contains all the records of a particular object type that are available in the ACS internal store.

Note You must have CLI administrator-level access to perform import and export operations. Additionally:

- To import ACS configuration data, you need CRUD permissions for the specific configuration object.
- To export data to a remote repository, you need read permission for the specific configuration object.

This functionality is not available for all ACS objects. This section describes the supported ACS objects and how to create the import files.

This section contains:

- Supported ACS Objects, page 5-18
- Creating Import Files, page 5-20

Supported ACS Objects

While ACS 5.1 allows you to perform bulk operations (add, update, delete) on ACS objects using the import functionality, you cannot import all ACS objects. The import functionality in ACS 5.1 supports the following ACS objects:

- Users
- Hosts
- Network Devices
- Identity Groups
- NDGs
- Downloadable ACLs
- Command Sets

Table 5-9 lists the ACS objects, their properties, and the property data types. The import template for each of the objects contains the properties described in this table.

Table 5-9 ACS Objects – Property Names and Data Types

Property Name	Property Data Type
Object Type: User	
Username	(Required in create, edit, and delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Enabled	(Required in create) Boolean.
Change Password	(Required in create) Boolean.
Password	(Required in create) String. Maximum length is 32 characters. Not available in Export.
Enable Password	(Optional) String. Maximum length is 32 characters.
User Identity Group	(Optional) String. Maximum length is 256 characters.
List of attributes	(Optional) String and other data types.
Object Type: Hosts	
MAC address	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Enabled	(Optional) Boolean.
Host Identity Group	(Optional) String. Maximum length is 256 characters.
List of attributes	(Optional) String.
Object Type: Network Device	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Subnet	(Required in create) String.
Support RADIUS	(Required in create) Boolean.
RADIUS secret	(Optional) String. Maximum length is 32 characters.
Support TACACS	(Required in create) Boolean.
TACACS secret	(Optional) String. Maximum length is 32 characters.
Single connect	(Optional) Boolean.
Legacy TACACS	(Optional) Boolean.
Support CTS	(Required in create) Boolean.
CTS Identity	(Optional) String. Maximum length is 32 characters.
CTS trusted	(Optional) Boolean.
Password	(Optional) String. Maximum length is 32 characters.
sgACLTTL	(Optional) Integer.
peerAZNTTL	(Optional) Integer.
envDataTTL	(Optional) Integer.
Session timeout	(Optional) Integer.
List of NDG names	(Optional) String.
Object Type: Identity Group	

Table 5-9 ACS Objects – Property Names and Data Types (continued)

Property Name	Property Data Type
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Object Type: NDG	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Object Type: Downloadable ACLs	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Content	(Required in create, edit, delete) String. Maximum length is 1024 characters.
Object Type: Command Set	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Commands (in the form of *grant*:*command*:*arguments*)	(Optional) String. **Note** This is a list with semi separators (:) between the values that you supply for *grant*.

Note Fields that are optional can be left empty and ACS substitutes the default values for those fields. For example, when fields that are related to a hierarchy are left blank, ACS assigns the value of the root node in the hierarchy. For network devices, if TrustSec is enabled, all the related configuration fields are set to default values.

Creating Import Files

This section describes how to create the *.csv* file for performing bulk operations on ACS objects. You can download the appropriate template for each of the objects from the ACS web interface. This section contains the following:

- Downloading the Template from the Web Interface, page 5-20
- Understanding the CSV Templates, page 5-21
- Creating the Import File, page 5-22

Downloading the Template from the Web Interface

Before you can create the import file, you must download the import file templates from the ACS web interface.

To download the import file templates for adding internal users:

Step 1 Log in to the ACS 5.1 web interface.

Step 2 Choose **Users and Identity Stores > Internal Identity Stores > Users**.

The Users page appears.

Step 3 Click **File Operations**.

The File Operations wizard appears.

Step 4 Choose any one of the following:

- Add—Adds users to the existing list. This option does not modify the existing list. Instead, it performs an append operation.
- Update—Updates the existing internal user list.
- Delete—Deletes the list of users in the import file from the internal identity store.

Step 5 Click **Next**.

The Template page appears.

Step 6 Click **Download Add Template**.

Step 7 Click **Save** to save the template to your local disk.

The following list gives you the location from which you can get the appropriate template for each of the objects:

- User—**Users and Identity Stores > Internal Identity Stores > Users**
- Hosts—**Users and Identity Stores > Internal Identity Stores > Hosts**
- Network Device—**Network Resources > Network Devices and AAA Clients**
- Identity Group—**Users and Identity Stores > Identity Groups**
- NDG
  - Location—**Network Resources > Network Device Groups > Location**
  - Device Type—**Network Resources > Network Device Groups > Device Type**
- Downloadable ACLs—**Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs**
- Command Set—**Policy Elements > Authorization and Permissions > Device Administration > Command Sets**

Follow the procedure described in this section to download the appropriate template for your object.

Understanding the CSV Templates

You can open your CSV template in Microsoft Excel or any other spreadsheet application and save the template to your local disk as a *.csv* file. The *.csv* template contains a header row that lists the properties of the corresponding ACS object.

For example, the internal user Add template contains the fields described in Table 5-10:

Table 5-10 Internal User Add Template

Header Field	Description
name:String(64):Required	Username of the user.
description:String(1024)	Description of the user.
enabled:Boolean(true,false):Required	A boolean field that indicates whether the user must be enabled or disabled.

Table 5-10 Internal User Add Template (continued)

Header Field	Description
changePassword:Boolean(true,false): Required	A boolean field that indicates whether the user must change password on first login.
password:String(32):Required	Password of the user.
enablePassword:String(32)	Enable password of the user.
UserIdentityGroup:String(256)	Identity group to which the user belongs.
All the user attributes that you have specified would appear here.	

Each row of the *.csv* file corresponds to one internal user record. You must enter the values into the *.csv* file and save it before you can import the users into ACS. See Creating the Import File, page 5-22 for more information on how to create the import file.

This example is based on the internal user Add template. For the other ACS object templates, the header row contains the properties described in Table 5-9 for that object.

Creating the Import File

After you download the import file template to your local disk, enter the records that you want to import into ACS in the format specified in the template. After you enter all the records into the *.csv* file, you can proceed with the import function. The import process involves the following:

- Adding Records to the ACS Internal Store, page 5-22
- Updating the Records in the ACS Internal Store, page 5-23
- Deleting Records from the ACS Internal Store, page 5-24

Adding Records to the ACS Internal Store

When you add records to the ACS internal store, you add the records to the existing list. This is an append operation, in which the records in the *.csv* file are added to the list that exists in ACS.

To add internal user records to the Add template:

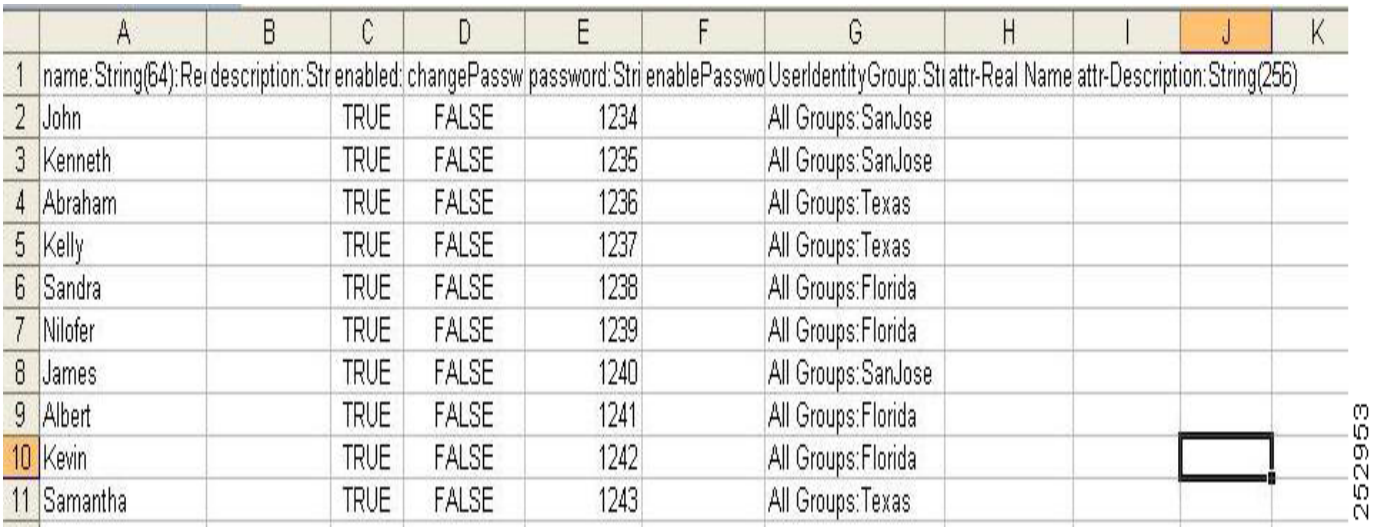
Step 1 Download the internal user Add template. See Downloading the Template from the Web Interface, page 5-20 for more information.

Step 2 Open the internal user Add template in Microsoft Excel or any other spreadsheet application. See Table 5-9 for a description of the fields in the header row of the template.

Step 3 Enter the internal user information. Each row of the .csv template corresponds to one user record.

Figure 5-12 shows a sample Add Users import file.

Figure 5-12 Add Users – Import File



	A	B	C	D	E	F	G	H	I	J	K
1	name:String(64):Re	description:Str	enabled:	changePassw	password:Stri	enablePasswo	UserIdentityGroup:Str	attr-Real Name	attr-Description:String(256)		
2	John		TRUE	FALSE	1234		All Groups:SanJose				
3	Kenneth		TRUE	FALSE	1235		All Groups:SanJose				
4	Abraham		TRUE	FALSE	1236		All Groups:Texas				
5	Kelly		TRUE	FALSE	1237		All Groups:Texas				
6	Sandra		TRUE	FALSE	1238		All Groups:Florida				
7	Nilofer		TRUE	FALSE	1239		All Groups:Florida				
8	James		TRUE	FALSE	1240		All Groups:SanJose				
9	Albert		TRUE	FALSE	1241		All Groups:Florida				
10	Kevin		TRUE	FALSE	1242		All Groups:Florida				
11	Samantha		TRUE	FALSE	1243		All Groups:Texas				

252953

Step 4 Save the add users import file to your local disk.

Updating the Records in the ACS Internal Store

When you update the records in the ACS store, the import process overwrites the existing records in the internal store with the records from the *.csv* file. This operation replaces the records that exist in ACS with the records from the *.csv* files.

The update operation is similar to the add operation except for one additional column that you can add to the Update templates. The Update template can contain an Updated name column for internal users and other ACS objects, and an Updated MAC address column for the internal hosts. The Updated Name replaces the name.

Timesaver Instead of downloading the update template for each of the ACS objects, you can use the export file of that object, retain the header row, and update the data to create your update .csv file.

Note To add an updated name or MAC address to the ACS objects, you have to download and use the particular update template. Also, for the NDGs, the export template contains only the NDG name, so in order to update any other property, you must download and use the NDG update template.

For example, Figure 5-13 shows a sample import file that updates existing user records.

Figure 5-13 Update Users–Import File

	A	B	C	D	E	F	G	H	I	J	K	L
1	name:Strir	Updated name:Strir	description	enabled:B(	changePas	password:!	enablePas	UserIdentit	attr-Real N	attr-Description:String(256)		
2	John	Mark		TRUE	FALSE	1234		All Groups:SanJose				
3	Kenneth	David		TRUE	FALSE	1235		All Groups:SanJose				
4	Abraham	Jamie		TRUE	FALSE	1236		All Groups:Texas				
5	Kelly	Lucy		TRUE	FALSE	1237		All Groups:Texas				
6	Sandra	Tina		TRUE	FALSE	1238		All Groups:Florida				
7	Nilofer	William		TRUE	FALSE	1239		All Groups:Florida				
8	James	Frank		TRUE	FALSE	1240		All Groups:SanJose				
9	Albert	George		TRUE	FALSE	1241		All Groups:Florida				
10	Kevin	Paul		TRUE	FALSE	1242		All Groups:Florida				
11	Samantha	Patrick		TRUE	FALSE	abcd		All Groups:Texas				

252971

Note The second column, Updated name, is the additional column that you can add to the Update template.

Deleting Records from the ACS Internal Store

You can use this option to delete a subset of records from the ACS internal store. The records that are present in the *.csv* file that you import are deleted from the ACS internal store. The Delete template contains only the key column to identify the records that must be deleted.

For example, to delete a set of internal users from the ACS internal identity store, download the internal user Delete template and add the list of users that you want to delete to this import file. Figure 5-14 shows a sample import file that deletes internal user records.

Timesaver To delete all users, you can export all users and then use the same export file as your import file to delete users.

Figure 5-14 Delete Users – Import File

	A	B	C	D	E	F
1	name:String(64):Required					
2	kenneth					
3	jamie					
4	john					
5	joseph					
6	nilofer					
7	casey					
8	lucie					
9	jacob					
10	george					

252956

Common Errors

You might encounter these common errors:

- Concurrency Conflict Errors, page 5-25
- Deletion Errors, page 5-26
- System Failure Errors, page 5-26
- Accessibility, page 5-27

Concurrency Conflict Errors

Concurrency conflict errors occur when more than one user tries to update the same object. When you click Submit and the web interface detects an error, a dialog box appears, with an error message and OK button. Read the error message, click **OK**, and resubmit your configuration, if needed.

Possible error messages, explanations, and recommended actions are:

Error Message `The item you are trying to Submit has been modified elsewhere while you were making your changes.`

Explanation You accessed an item to perform an edit and began to configure it; simultaneously, another user accessed and successfully submitted a modification to it. Your submission attempt failed.

Recommended Action Click **OK** to close the error message and display the content area list page. The page contains the latest version of all items. Resubmit your configuration, if needed.

Error Message `The item you are trying to Submit has been deleted while you were making your changes.`

Explanation If you attempt to submit an edited item that another user simultaneously accessed and deleted, your submission attempt fails. This error message appears in a dialog box with an OK button.

Recommended Action Click **OK** to close the error message and display the content area list page. The page contains the latest version of all items. The item that you tried to submit is not saved or visible.

Error Message `The item you are trying to Duplicate from has been deleted.`

Error Message `The item you are trying to Edit has been deleted.`

Explanation You attempted to duplicate or edit a selected item that another user deleted at the same time that you attempted to access it.

Recommended Action Click **OK** to close the error message and display the content area list page. The page contains the latest version of all items. The item that you tried to duplicate or edit is not saved or visible.

Error Message `The item you are trying to Submit is referencing items that do not exist anymore.`

Explanation You attempted to edit or duplicate an item that is referencing an item that another user deleted while you tried to submit your change.

Recommended Action Click **OK** to close the error message and display the previous page, the Create page or the Edit page. Your attempted changes are not saved, nor do they appear in the page.

Error Message `Either Import or Export is already in progress.`

Explanation You attempted to import or export a .csv file while a previous import or export is still in progress. The subsequent import or export will not succeed. The original import or export is not interrupted due to this error.

Recommended Action Click **OK** to close the error message and display the previous page. For a currently running import process, consult the Import Progress secondary window and wait for the Save Log button to become enabled. Save the log, then attempt to import or export your next .csv file.

Deletion Errors

Deletion errors occur when you attempt to delete an item (or items) that another item references. When you click Delete and an error is detected, a dialog box appears, with an error message and OK button. Read the error message, click **OK**, and perform the recommended action.

Possible error messages, explanations, and recommended actions are:

Error Message `The item you are trying to Delete is referenced by other Items. You must remove all references to this item before it can be deleted.`

Error Message `Some of the items you are trying to Delete are referenced by other Items. You must remove all references to the items before they can be deleted.`

Explanation If you attempt to delete one or more items that another item references, the system prevents the deletion.

Recommended Action Click **OK** to close the error message and display the content area list page. Your deletion does not occur and the items remain visible in the page. Remove all references to the item or items you want to delete, then perform your deletion.

System Failure Errors

System failure errors occur when a system malfunction is detected. When a system failure error is detected, a dialog box appears, with an error message and OK button. Read the error message, click **OK**, and perform the recommended action.

Possible error messages, explanations, and recommended actions are:

Error Message `The following System Failure occurred: <description>.`

Where <*description*> describes the specific malfunction.

Explanation You have attempted to make a configuration change and the system detected a failure at the same time.

Recommended Action Click **OK** to close the error message and display the content area list page. Your changes are not saved. Investigate and troubleshoot the detected malfunction, if possible.

Error Message `An unknown System Failure occurred.`

Explanation You tried to change the configuration and the system detected an unknown failure at the same time.

Recommended Action Click **OK** to close the error message and display the content area list page. Investigate possible system failure causes, if possible.

Accessibility

The ACS 5.1 web interface contains accessibility features for users with vision impairment and mobility limitations.

This section contains the following topics:

- Display and Readability Features, page 5-27
- Keyboard and Mouse Features, page 5-28
- Obtaining Additional Accessibility Information, page 5-28

Display and Readability Features

The ACS 5.1 web interface includes features that:

- Increase the visibility of items on the computer screen.
- Allow you to use screen reader software to interpret the web interface text and elements audibly.

The display and readability features include:

- Useful text descriptions that convey information that appears as image maps and graphs.
- Meaningful and consistent labels for tables, buttons, fields, and other web interface elements.
- Label placement directly on, or physically near, the element to which they apply.
- Color used as an enhancement of information only, not as the only indicator. For example, required fields are associated with a red asterisk.
- Confirmation messages for important settings and actions.
- User-controllable font, size, color, and contrast of the entire web interface.

Keyboard and Mouse Features

You can interact with the ACS 5.1 web interface by using the keyboard and the mouse to accomplish actions. The keyboard and mouse features include:

- Keyboard accessible links to pages that display dynamic content.
- Standard keyboard equivalents are available for all mouse actions.
- Multiple simultaneous keystrokes are not required for any action.
- Pressing a key for an extended period of time is not required for any action.
- Backspace and deletion are available for correcting erroneous entries.

Obtaining Additional Accessibility Information

For more information, refer to the Cisco Accessibility Program:

- E-mail: accessibility@cisco.com
- Web: http://www.cisco.com/go/accessibility

CHAPTER 6

Post-Installation Configuration Tasks

This chapter provides a set of configuration tasks that you must perform to work with ACS. This chapter contains the following sections:

- Configuring Minimal System Setup, page 6-1
- Configuring ACS to Perform System Administration Tasks, page 6-2
- Configuring ACS to Manage Access Policies, page 6-3
- Configuring ACS to Monitor and Troubleshoot Problems in the Network, page 6-4

Configuring Minimal System Setup

Table 6-1 lists the steps that you must follow for a minimal system setup to get ACS up and running quickly in a lab, evaluation, or demonstration environment.

Table 6-1 Minimal System Setup

Step No.	Task	Drawer	Refer to...
Step 1	Add network devices.	**Network Resources > Network Devices and AAA Clients**	Creating, Duplicating, and Editing Network Devices, page 7-10.
Step 2	Add users.	**Users and Identity Stores > Internal Identity Stores > Users**	Creating Internal Users, page 8-11.
Step 3	Create authorization rules to permit or deny access.	**Policy Elements > Authorization and Permissions**	Managing Authorizations and Permissions, page 9-18.

Configuring ACS to Perform System Administration Tasks

Table 6-2 lists the set of system administration tasks that you must perform to administer ACS.

Table 6-2 System Administration Tasks

Step No.	Task	Drawer	Refer to...
Step 1	Install ACS license.	**System Administration > Configuration > Licensing**	Licensing Overview, page 18-35.
Step 2	Install system certificates.	**System Administration > Configuration > Local Server Certificates > Local Certificates**	Configuring Local Server Certificates, page 18-14.
Step 3	Configure password policy rules for administrators and users.	• For administrators: **System Administration > Administrators > Settings > Authentication** • For administrator access settings: **System Administration > Administrators > Settings > Access** • For users: **System Administration > Users > Authentication Settings**	• For administrators: Configuring Authentication Settings for Administrators, page 16-9. • For administrator access settings: Configuring Administrator Access Settings, page 16-11 • For users: Configuring Authentication Settings for Users, page 8-9.
Step 4	Add ACS administrators.	**System Administration > Administrators > Accounts**	Configuring System Administrators and Accounts, page 16-3
Step 5	Configure primary and secondary ACS instances.	**System Administration > Operations > Distributed System Management**	Understanding Distributed Deployment, page 17-1.
Step 6	Configure logging.	**System Administration > Configuration > Log Configuration**	Configuring Logs, page 18-21.
Step 7	Add network devices.	**Network Resources > Network Devices and AAA Clients**	Creating, Duplicating, and Editing Network Devices, page 7-10.

Table 6-2 System Administration Tasks (continued)

Step No.	Task	Drawer	Refer to...
Step 8	Add users or hosts to the internal identity store, or define external identity stores, or both.	• For internal identity stores: **Users and Identity Stores > Internal Identity Stores** • For external identity stores: **Users and Identity Stores > External Identity Stores**	• For internal identity stores: – Creating Internal Users, page 8-11. – Creating Hosts in Identity Stores, page 8-15. • For external identity stores: – Creating External LDAP Identity Stores, page 8-22. – Configuring an AD Identity Store, page 8-43. – Creating and Editing RSA SecurID Token Servers, page 8-49. – Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-56.
Step 9	Add end user certificates.	**Users and Identity Stores > Certificate Authorities**	Adding a Certificate Authority, page 8-62.
Step 10	Configure identity sequence.	**Users and Identity Stores > Identity Store Sequences**	Creating, Duplicating, and Editing Identity Store Sequences, page 8-68.

Configuring ACS to Manage Access Policies

Table 6-3 lists the set of tasks that you must perform to manage access restrictions and permissions.

Table 6-3 Managing Access Policies

Step No.	Task	Drawer	Refer to...
Step 1	Define policy conditions.	**Policy Elements > Session Conditions**	Managing Policy Conditions, page 9-1.

Table 6-3 Managing Access Policies (continued)

Step No.	Task	Drawer	Refer to...
Step 2	Define authorization and permissions.	**Policy Elements > Authorization and Permissions**	Managing Authorizations and Permissions, page 9-18.
Step 3	Define access services and service selection policies.	**Access Policies > Access Services**	• To configure access services: Configuring Access Services, page 10-11. • To configure access service policies: Configuring Access Service Policies, page 10-20. • To configure compound conditions: Configuring Compound Conditions, page 10-42.

Configuring ACS to Monitor and Troubleshoot Problems in the Network

Table 6-4 lists a set of configuration tasks that you must perform to get the Monitoring & Report Viewer up and running.

Table 6-4 Monitoring and Troubleshooting Configuration

Step No.	Task	Drawer	Refer to...
Step 1	Configure data purge and backup.	**Monitoring Configuration > System Operations > Data Management**	Configuring Data Purging and Incremental Backup, page 15-2.
Step 2	Specify e-mail settings.	**Monitoring Configuration > System Configuration > Email Settings**	Specifying E-Mail Settings, page 15-13.
Step 3	Configure collection filters.	**Monitoring Configuration > System Configuration > Collection Filters**	Understanding Collection Filters, page 15-14.
Step 4	Enable system alarms and specify how you would like to receive notification.	**Monitoring Configuration > System Configuration > System Alarm Settings**	Configuring System Alarm Settings, page 15-16.

Table 6-4 Monitoring and Troubleshooting Configuration (continued)

Step No.	Task	Drawer	Refer to...
Step 5	Define schedules and create threshold alarms.	**Monitoring Configuration > System and Reports**	• To configure schedules: Understanding Alarm Schedules, page 12-7. • To create threshold alarms: Creating, Editing, and Duplicating Alarm Thresholds, page 12-9.
Step 6	Configure alarm syslog targets.	**Monitoring Configuration > System Configuration > Alarm Syslog Targets**	Configuring Alarm Syslog Targets, page 15-16.
Step 7	Configure remote database to export the Monitoring & Report Viewer data.	**Monitoring Configuration > System Configuration > Remote Database Settings**	Configuring Remote Database Settings, page 15-16.

CHAPTER 7

Managing Network Resources

The Network Resources drawer defines elements within the network that issue requests to ACS or those that ACS interacts with as part of processing a request. This includes the network devices that issue the requests and external servers, such as a RADIUS server that is used as a RADIUS proxy.

This drawer allows you to configure:

- Network Device Groups—Logically groups the network devices, which you can then use in policy conditions.
- Network Devices—Definition of all the network devices in the ACS device repository that accesses the ACS network.
- Default Network Device—A default network device definition that ACS can use for RADIUS or TACACS+ requests when it does not find the device definition for a particular IP address.
- External Servers—RADIUS servers that can be used as a RADIUS proxy.

When ACS receives a request from a network device to access the network, it searches the network device repository to find an entry with a matching IP address. ACS then compares the shared secret with the secret retrieved from the network device definition, and, if they match, the network device groups associated with the network device are retrieved and can be used in policy decisions. See ACS 5.x Policy Model for more information on policy decisions.

External Servers

The Network Resources drawer contains:

- Network Device Groups, page 7-1
- Network Devices and AAA Clients, page 7-5
- Configuring a Default Network Device, page 7-16
- Working with External RADIUS Servers, page 7-17

Network Device Groups

In ACS, you can define network device groups (NDGs), which are sets of devices. These NDGs provide logical grouping of devices, for example, Device Location or Type, which you can use in policy conditions. When the ACS receives a request for a device, the network device groups associated with that device are retrieved and compared against those in the policy table. With this method, you can group multiple devices and assign them the same policies. For example, you can group all devices in a specific location together and assign to them the same policy.

You can define up to 12 network device groups.

The Device Group Hierarchy is the hierarchical structure that contains the network device groups. Two of these, *Location* and *Device Type*, are predefined; you cannot change their names or delete them. You can add up to 10 additional hierarchies.

An NDG relates to any node in the hierarchy and is the entity to which devices are associated. These nodes can be any node within the hierarchy, not just leaf nodes.

Note You can have a maximum of six nodes in the NDG hierarchy, including the root node.

Related Topics

- Creating, Duplicating, and Editing Network Device Groups, page 7-2
- Deleting Network Device Groups, page 7-3

Creating, Duplicating, and Editing Network Device Groups

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a network device group:

Step 1 Choose **Network Resources > Network Device Groups**.

The Network Device Groups page appears. If you have defined additional network device groups, they appear in the left navigation pane, beneath the Network Device Groups option.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the network device group that you want to duplicate, then click **Duplicate**.
- Click the network device group name that you want to modify, or check the check box next to the name and click **Edit**.

The Hierarchy - General page appears.

Step 3 Modify the fields in the Hierarchy - General page as described in Table 7-1:

Table 7-1 Device Groups - General Page Field Descriptions

Field	Description
Name	Enter a name for the network device group (NDG).
Description	(Optional) Enter a description for the NDG.
Root Node Name/Parent	Enter the name of the root node associated with the NDG. The NDG is structured as an inverted tree, and the root node is at the top of the tree. The root node name can be the same as the NDG name. The root node name is displayed when you click an NDG in the Network Resources drawer.

Step 4 Click **Submit**.

The network device group configuration is saved. The Network Device Groups page appears with the new network device group configuration.

Related Topics

- Network Device Groups, page 7-1
- Deleting Network Device Groups, page 7-3
- Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy, page 7-3
- Performing Bulk Operations for Network Resources and Users, page 7-8

Deleting Network Device Groups

To delete a network device group:

Step 1 Choose **Network Resources > Network Device Groups**.

The Network Device Groups page appears.

Step 2 Check one or more check boxes next to the network device groups you want to delete, and click **Delete**.

The following error message appears:

```
You have requested to delete a network device group. If this group is referenced from a
network device definition, the network device will be modified to reference the root node
name group.
```

Step 3 Click **OK**.

The Network Device Groups page appears without the deleted network device groups.

Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy

You can arrange the network device group node hierarchy according to your needs by choosing parent and child relationships for new, duplicated, or edited network device group nodes. You can also delete network device group nodes from a hierarchy.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a network device group node within a hierarchy:

Step 1 Choose **Network Resources > Network Device Groups**.

The Network Device Groups page appears.

Step 2 Click **Location**, **Device Type**, or another previously defined network device group in which you want to create a new network device group, and add it to the hierarchy of that group.

The Network Device Group hierarchy page appears.

Step 3 Do one of the following:

- Click **Create**. If you click **Create** when you have a group selected, the new group becomes a child of the parent group you selected. You can move a parent and all its children around in the hierarchy by clicking **Select** from the Create screen.
- Check the check box next to the network device group name that you want to duplicate, then click **Duplicate**.
- Click the network device group name that you want to modify, or check the check box next to the name and click **Edit**.

The Device Group - General page appears.

Step 4 Modify fields in the Device Groups - General page as shown in Table 7-2:

Table 7-2 Device Groups - General Page Field Descriptions

Field	Description
Name	Enter a name for the NDG.
Description	(Optional) Enter a description for the NDG.
Parent	Enter the name of the parent associated with the NDG. The NDG is structured as an inverted tree, and the parent name is the name of the top of the tree. Click **Select** to open the Groups dialog box from which you can select the appropriate parent for the group.

Step 5 Click **Submit**.

The new configuration for the network device group is saved. The Network Device Groups hierarchy page appears with the new network device group configuration.

Related Topics

- Network Device Groups, page 7-1
- Deleting Network Device Groups, page 7-3
- Creating, Duplicating, and Editing Network Device Groups, page 7-2
- Performing Bulk Operations for Network Resources and Users, page 7-8

Deleting Network Device Groups from a Hierarchy

To delete a network device group from within a hierarchy:

Step 1 Choose **Network Resources > Network Device Groups**.

The Network Device Groups page appears.

Step 2 Click **Location**, **Device Type**, or another previously defined network device group in which you want to edit a network device group node.

The Network Device Groups node hierarchy page appears.

Step 3 Select the nodes that you want to delete and click **Delete**.

The following message appears:

```
You have requested to delete a network device group. If this group is referenced from a
network device definition, the network device will be modified to reference the root node
name group.
```

Step 4 Click **OK**.

The network device group node is removed from the configuration. The Network Device Groups hierarchy page appears without the device group node that you deleted.

Network Devices and AAA Clients

You must define all devices in the ACS device repository that access the network. The network device definition can be associated with a specific IP address or a subnet mask, where all IP addresses within the subnet can access the network. The device definition includes the association of the device to network device groups (NDGs). You also configure whether the device uses TACACS+ or RADIUS, and if it is a TrustSec device.

Note When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses.

You can import devices with their configurations into the network devices repository.

When ACS receives a request, it searches the network device repository for a device with a matching IP address; then ACS compares the secret or password information against that which was retrieved from the network device definition. If the information matches, the NDGs associated with the device are retrieved and can be used in policy decisions.

Note You must install TrustSec license to enable TrustSec options. The TrustSec options only appear if you have installed the TrustSec license. For more information on TrustSec licenses, see Licensing Overview, page 18-35.

Viewing and Performing Bulk Operations for Network Devices

You can view the network devices and AAA clients. These are the devices sending access requests to ACS. The access requests are sent via TACACs+ or RADIUS.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To view and import network devices:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

The Network Device page appears, with any configured network devices listed. Table 7-3 provides a description of the fields in the Network Device page:

Table 7-3 Network Device Page Field Descriptions

Option	Description
Name	The user-specified name of network devices in ACS. Click a name to edit the associated network device (see Displaying Network Device Properties, page 7-13).
IP / Mask	*Display only.* The IP address or subnet mask of each network device. The first three IP addresses appear in the field, each separated by a comma (,). If this field contains a subnet mask, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition. **Note** When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses.
NDG: <string>	The network device group. The two predefined NDGs are Location and Device Type. If you have defined additional network device groups, they are listed here as well.
Description	*Display only.* Descriptions of the network devices.

Step 2 Do any one of the following:

- Click **Create** to create a new network device. See Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy, page 7-3.
- Check the check box next to the network device that you want to edit and click **Edit**. See Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy, page 7-3.
- Check the check box next to the network device that you want to duplicate and click **Duplicate**. See Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy, page 7-3.
- Click **File Operations** to perform any of the following functions:
  - Add—Choose this option to add a list of network devices from the import file in a single shot.
  - Update—Choose this option to replace the list of network devices in ACS with the network devices in the import file.
  - Delete—Choose this option to delete from ACS the network devices listed in the import file.

  See Performing Bulk Operations for Network Resources and Users, page 7-8 for more information.

For information on how to create the import files, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/cli_imp_exp.html#wp1055255.

Timesaver To perform a bulk add, edit, or delete operation on any of the ACS objects, you can use the export file of that object, retain the header row, and create the .csv import file. However, to add an updated name or MAC address to the ACS objects, must to download and use the particular update template. Also, for the NDGs, the export template contains only the NDG name, so in order to update any other property, you must download and use the NDG update template.

Related Topics:

- Network Devices and AAA Clients, page 7-5
- Performing Bulk Operations for Network Resources and Users, page 7-8
- Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy, page 7-3

Exporting Network Devices and AAA Clients

Note You must turn off the popup blockers in your browser to ensure that the export process completes successfully.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To export a list of network devices:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

The Network Device page appears.

Step 2 Choose the filter condition and the Match if operator, and enter the filter criterion that you are looking for in the text box.

Step 3 Click **Go**.

A list of records that match your filter criterion appears. You can export this list to a .csv file.

Step 4 Click **Export** to export the records to a .csv file.

A system message box appears, prompting you for an encryption password to encrypt the .csv file during file transfer.

Step 5 To encrypt the export .csv file, check the **Password** check box and enter the encryption password. You can optionally choose to not encrypt the file during transfer.

Step 6 Click **Start Export** to begin the export process.

The Export Progress window appears, displaying the progress of the export process. If any errors are encountered during this process, they are displayed in the Export Progress window. You can abort the export process at any time during this process.

Step 7 After the export process is complete, Click **Save File** to save the export file to your local disk.

The export file is a .csv file that is compressed as export.zip.

Performing Bulk Operations for Network Resources and Users

You can use the file operation function to perform bulk operations (add, update, and delete) for the following on your database:

- Internal users
- Internal hosts
- Network devices

For bulk operations, you must download the .csv file template from ACS and add the records that you want to add, update, or delete to the .csv file and save it to your local disk. Use the Download Template function to ensure that your .csv file adheres to the requirements. The .csv templates for users, internal hosts, and network devices are specific to their type; for example, you cannot use a downloaded template accessed from the Users page to add internal hosts or network devices. Within the .csv file, you must adhere to these requirements:

- Do not alter the contents of the first record (the first line, or row, of the .csv file).
- Use only one line for each record.
- Do not imbed new-line characters in any fields.
- For non-English languages, encode the .csv file in utf-8 encoding, or save it with a font that supports Unicode.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Note Before you begin the bulk operation, ensure that your browser's popup blocker is disabled.

Step 1 Click **File Operations** on the Users, Network Devices, or MAC Address page of the web interface.

The Operation dialog box appears.

Step 2 Click **Next** to download the .csv file template if you do not have it.

Step 3 Click any one of the following operations if you have previously created a template-based .csv file on your local disk:

- Add—Adds the records in the .csv file to the records currently available in ACS.
- Update—Overwrites the records in ACS with the records from the .csv file.
- Delete—Removes the records in the .csv file from the list in ACS.

Step 4 Click **Next** to move to the next page.

Step 5 Click **Browse** to navigate to your .csv file.

Step 6 Choose either of the following options that you want ACS to follow in case of an error during the import process:

- Continue processing remaining records; successful records will be imported.
- Stop processing the remaining records; only the records that were successfully imported before the error will be imported.

Step 7 Check the **Password** check box and enter the password to decrypt the .csv file if it is encrypted in GPG format.

Step 8 Click **Finish** to start the bulk operation.

The Import Progress window appears. Use this window to monitor the progress of the bulk operation. Data transfer failures of any records within your .csv file are displayed.

Note You can click the Abort button to stop importing data that is under way; however, the data that was successfully transferred is not removed from your database.

When the operation completes, the Save Log button is enabled.

Step 9 Click **Save Log** to save the log file to your local disk.

Step 10 Click **OK** to close the Import Progress window.

Note You can submit only one .csv file to the system at one time. If an operation is under way, an additional operation cannot succeed until the original operation is complete.

For information on how to create the import files, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/cli_imp_exp.html#wp1055255.

Timesaver To perform a bulk add, edit, or delete operation on any of the ACS objects, you can use the export file of that object, retain the header row, and create the .csv import file. However, to add an updated name or MAC address to the ACS objects, you must download and use the particular update template. Also, for the NDGs, the export template contains only the NDG name, so in order to update any other property, you must download and use the NDG update template.

Exporting Network Resources and Users

Note You must turn off the popup blockers in your browser to ensure that the export process completes successfully.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To export a list of network resources or users:

Step 1 Click **Export** on the Users, Network Devices, or MAC Address page of the web interface.

The Network Device page appears.

Step 2 Choose the filter condition and the Match if operator, and enter the filter criterion that you are looking for in the text box.

Step 3 Click **Go**.

A list of records that match your filter criterion appears. You can export these to a .csv file.

Step 4 Click **Export** to export the records to a .csv file.

A system message box appears, prompting you for an encryption password to encrypt the .csv file during file transfer.

Step 5 To encrypt the export .csv file, check the **Password** check box and enter the encryption password. You can optionally choose to not encrypt the file during transfer.

Step 6 Click **Start Export** to begin the export process.

The Export Progress window appears, displaying the progress of the export process. If any errors are encountered during this process, they are displayed in the Export Progress window. You can abort the export process at any time during this process.

Step 7 After the export process is complete, Click **Save File** to save the export file to your local disk.

The export file is a .csv file that is compressed as export.zip.

Creating, Duplicating, and Editing Network Devices

You can use the bulk import feature to import a large number of network devices in a single operation; see Performing Bulk Operations for Network Resources and Users, page 7-8 for more information. Alternatively, you can use the procedure described in this topic to create network devices.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a network device:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

The Network Devices page appears, with a list of your configured network devices, if any.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the network device name that you want to duplicate, then click **Duplicate**.
- Click the network device name that you want to modify, or check the check box next to the name and click **Edit**.

The first page of the Create Network Device process appears if you are creating a new network device. The Network Device Properties page for the selected device appears if you are duplicating or editing a network device.

Step 3 Modify the fields as required. For field descriptions, see Configuring Network Device and AAA Clients, page 7-11.

Step 4 Click **Submit**.

Your new network device configuration is saved. The Network Devices page appears, with your new network device configuration listed.

Related Topics

- Viewing and Performing Bulk Operations for Network Devices, page 7-5
- Configuring Network Device and AAA Clients, page 7-11

Configuring Network Device and AAA Clients

To display this page, choose **Network Resources > Network Devices and AAA Clients**, then click **Create**.

Table 7-4 Creating Network Devices and AAA Clients

Option	Description
General	
Name	The name of the network device. If you are duplicating a network device, you must enter a unique name as a minimum configuration; all other fields are optional.
Description	The description of the network device.
Network Device Groups[1]	
Location	Click **Select** to display the Network Device Groups selection box. Click the radio button next to the Location network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type	Click **Select** to display the Network Device Groups selection box. Click the radio button next to the Device Type network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
IP Address	
IP	The IP addresses and subnet masks associated with the network device. Select to enter a single IP address or to define a range.

Table 7-4 Creating Network Devices and AAA Clients (continued)

Option	Description
IP / Mask	For a single IP address, enter the address in the IP field, and click **Single IP Address**. For an IP address range, click **IP Range(s)**. You can configure up to 40 IP addresses or subnet masks for each network device. If you use a subnet mask in this field, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition. **Note** When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses. The first six IP addresses appear in the field; use the scroll bar to see any additional configured IP addresses. **Note** A mask is needed only for wildcards—if you want an IP address range. You cannot use an asterisk (*) as a wildcard.
Authentication Options	
TACACS+	Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device. You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall.
TACACS+ Shared Secret	The shared secret of the network device, if you enabled the TACACS+ protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Single Connect Device	Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one: • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support If you disable this option, a new TCP connection is used for every TACACS+ request.
RADIUS	Check to use the RADIUS protocol to authenticate communication to and from the network device.
RADIUS Shared Secret	The shared secret of the network device, if you have enabled the RADIUS protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
TrustSec	Appears only when you enable the Cisco TrustSec feature. Check to use TrustSec functionality on the network device. If the network device is the seed device (first device in the TrustSec network), you must also check the RADIUS check box.
Use Device ID for TrustSec Identification	Check this check box to use the device ID for TrustSec Identification. When you check this check box, the following field, Device ID, is disabled.
Device ID	The name that will be used for TrustSec identification of this device. By default, you can use the configured device name. If you want to use another name, clear the Use device name for TrustSec identification check box, and enter the name in the Identification field.

Table 7-4 Creating Network Devices and AAA Clients (continued)

Option	Description
Password	The TrustSec authentication password.
TrustSec Advanced Settings	Check to display additional TrustSec fields.
Other TrustSec devices to trust this device (CTS trusted)	Specifies whether all the device's peer devices trust this device. The default is checked, which means that the peer devices trust this device, and do not change the SGTs on packets arriving from this device. If you uncheck the check box, the peer devices repaint packets from this device with the related peer SGT.
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for the peer authorization policy. ACS returns this information to the device in the response to a peer policy request. The default is 1 day.
Download SGACL lists every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for SGACL lists. ACS returns this information to the device in the response to a request for SGACL lists. The default is 1 day.
Download environment data every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for environment data. ACS returns this information to the device in the response to a request for environment data. The default is 1 day.
Re-authentication every: Weeks Days Hours Minutes Seconds	Specifies the dot1x (.1x) reauthentication period. ACS configures this for the supplicant and returns this information to the authenticator. The default is 1 day.

1. The Device Type and Location network device groups are predefined at installation. You can define an additional 10 network device groups. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information on how to define network device groups. If you have defined additional network device groups, they appear in alphabetical order in the Network Device Groups page and in the Network Resources drawer in the left navigation pane.

Displaying Network Device Properties

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Choose **Network Resources > Network Devices and AAA Clients**, then click a device name or check the check box next to a device name, and click **Edit** or **Duplicate**.

The Network Devices and AAA Clients Properties page appears, displaying the information described in Table 7-5:

Table 7-5 Network Devices and AAA Clients Properties Page

Option	Description
Name	The name of the network device. If you are duplicating a network device, you must enter a unique name as a minimum configuration; all other fields are optional.
Description	The description of the network device.
Network Device Groups[1]	
Location: Select	Click **Select** to display the Network Device Groups selection box. Click the radio button next to the network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type: Select	Click **Select** to display the Network Device Groups selection box. Click the radio button next to the device type network device group that you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
IP Address	
IP Address	The IP addresses and subnet masks associated with the network device. Select to enter a single IP address or to define a range.
IP / Mask	For a single IP address, enter the address in the IP field, and click **Single IP Address**. For an IP address range, click **IP Range(s)**. You can configure up to 40 IP addresses or subnet masks for each network device. If you use a subnet mask in this field, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition. **Note** When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses. The first six IP addresses appear in the field; use the scroll bar to see any additional configured IP addresses.
Authentication Options	
TACACS+	Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device. You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall.
TACACS+ Shared Secret	The shared secret of the network device, if you enabled the TACACS+ protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Single Connect Device	Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one: • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support If you disable this option, a new TCP connection is used for every TACACS+ request.

Table 7-5 Network Devices and AAA Clients Properties Page (continued)

Option	Description
RADIUS	Check to use the RADIUS protocol to authenticate communication to and from the network device.
RADIUS Shared Secret	The shared secret of the network device, if you have enabled the RADIUS protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
TrustSec	Appears only when you enable the Cisco TrustSec feature. Check to use TrustSec functionality on the network device. If the network device is the seed device (first device in the TrustSec network), you must also check the RADIUS check box.
Identification	The name that will be used for TrustSec identification of this device. By default, you can use the configured device name. If you want to use another name, clear the Use device name for TrustSec identification check box, and enter the name in the Identification field.
Password	The TrustSec authentication password.
TrustSec Advanced Settings	Check to display additional TrustSec fields.
Other TrustSec devices to trust this device	Specifies whether all the device's peer devices trust this device. The default is checked, which means that the peer devices trust this device, and do not change the SGTs on packets arriving from this device. If you uncheck the check box, the peer devices repaint packets from this device with the related peer SGT.
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for the peer authorization policy. ACS returns this information to the device in the response to a peer policy request. The default is 1 day.
Download SGACL lists every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for SGACL lists. ACS returns this information to the device in the response to a request for SGACL lists. The default is 1 day.
Download environment data every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for environment data. ACS returns this information to the device in the response to a request for environment data. The default is 1 day.
Re-authentication every: Weeks Days Hours Minutes Seconds	Specifies the dot1x (.1x) reauthentication period. ACS configures this for the supplicant and returns this information to the authenticator. The default is 1 day.

1. The Device Type and Location network device groups are predefined at installation. You can define an additional 10 network device groups. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information on how to define network device groups. If you have defined additional network device groups, they appear in the Network Device Groups page and in the Network Resources drawer in the left navigation pane, in alphabetical order.

Related Topics:

- Viewing and Performing Bulk Operations for Network Devices, page 7-5
- Creating, Duplicating, and Editing Network Device Groups, page 7-2

Deleting Network Devices

To delete a network device:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

The Network Devices page appears, with a list of your configured network devices.

Step 2 Check one or more check boxes next to the network devices you want to delete.

Step 3 Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 4 Click **OK**.

The Network Devices page appears, without the deleted network devices listed. The network device is removed from the device repository.

Configuring a Default Network Device

While processing requests, ACS searches the network device repository for a network device whose IP address matches the IP address presented in the request. If the search does not yield a match, ACS uses the default network device definition for RADIUS or TACACS+ requests.

The default network device defines the shared secret to be used and also provides NDG definitions for RADIUS or TACACS+ requests that use the default network device definition.

Choose **Network Resources > Default Network Device** to configure the default network device. The Default Network Device page appears, displaying the information described in Table 7-6.

Table 7-6 Default Network Device Page

Option	Description
Default Network Device	
The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address.	
Default Network Device Status	Choose Enabled from the drop-down list box to move the default network device to the active state.
Network Device Groups	
Location	Click **Select** to display the Network Device Groups selection box. Click the radio button next to the Location network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type	Click **Select** to display the Network Device Groups selection box. Click the radio button next to the Device Type network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Authentication Options	

Table 7-6 Default Network Device Page (continued)

Option	Description
TACACS+	Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device. You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall.
Shared Secret	The shared secret of the network device, if you enabled the TACACS+ protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Single Connect Device	Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one: • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support If you disable this option, ACS uses a new TCP connection for every TACACS+ request.
RADIUS	Check to use the RADIUS protocol to authenticate communication to and from the network device.
Shared Secret	The shared secret of the network device, if you have enabled the RADIUS protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.

Related Topics

- Network Device Groups, page 7-1
- Network Devices and AAA Clients, page 7-5
- Creating, Duplicating, and Editing Network Device Groups, page 7-2

Working with External RADIUS Servers

ACS 5.1 can function both as a RADIUS server and as a RADIUS proxy server. When it acts as a proxy server, ACS receives authentication and accounting requests from the NAS and forwards them to the external RADIUS server. ACS accepts the results of the requests and returns them to the NAS. You must configure the external RADIUS servers in ACS to enable ACS to forward requests to them. You can define the timeout period and the number of connection attempts.

ACS can simultaneously act as a proxy server to multiple external RADIUS servers.

Note You can use the external RADIUS servers that you configure here in access services of the RADIUS proxy service type.

This section contains the following topics:

- Creating, Duplicating, and Editing External RADIUS Servers, page 7-18
- Deleting External RADIUS Servers, page 7-19

Creating, Duplicating, and Editing External RADIUS Servers

To create, duplicate, or edit an external RADIUS server:

Step 1 Choose **Network Resources > External RADIUS Servers**.

The External RADIUS Servers page appears with a list of configured servers.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the external RADIUS server that you want to duplicate, then click **Duplicate**.
- Click the external RADIUS server name that you want to edit, or check the check box next to the name and click **Edit**.

The External RADIUS Servers page appears.

Step 3 Edit fields in the External Policy Servers page as shown in Table 7-7.

Table 7-7 External Policy Servers Page

Option	Description
General	
Name	Name of the external RADIUS server.
Description	(Optional) The description of the external RADIUS server.
Server Connection	
Server IP Address	IP address of the external RADIUS server.
Shared Secret	Shared secret between ACS 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.
Advanced Options	
Authentication Port	RADIUS authentication port number. The default is 1812.
Accounting Port	RADIUS accounting port number. The default is 1813.
Server Timeout	Number of seconds ACS waits for a response from the external RADIUS server. The default is 5 seconds. Valid values are from 1 to 120.
Connection Attempts	Number of times ACS attempts to connect to the external RADIUS server. The default is 3 attempts. Valid values are from 1 to 10.

Step 4 Click **Submit** to save the changes.

The external RADIUS server configuration is saved. The External RADIUS Server page appears with the new configuration.

Related Topics

- RADIUS Proxy Services, page 3-7
- RADIUS Proxy Requests, page 4-27
- Configuring General Access Service Properties, page 10-14
- Deleting External RADIUS Servers, page 7-19

Deleting External RADIUS Servers

To delete an external RADIUS server:

Step 1 Choose **Network Resources > External RADIUS Servers**.

The External RADIUS Servers page appears with a list of configured servers.

Step 2 Check one or more check boxes next to the external RADIUS servers you want to delete, and click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Step 3 Click **OK.**

The External RADIUS Servers page appears without the deleted server(s).

CHAPTER 8

Managing Users and Identity Stores

Overview

ACS manages your network devices and other ACS clients by using the ACS network resource repositories and identity stores. When a host connects to the network through ACS requesting access to a particular network resource, ACS authenticates the host and decides whether the host can communicate with the network resource.

To authenticate and authorize a user or host, ACS uses the user definitions in identity stores. There are two types of identity stores:

- Internal—Identity stores that ACS maintains locally (also called local stores) are called *internal identity stores*. For internal identity stores, ACS provides interfaces for you to configure and maintain user records.
- External—Identity stores that reside outside of ACS are called *external identity stores*. ACS requires configuration information to connect to these external identity stores to perform authentication and obtain user information.

In addition to authenticating users and hosts, identity stores return attributes that are associated with the users and hosts. You can use these attributes in policy conditions while processing a request and can also populate the values returned for RADIUS attributes in authorization profiles.

Internal Identity Stores

ACS maintains different internal identity stores to maintain user and host records. For each identity store, you can define identity attributes associated with that particular store for which values are defined while creating the user or host records. You can define these identity attributes as part of identity dictionaries under the System Administration section of the ACS application (**System Administration > Configuration > Dictionaries > Identity**).

Each internal user record includes a password, and you can define a second password as a TACACS+ enable password. You can configure the password stored within the internal user identity store to expire after a particular time period and thus force users to change their own passwords periodically. Users can change their passwords over the RADIUS or TACACS+ protocols or use the UCP web service. Passwords must conform to the password complexity criteria that you define in ACS.

Internal user records consist of two component types: fixed and configurable.

Fixed components are:

- Name
- Description

- Password
- Enabled or disabled status
- Identity group to which users belong

Configurable components are:

- Enable password for TACACS+ authentication
- Sets of identity attributes that determine how the user definition is displayed and entered

Cisco recommends that you configure identity attributes before you create users. When identity attributes are configured:

- You can enter the corresponding values as part of a user definition.
- They are available for use in policy decisions when the user authenticates.
- They can be used to populate the values returned for RADIUS attributes in an authorization profile.

Internal user identity attributes are applied to the user for the duration of the user's session.

Internal identity stores contain the internal user attributes and credential information used to authenticate internal users.

Internal host records are similar to internal user records, except that they do not contain any password information. Hosts are identified by their MAC addresses. For information on managing internal identity stores, see Managing Internal Identity Stores, page 8-4.

External Identity Stores

External identity stores are external databases on which ACS performs authentications for internal and external users. ACS 5.1 supports the following external identity stores:

- LDAP
- Active Directory
- RSA SecurID Token Server
- RADIUS Identity Server

External identity store user records include configuration parameters that are required to access the specific store. You can define attributes for user records in all the external identity stores except the RSA SecurID Token Server. External identity stores also include certificate information for the ACS server certificate and certificate authentication profiles. The RSA SecurID Token Server and RADIUS Identity Server provide increased security in the form of two-factor authentication. For more information on how to manage external identity stores, see Managing External Identity Stores, page 8-18.

Identity Stores with Two-Factor Authentication

You can use the RSA SecurID Token Server and RADIUS Identity Server to provide two-factor authentication. These external identity stores use an OTP that provides greater security. The following additional configuration options are available for these external identity stores:

- Identity caching—You can enable identity caching for ACS to use the identity store while processing a request in cases where authentication is not performed. In LDAP and AD, you can perform a user lookup without user authentication. For example, if you must authorize a TACACS+ request separately from the authentication request, it is not possible for the identity store to retrieve

the data because authentication is not performed. You can, however, enable identity caching to cache results and attributes retrieved from the last successful authentication for the user. You can use this cache to authorize the request.

- Treat authentication rejects as—The RSA and RADIUS identity stores do not differentiate between the following results when an authentication attempt is rejected:
  - Authentication Failed
  - User Not Found

  This classification is very important when you determine the fail-open operation. A configuration option is available, allowing you to define which result must be used.

Identity Groups

Identity groups are logical entities that are defined within a hierarchy and are associated with users and hosts. These identity groups are used to make policy decisions. For internal users and hosts, the identity group is defined as part of the user or host definition. When external identity stores are used, the group mapping policy is used to map attributes and groups retrieved from the external identity store to an ACS identity group.

Certificate-Based Authentication

Users and hosts can identify themselves with a certificate-based access request. To process this request, you must define a certificate authentication profile in the identity policy. The certificate authentication profile includes the attribute from the certificate that is used to identify the user or host and can also optionally include an LDAP or AD identity store that can be used to validate the certificate present in the request. For more information on certificates and certificate-based authentication, see:

- Configuring CA Certificates, page 8-61
- Configuring Certificate Authentication Profiles, page 8-66

Identity Sequences

You can configure a complex condition where multiple identity stores and profiles are used to process a request. You can define these identity methods in an Identity Sequence object. The identity methods within a sequence can be of any type. The identity sequence is made up of two components, one for authentication and the other for retrieving attributes. If you choose to perform authentication based on a certificate, a single certificate authentication profile is used. If you choose to perform authentication on an identity database, you can define a list of identity databases to be accessed in sequence until the authentication succeeds. If the authentication succeeds, the attributes within the database are retrieved.

In addition, you can configure an optional list of databases from which additional attributes can be retrieved. These additional databases can be configured irrespective of whether you use password-based or certificate-based authentication. If a certificate-based authentication is performed, the username is populated from a certificate attribute and this username is used to retrieve attributes from all the databases in the list. When a matching record is found for the user, the corresponding attributes are retrieved. ACS retrieves attributes even for users whose accounts are disabled or whose passwords are marked for change.

Note An internal user account that is disabled is available as a source for attributes, but not for authentication.

For more information on identity sequences, see Configuring Identity Store Sequences, page 8-67.

This chapter contains the following sections:

- Managing Internal Identity Stores, page 8-4
- Managing External Identity Stores, page 8-18
- Configuring CA Certificates, page 8-61
- Configuring Certificate Authentication Profiles, page 8-66
- Configuring Identity Store Sequences, page 8-67

Managing Internal Identity Stores

ACS contains an identity store for users and an identity store for hosts:

- The internal identity store for *users* is a repository of users, user attributes, and user authentication options.
- The internal identity store for *hosts* contains information about hosts for MAC Authentication Bypass (Host Lookup).

You can define each user and host in the identity stores, and you can import files of users and hosts.

The identity store for users is shared across all ACS instances in a deployment and includes for each user:

- Standard attributes
- User attributes
- Authentication information

Note ACS 5.1 supports authentication for internal users against the internal identity store only.

This section contains the following topics:

- Authentication Information, page 8-5
- Identity Groups, page 8-5
- Managing Identity Attributes, page 8-7
- Configuring Authentication Settings for Users, page 8-9
- Creating Internal Users, page 8-11
- Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-14
- Creating Hosts in Identity Stores, page 8-15
- Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17

Authentication Information

You can configure an additional password, stored as part of the internal user record that defines the user's TACACS+ enable password. If you do not select this option, the standard user password is also used for TACACS+ enable.

If the system is not being used for TACACS+ enable operations, you should not select this option.

To use the identity store sequence feature, you define the list of identity stores to be accessed in a sequence. You can include the same identity store in authentication and attribute retrieval sequence lists; however, if an identity store is used for authentication, it is not accessed for additional attribute retrieval.

For certificate-based authentication, the username is populated from the certificate attribute and is used for attribute retrieval. During the authentication process, authentication fails if more than one instance of a user or host exists in internal identity stores. Attributes are retrieved (but authentication is denied) for users who have disabled accounts or passwords that must be changed.

These types of failures can occur while processing the identity policy:

- Authentication failure; possible causes include bad credentials, disabled user, and so on.
- User or host does not exist in any of the authentication databases.
- Failure occurred while accessing the defined databases.

You can define fail-open options to determine what actions to take when each of these failures occurs:

- Reject—Send a reject reply.
- Drop—Do not send a reply.
- Continue—Continue processing to the next defined policy in the service.

The system attribute, *AuthenticationStatus*, retains the result of the identity policy processing. If you choose to continue policy processing when a failure occurs, you can use this attribute in a condition in subsequent policy processing to distinguish cases where identity policy processing did not succeed.

You can continue processing when authentication fails for PAP/ASCII, EAP-TLS, or EAP-MD5. For all other authentication protocols, the request is rejected and a message to this effect is logged.

Identity Groups

You can assign each internal user to one identity group. Identity groups are defined within a hierarchical structure. They are logical entities that are associated with users, but do not contain data or attributes other than the name you give to them. You use identity groups within policy conditions to create logical groups of users to which the same policy results are applied. You can associate each user in the internal identity store with a single identity group. When ACS processes a request for a user, the identity group for the user is retrieved and can then be used in conditions in the rule table. Identity groups are hierarchical in structure.

You can map identity groups and users in external identity stores to ACS identity groups by using a group mapping policy.

Creating Identity Groups

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create an identity group:

Step 1 Select **Users and Identity Stores > Identity Groups**.

The Identity Groups page appears.

Step 2 Click **Create**. You can also:

- Check the check box next to the identity group that you want to duplicate, then click **Duplicate**.
- Click the identity group name that you want to modify, or check the check box next to the name and click **Edit**.
- Click **File Operations** to:
  - Add—Adds identity groups from the import to ACS.
  - Update—Overwrites the existing identity groups in ACS with the list from the import.
  - Delete—Removes the identity groups listed in the import from ACS.
- Click **Export** to export a list of identity groups to your local hard disk.

  For more information on the File Operations option, see Performing Bulk Operations for Network Resources and Users, page 7-8.

The Create page or the Edit page appears when you choose the Create, Duplicate, or Edit option.

Step 3 Enter information in the following fields:

- Name—Enter a name for the identity group. If you are duplicating an identity group, you must enter a unique name; all other fields are optional.
- Description—Enter a description for the identity group.
- Parent—Click **Select** to select a network device group parent for the identity group.

Step 4 Click **Submit** to save changes.

The identity group configuration is saved. The Identity Groups page appears with the new configuration. If you created a new identity group, it is located within the hierarchy of the page beneath your parent identity group selection.

Related Topics

- Managing Users and Identity Stores, page 8-1
- Managing Internal Identity Stores, page 8-4
- Performing Bulk Operations for Network Resources and Users, page 7-8
- Identity Groups, page 8-3
- Creating Identity Groups, page 8-6
- Deleting an Identity Group, page 8-7

Deleting an Identity Group

To delete an identity group:

Step 1 Select **Users and Identity Stores > Identity Groups**.

The Identity Groups page appears.

Step 2 Check one or more check boxes next to the identity groups you want to delete and click **Delete**.

The following error message appears:

Are you sure you want to delete the selected item/items?

Step 3 Click **OK**.

The Identity Groups page appears without the deleted identity groups.

Related Topic

- Managing Identity Attributes, page 8-7

Managing Identity Attributes

Administrators can define sets of identity attributes that become elements in policy conditions. For information about the ACS 5.1 policy model, see Chapter 3, "ACS 5.x Policy Model." During authentication, identity attributes are taken from the internal data store when they are part of a policy condition.

ACS 5.1 interacts with identity elements to authenticate users and obtain attributes for input to an ACS policy.

Attribute definitions include the associated data type and valid values. The set of values depends on the type. For example, if the type is *integer*, the definition includes the valid range. ACS 5.1 provides a default value definition that can be used in the absence of an attribute value. The default value ensures that all attributes have at least one value.

Related Topics

- Standard Attributes, page 8-8
- User Attributes, page 8-8
- Host Attributes, page 8-9

Standard Attributes

Table 8-1 describes the standard attributes in the internal user record.

Table 8-1 Standard Attributes

Attribute	Description
Username	ACS compares the username against the username in the authentication request. The comparison is case-insensitive.
Status	The enabled status indicates that the account is active. The disabled status means that authentications for the username will fail.
Description	A text description of the attribute.
Identity Group	ACS associates each user to an identity group. See Managing Identity Attributes, page 8-7 for information.

User Attributes

Administrators can create and add user-defined attributes from the set of identity attributes. You can then assign default values for these attributes for each user in the internal identity store and define whether the default values are required or optional.

You need to define users in ACS, which includes associating each internal user with an identity group, a description (optional), a password, an enable password (optional), and internal and external user attributes.

Internal users are defined by two components: fixed and configurable. Fixed components consist of these attributes:

- Name
- Description
- Password
- Enabled or disabled status
- Identity group to which they belong

Configurable components consist of these attributes:

- Enable password for TACACS+ authentication
- Sets of identity attributes that determine how the user definition is displayed and entered

Cisco recommends that you configure identity attributes before you create users. When identity attributes are configured:

- You can enter the corresponding values as part of a user definition.
- They are available for use in policy decisions when the user authenticates.

Internal user identity attributes are applied to the user for the duration of the user's session.

Internal identity stores contain the internal user attributes and credential information used to authenticate internal users (as defined by you within a policy).

External identity stores are external databases on which to perform credential and authentication validations for internal and external users (as defined by you within a policy).

In ACS 5.1, you can configure identity attributes that are used within your policies, in this order:

1. Define an identity attribute (using the user dictionary).
2. Define custom conditions to be used in a policy.
3. Populate values for each user in the internal database.
4. Define rules based on this condition.

As you become more familiar with ACS 5.1 and your identity attributes for users, the policies themselves will become more robust and complex.

You can use the user-defined attribute values to manage policies and authorization profiles. See Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-10 for information on how to create a user attribute.

Host Attributes

You can configure additional attributes for internal hosts. You can do the following when you create an internal host:

- Create host attributes
- Assign default values to the host attributes
- Define whether the default values are required or optional

You can enter values for these host attributes and can use these values to manage policies and authorization profiles. See Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-13 for information on how to create a host attribute.

Configuring Authentication Settings for Users

You can configure the authentication settings for user accounts in ACS to force users to use strong passwords. Any password policy changes that you make in the Authentication Settings page apply to all internal identity store user accounts. The User Authentication Settings page consists of the following tabs:

- Password complexity
- Advanced

To configure a password policy:

Step 1 Choose **System Administration > Users > Authentication Settings**.

The User Authentication Settings page appears with the Password Complexity and Advanced tabs.

Step 2 In the **Password Complexity** tab, check each check box that you want to use to configure your user password. Table 8-2 describes the fields in the Password Complexity tab.

Table 8-2 Password Complexity Tab

Option	Description
Applies to all ACS internal identity store user accounts	
Minimum length	The required minimum length; the valid options are 4 to 20.
Password may not contain the username	Whether the password may contain the username or reverse username.

Table 8-2 Password Complexity Tab (continued)

Option	Description
Password may not contain 'cisco'	Check to specify that the password cannot contain the word *cisco*.
Password may not contain	Check to specify that the password does not contain the string that you enter.
Password may not contain repeated characters four or more times consecutively	Check to specify that the password cannot repeat characters four or more times consecutively.
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	Password must contain at least one lowercase alphabetic character.
Upper case alphabetic characters	Password must contain at least one uppercase alphabetic character.
Numeric characters	Password must contain at least one numeric character.
Non alphanumeric characters	Password must contain at least one nonalphanumeric character.

Step 3 In the **Advanced** tab, enter the values for the criteria that you want to configure for your user authentication process. Table 8-3 describes the fields in the Advanced tab.

Table 8-3 Advanced Tab

Options	Description
Password History	
Password must be different from the previous *n* versions.	Specifies the number of previous passwords for this user to be compared against. The number of previous passwords include the default password as well. This option prevents the users from setting a password that was recently used. Valid options are 1 to 99.
Password Lifetime	
Users can be required to periodically change password	
Disable user account after *n* days if password is not changed	Specifies that the user account must be disabled after *n* days if the password is not changed; the valid options are 1 to 365.
Display reminder after *n* days	Displays a reminder after *n* days to change password; the valid options are 1 to 365. This option, when set, only displays a reminder. It does not prompt you for a new password.
TACACS Enable Password	
Select whether a separate password should be defined in the user record to store the Enable Password	
TACACS Enable Password	Check the check box to enable a separate password for TACACS authentication.

Step 4 Click **Submit**.

The user password is configured with the defined criteria. These criteria will apply only for future logins.

Creating Internal Users

In ACS, you can create internal users that do not access external identity stores for security reasons.

You can use the bulk import feature to import hundreds of internal users at a time; see Performing Bulk Operations for Network Resources and Users, page 7-8 for more information. Alternatively, you can use the procedure described in this topic to create internal users one at a time.

Step 1 Select **Users and Identity Stores > Internal Identity Store > Users**.

The Internal Users page appears.

Step 2 Click **Create**. You can also:

- Check the check box next to the user that you want to duplicate, then click **Duplicate**.
- Click the username that you want to modify, or check the check box next to the name and click **Edit**.
- Check the check box next to the user whose password you want to change, then click **Change Password**.

  The Change Password page appears. Complete the fields as described in Table 8-4 to change the internal user password.

Table 8-4 Internal User - Change Password Page

Option	Description
Password Information	
Password	The user's current password, which must comply with the password policies defined under **System Administration > Users > Authentication Settings**.
Confirm Password	The user's password, which must match the Password entry exactly.
Enable Password Information	
Enable Password	(Optional) The internal user's TACACS+ enable password, from 4 to 32 characters. You can disable this option. See Authentication Information, page 8-5 for more information.
Confirm Password	(Optional) The internal user's TACACS+ enable password, which must match the Enable Password entry exactly.
Change Password on Next Login	Check this box to start the process to change the user's password at the next user login, after authentication with the old password.

- Click **File Operations** to:
  - Add—Adds internal users from the import to ACS.
  - Update—Overwrites the existing internal users in ACS with the list of users from the import.
  - Delete—Removes the internal users listed in the import from ACS.
- Click **Export** to export a list of internal users to your local hard disk.

For more information on the File Operations option, see Performing Bulk Operations for Network Resources and Users, page 7-8.

The User Properties page appears when you choose the Create, Duplicate, or Edit option. In the Edit view, you can see the information on the original creation and last modification of the user. You cannot edit this information.

Step 3 Complete the fields as described in Table 8-5.

Table 8-5 Users and Identity Stores > Internal Identity Store > User Properties Page

Option	Description
General	
Name	The username of the user.
Status	Use the drop-down list box to select the status for the user: • Enabled—Authentication requests for this user are allowed. • Disabled—Authentication requests for this user fail.
Description	(Optional) The description of the user.
Identity Group	Click **Select** to display the Identity Groups window. Choose an identity group and click **OK** to configure the user with a specific identity group.
Password Information	
Note This section of the page appears only when you create an internal user. Password must contain at least 4 characters	
Password	The user's password, which must comply with the password policies defined under **System Administration > Users > Authentication Settings**.
Confirm Password	The user's password, which must match the Password entry exactly.
Change Password on next login	Check this box to start the process to change the user's password at the next user login, after authentication with the old password.
Enable Password Information	
Note This section of the page appears only when you create an internal user. Password must contain 4-32 characters	
Enable Password	(Optional) The internal user's TACACS+ enable password, from 4 to 32 characters. You can disable this option. See Authentication Information, page 8-5 for more information.
Confirm Password	(Optional) The internal user's TACACS+ enable password, which must match the Enable Password entry exactly.
User Information	
If defined, this section displays additional identity attributes defined for user records.	
Creation/Modification Information	
Note This section of the page appears only after you have created or modified an internal user.	

Table 8-5 Users and Identity Stores > Internal Identity Store > User Properties Page (continued)

Option	Description
Date Created	*Display only.* The date and time when the user's account was created, in the format *Day Mon dd hh:mm:ss* **UTC** *YYYY*, where: • *Day* = Day of the week. • *Mon* = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • *DD* = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • *hh*:*mm*:*ss* = Hour, minute, and second, respectively • *YYYY* = Four digits that represent the year
Date Modified	*Display only.* The date and time when the user's account was last modified (updated), in the format *Day Mon dd hh:mm:ss* **UTC** *YYYY*, where: • *Day* = Day of the week. • *Mon* = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • *DD* = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • *hh*:*mm*:*ss* = Hour, minute, and second, respectively • *YYYY* = Four digits that represent the year

Step 4 Click **Submit**.

The user configuration is saved. The Internal Users page appears with the new configuration.

Related Topics

- Configuring Authentication Settings for Users, page 8-9
- Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-14
- Deleting Users from Internal Identity Stores, page 8-13

Deleting Users from Internal Identity Stores

To delete a user from an internal identity store:

Step 1 Select **Users and Identity Stores > Internal Identity Store > Users**.

The Internal Users page appears.

Step 2 Check one or more check boxes next to the users you want to delete.

Step 3 Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Click **OK**.

The Internal Users page appears without the deleted users.

Related Topics

- Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-14
- Creating Internal Users, page 8-11

Viewing and Performing Bulk Operations for Internal Identity Store Users

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To view and perform bulk operations to internal identity store users:

Step 1 Select **Users and Identity Stores > Internal Identity Stores > Users**.

The Internal Users page appears, with the following information for all configured users:

- Status—The status of the user
- User Name—The username of the user
- Identity Group—The identity group to which the user belongs
- Description—(Optional) A description of the user.

Step 2 Do one of the following:

- Click **Create**. For more information on creating internal users, see Creating Internal Users, page 8-11.
- Check the check box next to an internal user whose information you want to edit and click **Edit**. For more information on the various fields in the edit internal user page, see Creating Internal Users, page 8-11.
- Check the check box next to an internal user whose information you want to duplicate and click **Duplicate**. For more information on the various fields in the duplicate internal user page, see Creating Internal Users, page 8-11.
- Click **File Operations** to perform any of the following bulk operations:
  - Add—Choose this option to add internal users from the import file to ACS.
  - Update—Choose this option to replace the list of internal users in ACS with the list of internal users in the import file.
  - Delete—Choose this option to delete the internal users listed in the import file from ACS.

  See Performing Bulk Operations for Network Resources and Users, page 7-8 for a detailed description of the bulk operations.

Related Topics

- Creating Internal Users, page 8-11
- Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-14
- Deleting Users from Internal Identity Stores, page 8-13

Creating Hosts in Identity Stores

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a MAC address and assign identity groups to internal hosts:

Step 1 Select **Users and Identity Stores > Internal Identity Stores > Hosts**.

The Internal Hosts page appears listing any configured internal hosts.

Step 2 Click **Create**. You can also:

- Check the check box next to the MAC address you want to duplicate, then click **Duplicate**.
- Click the MAC address that you want to modify, or check the check box next to the MAC address and click **Edit**.
- Click **File Operations** to perform bulk operations. See Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17 for more information on the import process.
- Click **Export** to export a list of hosts to your local hard drive.

The Internal Hosts General page appears when you click the Create, Duplicate, or Edit options.

Step 3 Complete the fields in the Internal MAC Address Properties page as described in Table 8-6:

Table 8-6 Internal Hosts Properties Page

Option	Description
General	
MAC Address	Enter a valid MAC address, using any of the following formats: • 01-23-45-67-89-AB • 01:23:45:67:89:AB • 0123.4567.89AB • 0123456789AB ACS accepts a MAC address in any of the above formats, and converts and stores the MAC address as six hexadecimal digits separated by hyphens; for example, 01-23-45-67-89-AB.
Status	Use the drop-down list box to enable or disable the MAC address.
Description	(Optional) Enter a description of the MAC address.

Table 8-6 Internal Hosts Properties Page (continued)

Option	Description
Identity Group	Enter an identity group with which to associate the MAC address, or click **Select** to display the Identity Groups window. Choose an identity group with which to associate the MAC address, then click **OK**.
MAC Host Information	*Display only.* Contains MAC host identity attribute information.
Creation/Modification Information	
Note This section of the page appears only after you have created or modified a MAC address.	
Date Created	*Display only.* The date that the host account was created, in the format *Day Mon dd hh:mm:ss* **UTC** *YYYY*, where: • *Day* = Day of the week. • *Mon* = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • *DD* = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • *hh***:***mm***:***ss* = Hour, minute, and second, respectively • *YYYY* = Four digits that represent the year
Date Modified	*Display only.* The date that the host account was last modified (updated), in the format *Day Mon dd hh:mm:ss* **UTC** *YYYY*, where: • *Day* = Day of the week. • *Mon* = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • *DD* = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • *hh***:***mm***:***ss* = Hour, minute, and second, respectively • *YYYY* = Four digits that represent the year

Step 4 Click **Submit** to save changes.

The MAC address configuration is saved. The Internal MAC list page appears with the new configuration.

Related Topics

- Host Lookup, page 4-12
- Deleting Internal Hosts, page 8-17
- Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17
- Policies and Identity Attributes, page 3-16
- Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17

Deleting Internal Hosts

To delete a MAC address:

Step 1 Select **Users and Identity Stores > Internal Identity Stores > Hosts**.

The Internal MAC List page appears, with any configured MAC addresses listed.

Step 2 Check one or more of the check boxes next to the internal hosts you want to delete.

Step 3 Click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item/items?
```

Click **OK**.

The Internal MAC List page appears without the deleted MAC address(es).

Related Topics

- Host Lookup, page 4-12
- Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-17
- Creating Hosts in Identity Stores, page 8-15
- Policies and Identity Attributes, page 3-16
- Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17

Viewing and Performing Bulk Operations for Internal Identity Store Hosts

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To view and perform bulk operations for internal identity stores:

Step 1 Select **Users and Identity Stores > Internal Identity Stores > Hosts**.

The Internal Hosts page appears, with any configured internal hosts listed.

Step 2 Click **File Operations** to perform any of the following functions:

- Add—Choose this option to add internal hosts from an import file to ACS.
- Update—Choose this option to replace the list of internal hosts in ACS with the internal hosts in the import file.
- Delete—Choose this option to delete the internal hosts listed in the import file from ACS.

See Performing Bulk Operations for Network Resources and Users, page 7-8 for a detailed description of the bulk operations.

Related Topics

- Host Lookup, page 4-12
- Creating Hosts in Identity Stores, page 8-15
- Deleting Internal Hosts, page 8-17
- Policies and Identity Attributes, page 3-16
- Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17

Managing External Identity Stores

ACS 5.1 integrates with external identity systems in a number of ways. You can leverage an external authentication service or use an external system to obtain the necessary attributes to authenticate a principal, as well to integrate the attributes into an ACS policy. For example, ACS can leverage Microsoft AD to authenticate a principal, or it could leverage an LDAP bind operation to find a principal in the database and authenticate it. ACS can obtain identity attributes such as AD group affiliation to make an ACS policy decision.

Note ACS 5.1 does not have a built-in check for the dial-in permission attribute for Windows users. You must set the msNPAllowDialin attribute through LDAP or Windows AD. Please refer to Microsoft documentation for information on how to set this attribute.

This section provides an overview of the external identity stores that ACS 5.1 supports and then describes how you can configure them.

This section contains the following topics:

- LDAP Overview, page 8-18
- Leveraging Cisco NAC Profiler as an External MAB Database, page 8-31
- Microsoft AD, page 8-38
- RSA SecurID Server, page 8-47
- RADIUS Identity Stores, page 8-53

LDAP Overview

Lightweight Directory Access Protocol (LDAP), is a networking protocol for querying and modifying directory services that run on TCP/IP. LDAP is a lightweight mechanism for accessing an x.500-based directory server. RFC 2251 defines LDAP.

ACS 5.1 integrates with an LDAP external database, which is also called an identity store, by using the LDAP protocol. See Creating External LDAP Identity Stores, page 8-22 for information about configuring an LDAP identity store.

This section contains the following topics:

- Directory Service, page 8-19
- Authentication Using LDAP, page 8-19
- Multiple LDAP Instances, page 8-20
- Failover, page 8-20
- LDAP Connection Management, page 8-20
- Authenticating a User Using a Bind Connection, page 8-20
- Group Membership Information Retrieval, page 8-21
- Attributes Retrieval, page 8-22
- Certificate Retrieval, page 8-22
- Creating External LDAP Identity Stores, page 8-22
- Configuring LDAP Groups, page 8-29
- Viewing LDAP Attributes, page 8-30

Directory Service

The directory service is a software application, or a set of applications, for storing and organizing information about a computer network's users and network resources. You can use the directory service to manage user access to these resources. The LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server, and sends operation requests to the server. The server then sends its responses. One or more LDAP servers contain data from the LDAP directory tree or the LDAP backend database.

The directory service manages the directory, which is the database that holds the information. Directory services use a distributed model for storing information, and that information is usually replicated between directory servers.

An LDAP directory is organized in a simple tree hierarchy and can be distributed among many servers. Each server can have a replicated version of the total directory that 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) constructed from attributes in the entry, followed by the parent entry's DN. You can think of the DN as a full filename, and the RDN as a relative filename in a folder.

Authentication Using LDAP

ACS 5.1 can authenticate a principal against an LDAP identity store by performing a bind operation on the directory server to find and authenticate the principal. If authentication succeeds, ACS can retrieve groups and attributes that belong to the principal. The attributes to retrieve can be configured in the ACS web interface (LDAP pages). These groups and attributes can be used by ACS to authorize the principal.

To authenticate a user or query the LDAP identity store, ACS connects to the LDAP server and maintains a connection pool. See LDAP Connection Management, page 8-20.

Multiple LDAP Instances

You can create more than one LDAP instance in ACS 5.1. By creating more than one LDAP instance with different IP address or port settings, you can configure ACS to authenticate by using different LDAP servers or different databases on the same LDAP server. Each primary server IP address and port configuration, along with the secondary server IP address and port configuration, forms an LDAP instance that corresponds to one ACS LDAP identity store instance.

ACS 5.1 does not require that each LDAP instance correspond to a unique LDAP database. You can have more than one LDAP instance set to access the same database. This method is useful when your LDAP database contains more than one subtree for users or groups. Because each LDAP instance supports only one subtree directory for users and one subtree directory for groups, you must configure separate LDAP instances for each user directory subtree and group directory subtree combination for which ACS should submit authentication requests.

Failover

ACS 5.1 supports failover between a primary LDAP server and secondary LDAP server. In the context of LDAP authentication with ACS, failover applies when an authentication request fails because ACS could not connect to an LDAP server; for example, as when the server is down or is otherwise unreachable by ACS. To use this feature, you must define primary and secondary LDAP servers, and you must set failover settings.

If you set failover settings and if the first LDAP server that ACS attempts to contact cannot be reached, ACS always attempts to contact the other LDAP server. The first server ACS attempts to contact might not always be the primary LDAP server. Instead, the first LDAP server that ACS attempts to contact depends on the previous LDAP authentications attempts and on the value that you enter in the Failback Retry Delay box.

LDAP Connection Management

ACS 5.1 supports multiple concurrent LDAP connections. Connections are opened on demand at the time of the first LDAP authentication. The maximum number of connections is configured for each LDAP server. Opening connections in advance shortens the authentication time. You can set the maximum number of connections to use for concurrent binding connections. The number of opened connections can be different for each LDAP server (primary or secondary) and is determined according to the maximum number of administration connections configured for each server.

ACS retains a list of open LDAP connections (including the bind information) for each LDAP server that is configured in ACS. 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 to the connection manager.

Authenticating a User Using a Bind Connection

ACS sends a bind request to authenticate the user against an LDAP server. The bind request contains the user's DN and user password in clear text. A user is authenticated when the user's DN and password matches the username and password in the LDAP directory.

- Authentication Errors—ACS logs authentication errors in the ACS log files.
- Initialization Errors—Use the LDAP server timeout settings to configure the number of seconds that ACS waits for a response from an LDAP server before determining that the connection or authentication on that server has failed.

  Possible reasons for an LDAP server to return an initialization error are:

  - LDAP is not supported.
  - The server is down.
  - The server is out of memory.
  - The user has no privileges.
  - Incorrect administrator credentials are configured.
- Bind Errors

  Possible reasons for an LDAP server to return bind (authentication) errors are:

  - Filtering errors—A search using filter criteria fails.
  - Parameter errors—Invalid parameters were entered.
  - User account is restricted (disabled, locked out, expired, password expired, and so on).

The following errors are logged as external resource errors, indicating a possible problem with the LDAP server:

- A connection error occurred.
- The timeout expired.
- The server is down.
- The server is out of memory.

The following error is logged as an Unknown User error:

A user does not exist in the database.

The following error is logged as an Invalid Password error, where the user exists, but the password sent is invalid:

```
An invalid password was entered.
```

Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, ACS must retrieve the group membership information from LDAP databases. LDAP servers represent the association between a subject (a user or a host) and a group in one of the following two ways:

- Groups Refer to Subjects—The group objects contain an attribute that specifies the subject. Identifiers for subjects can be stored in the group as:
  - Distinguished Names (DNs)
  - Plain usernames
- Subjects Refer to Groups—The subject objects contain an attribute that specify the group they belong to.

LDAP identity stores contain the following parameters for group membership information retrieval:

- Reference Direction—Specifies the method to use when determining group membership (either Groups to Subjects or Subjects to Groups).
- Group Map Attribute—Indicates which attribute contains the group membership information.
- Group Object Class—Determines that we recognize certain objects as groups.
- Group Search Subtree—Indicates the search base for group searches.
- Member Type Option—Specifies how members are stored in the group member attribute (either as DNs or plain usernames).

Attributes Retrieval

For user authentication, user lookup, and MAC address lookup, ACS must retrieve the subject attributes from LDAP databases. For each instance of an LDAP identity store, an identity store dictionary is created. These dictionaries support attributes of the following data types:

- String
- Unsigned Integer 32
- IPv4 Address

For unsigned integers and IPv4 attributes, ACS converts the strings that it has retrieved to the corresponding data types. If conversion fails or if no values are retrieved for the attributes, ACS logs a debug message, but does not fail the authentication or the lookup process.

You can optionally configure default values for the attributes that ACS can use when the conversion fails or when ACS does not retrieve any values for the attributes.

Certificate Retrieval

If you have configured certificate retrieval as part of user lookup, then ACS must retrieve the value of the certificate attribute from LDAP. To do this, you must have configured certificate attribute in the List of attributes to fetch while configuring an LDAP identity store.

Creating External LDAP Identity Stores

Note Configuring an LDAP identity store for ACS has no effect on the configuration of the LDAP database. ACS recognizes the LDAP database, enabling the database to be authenticated against. To manage your LDAP database, see your LDAP database documentation.

When you create an LDAP identity store, ACS also creates:

- A new dictionary for that store with two attributes, ExternalGroups and IdentityDn.
- A custom condition for group mapping from the ExternalGroup attribute; the condition name has the format LDAP:<*ID_store_name*>ExternalGroups.

You can edit the predefined condition name, and you can create a custom condition from the IdentityDn attribute in the Custom condition page. See Creating, Duplicating, and Editing a Custom Session Condition, page 9-5.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit an external LDAP identity store:

Step 1 Select **Users and Identity Stores > External Identity Stores > LDAP**.

The LDAP Identity Stores page appears.

Step 2 Click **Create**. You can also:

- Check the check box next to the identity store you want to duplicate, then click **Duplicate**.
- Click the identity store name that you want to modify, or check the box next to the name and click **Edit**.

If you are creating an identity store, the first page of a wizard appears: General.

If you are duplicating an identity store, the External Identity Stores > Duplicate: "<*idstore*>" page General tab appears, where <*idstore*> is the name of the external identity store that you chose.

If you are editing an identity store, the External Identity Stores > Edit: "<*idstore*>" page General tab appears, where <*idstore*> is the name of the external identity store that you chose.

Step 3 Complete the Name and Description fields as required.

Step 4 Click **Next**. Continue with Configuring an External LDAP Server Connection, page 8-23.

Related Topic

- Deleting External LDAP Identity Stores, page 8-29

Configuring an External LDAP Server Connection

Use this page to configure an external LDAP identity store.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Users and Identity Stores > External Identity Stores > LDAP**, then click:

- **Create** and follow the wizard.
- **Duplicate**, then click **Next**. The Server Connection page appears.
- **Edit**, then click **Next**. The Server Connection page appears.

Table 8-7 LDAP: Server Connection Page

Option	Description
Server Connection	
Enable Secondary Server	Check to enable the secondary LDAP server, to use as a backup in the event that the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server.
Always Access Primary Server First	Click to ensure that the primary LDAP server is accessed first, before the secondary LDAP server is accessed.
Failback to Primary Server After <*min.*> Minutes	Click to set the number of minutes that ACS authenticates using the secondary LDAP server if the primary server cannot be reached, where <min.> is the number of minutes. After this time period, ACS reattempts authentication using the primary LDAP server. (Default = 5.)
Primary Server	
Hostname	Enter the IP address or DNS name of the machine that is running the primary 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 primary 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 by referring to the administrator of the LDAP server.
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 accessible to any unauthenticated client. In the absence of 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 distinguished name of the administrator; that is, the LDAP account which, if bound to, permits searching all required users under the User Directory Subtree and permits searching groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users that LDAP authenticates.
Password	Enter the LDAP administrator account password.
Use Secure Authentication	Click to use Secure Sockets Layer (SSL) to encrypt communication between ACS and the primary LDAP server. Verify the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must select a root CA.
Root CA	Select a trusted root certificate authority from the drop-down list box to enable secure authentication with a certificate.
Server Timeout <*sec.*> Seconds	Enter the number of seconds that ACS waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed, where <*sec.*> is the number of seconds. Valid values are 1 to 300. (Default = 10.)
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 Group Directory Subtree. Valid values are 1 to 99. (Default = 8.)

Table 8-7 LDAP: Server Connection Page (continued)

Option	Description
Test Bind To Server	Click to test and ensure that the primary LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.
Secondary Server	
Hostname	Enter the IP address or DNS name of the machine that is running the secondary 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 secondary 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 by viewing DS Properties on the LDAP machine.
Anonymous Access	Click to verify that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client to access (read and update) any data that is configured to be accessible to any unauthenticated client. In the absence of 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 domain name of the administrator; that is, the LDAP account which, if bound to, permits searching for all required users under the User Directory Subtree and permits searching groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users that LDAP authenticates.
Password	Type the LDAP administrator account password.
Use Secure Authentication	Click to use Secure Sockets Layer (SSL) to encrypt communication between ACS and the secondary LDAP server. Verify the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must select a root CA.
Root CA	Select a trusted root certificate authority from the drop-down list box to enable secure authentication with a certificate.
Server Timeout <*sec.*> Seconds	Type the number of seconds that ACS waits for a response from the secondary LDAP server before determining that the connection or authentication with that server has failed, where <*sec.*> is the number of seconds. Valid values are 1 to 300. (Default = 10.)
Max Admin Connections	Type 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 Group Directory Subtree. Valid values are 1 to 99. (Default = 8.)
Test Bind To Server	Click to test and ensure that the secondary LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.

Step 2 Click **Next**. Continue with Configuring External LDAP Directory Organization, page 8-26.

Configuring External LDAP Directory Organization

Use this page to configure an external LDAP identity store.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Users and Identity Stores > External Identity Stores > LDAP**, then click:

- **Create** and follow the wizard until you reach the Directory Organization page.
- **Duplicate**, then click **Next** until the Directory Organization page appears.
- **Edit**, then click **Next** until the Directory Organization page appears.

Table 8-8 LDAP: Directory Organization Page

Option	Description
Schema	
Subject Object class	The value of the LDAP *objectClass* attribute that identifies the subject. Often, subject records have several values for the *objectClass* attribute, some of which are unique to the subject, some of which are shared with other object types. This box should contain a value that is not shared. Valid values are from 1 to 20 characters and must be a valid LDAP object type. This parameter can contain any UTF-8 characters. (Default = Person.)
Group Object class	Enter the group object class that you want to use in searches that identify objects as groups. (Default = GroupOfUniqueNames.)
Subject Name Attribute	The name of the attribute in the subject record that contains the subject name. You can obtain this attribute name from your directory server. This attribute specifies the subject name in the LDAP schema. You use this attribute to construct queries to search for subject objects. For more information, refer to the LDAP database documentation. Valid values are from 1 to 20 characters and must be a valid LDAP attribute. This parameter can contain any UTF-8 characters. Common values are *uid* and *CN*. (Default = uid.*)*
Group Map Attribute	For user authentication, user lookup, and MAC address lookup, ACS must retrieve group membership information from LDAP databases. LDAP servers represent an association between a subject (a user or a host) and a group in one of the following two ways: • Groups refer to subjects • Subjects refer to groups The Group Map Attribute contains the mapping information. You must enter the attribute that contains the mapping information: an attribute in either the subject or the group, depending on: • If you select the Subject Objects Contain Reference To Groups radio button, enter a subject attribute. • If you select Group Objects Contain Reference To Subjects radio button, enter a group attribute.

Table 8-8 LDAP: Directory Organization Page (continued)

Option	Description
Certificate Attribute	Enter the attribute that contains certificate definitions. These definitions can optionally be used to validate certificates presented by clients when defined as part of a certificate authentication profile. In such cases, a binary comparison is performed between the client certificate and the certificate retrieved from the LDAP identity store.
Subject Objects Contain Reference To Groups	Click if the subject objects contain a reference to groups.
Group Objects Contain Reference To Subjects	Click if the group objects contain a reference to subjects.
Subjects In Groups Are Stored In Member Attribute As	Use the drop-down list box to indicate if the subjects in groups are stored in member attributes as either: • Username • Distinguished name
Directory Structure	

Subject Search Base	Enter the distinguished name (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 distinguished name (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.

Test Configuration	Click to obtain the expected connection and schema results by counting the number of users and groups that may result from your configuration.
Username Prefix\Suffix Stripping	

Table 8-8 LDAP: Directory Organization Page (continued)

Option	Description
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, ACS finds the delimiter character that is specified in the <start_string> box, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the <start_string> box, ACS strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is DOMAIN\echamberlain, ACS submits echamberlain to an LDAP server. **Note** The <start_string> cannot contain the following special characters: the pound sign (#), the question mark (?), the quote (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ACS does not allow these characters in usernames. If the X box contains any of these characters, stripping fails.
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, ACS finds the delimiter character that is specified in the Y box, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the character specified in the Y box, ACS strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is the at symbol (@) and the username is *jwiedman@domain*, then ACS submits *jwiedman* to an LDAP server. **Note** The <*end_string*> box cannot contain the following special characters: the pound sign (#), the question mark (?), the quote ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ACS does not allow these characters in usernames. If the <*end_string*> box contains any of these characters, stripping fails.
MAC Address Format	
Search for MAC Address in Format <*format*>	MAC addresses in internal identity stores are stored in the format xx-xx-xx-xx-xx-xx. MAC addresses in LDAP databases can be stored in different formats. However, when ACS receives a host lookup request, ACS converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list box to enable search for MAC addresses in a specific format, where <*format*> can be any one of the following: • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx • xxxx.xxxx.xxxx The format you select must match the format of the MAC address stored in the LDAP server.

Step 2 Click **Finish**.

The external identity store you created is saved.

Related Topics

- Configuring LDAP Groups, page 8-29
- Deleting External LDAP Identity Stores, page 8-29

Deleting External LDAP Identity Stores

You can delete one or more external LDAP identity stores simultaneously.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To delete an external LDAP identity store:

Step 1 Select **Users and Identity Stores > External Identity Stores > LDAP**.

The LDAP Identity Stores page appears, with a list of your configured external identity stores.

Step 2 Check one or more check boxes next to the external identity stores you want to delete.

Step 3 Click **Delete**.

The following error message appears:

Are you sure you want to delete the selected item/items?

Step 4 Click **OK**.

The External Identity Stores page appears, without the deleted identity stores in the list.

Related Topic

- Creating External LDAP Identity Stores, page 8-22

Configuring LDAP Groups

Use this page to configure an external LDAP group.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Users and Identity Stores > External Identity Stores > LDAP**, then click:

- **Create** and follow the wizard.
- **Duplicate**, then click the **Directory Groups** tab.
- **Edit**, then click the **Directory Groups** tab.

The Selected Directory Groups field displays a list of groups that are available as options in rule-table group-mapping conditions.

Step 2 Do one of the following:

- Click **Select** to open the Groups secondary window from which you can select groups and add them to the Selected Directory Groups list.

- You can alternatively enter the LDAP groups in the Group Name field and click **Add**.

To remove a selected group from the Selected Directory Groups list, select that group in the Selected Directory Groups list and Click **Deselect**.

Step 3 Click **Submit** to save your changes.

Viewing LDAP Attributes

Use this page to view the external LDAP attributes.

Step 1 Select **Users and Identity Stores > External Identity Stores > LDAP**.

Step 2 Check the check box next to the LDAP identity store whose attributes you want to view, click **Edit**, and then click the **Directory Attributes** tab.

Step 3 In the Name of example Subject to Select Attributes field, enter the name of an example object from which to retrieve attributes, then click **Select**. For example, the object can be an user and the name of the object could either be the username or the user's DN.

Step 4 Complete the fields as described in Table 8-9

Table 8-9 LDAP: Attributes Page

Option	Description
Attribute Name	Type an attribute name that you want included in the list of available attributes for policy conditions.
Type	Select the type you want associated with the attribute name you entered in the Attribute Name field.
Default	Specify the default value you want associated with the attribute name you entered in the Attribute Name field. If you do not specify a default value, no default is used. **Note** When attributes are imported to the Attribute Name/Type/Default box via the Select button, these default values are used: – String—Name of the attribute – Unsigned Integer 32 – IPv4 Address
Policy Condition Name	(*Optional*) Specify the name of the custom condition for this attribute. This condition will be available for selection when customizing conditions in a policy.

Step 5 Click **Add** and the information you entered is added to the fields on the screen. The attributes listed here are available for policy conditions.

Step 6 Click **Submit** to save your changes.

Leveraging Cisco NAC Profiler as an External MAB Database

ACS communicates with Cisco NAC Profiler to enable non-802.1X-capable devices to authenticate in 802.1X-enabled networks. Endpoints that are unable to authenticate through 802.1X use the MAC Authentication Bypass (MAB) feature in switches to connect to an 802.1X-enabled network.

Typically, non-user-attached devices such as printers, fax machines, IP phones, and Uninterruptible Power Supplies (UPSs) are not equipped with an 802.1x supplicant.

This means the switch port to which these devices attach cannot authenticate them using the 802.1X exchange of device or user credentials and must revert to an authentication mechanism other than port-based authentication (typically endpoint MAC address-based) in order for them to connect to the network.

Cisco NAC Profiler provides a solution for identifying and locating the endpoints that are unable to interact with the authentication component of these systems so that these endpoints can be provided an alternative mechanism for admission to the network.

NAC Profiler consists of an LDAP-enabled directory, which can be used for MAC Authentication Bypass (MAB). Thus, the NAC Profiler acts as an external LDAP database for ACS to authenticate non-802.1X-capable devices.

Note You can use the ACS internal host database to define the MAC addresses for non-802.1X-capable devices. However, if you already have a NAC Profiler in your network, you can use it to act as an external MAB database.

To leverage Cisco NAC Profiler as an external MAB database, you must:

- Enable the LDAP Interface on Cisco NAC Profiler. See Enabling the LDAP Interface on Cisco NAC Profiler to Communicate with ACS, page 8-31.
- Configure NAC Profiler in ACS. See Configuring NAC Profile LDAP Definition in ACS for Use in Identity Policy, page 8-33.

Enabling the LDAP Interface on Cisco NAC Profiler to Communicate with ACS

Note Before you can enable the LDAP interface on the NAC Profiler, ensure that you have set up your NAC Profiler with the NAC Profiler Collector. For more information on configuring Cisco NAC Profiler, refer to the *Cisco NAC Profiler Installation and Configuration Guide*, available under http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html.

To enable the LDAP interface on the NAC Profiler to communicate with ACS:

Step 1 Log in to your Cisco NAC Profiler.

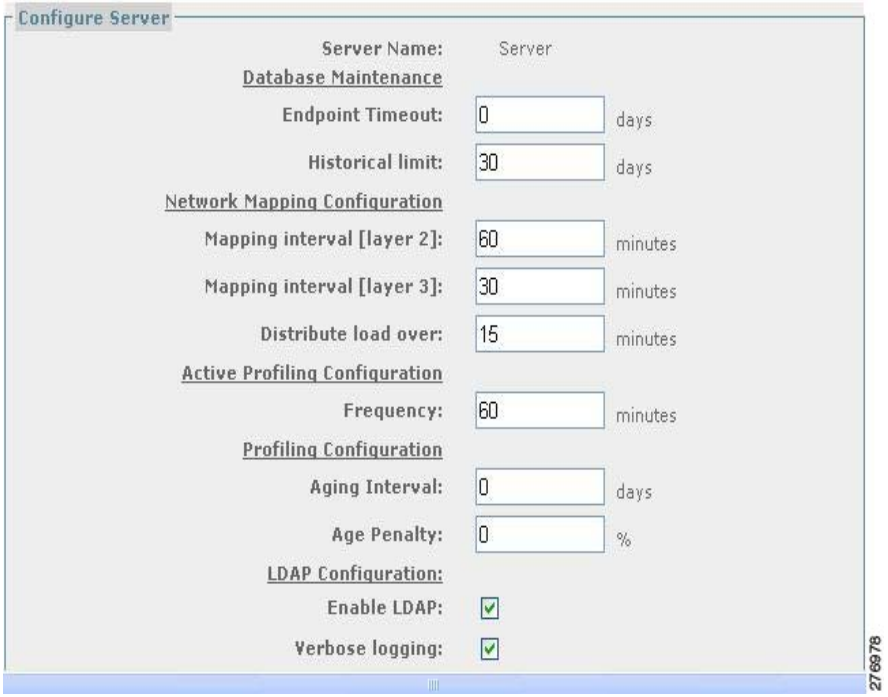
Step 2 Choose **Configuration > NAC Profiler Modules > List NAC Profiler Modules**.

Step 3 Click **Server**.

The Configure Server page appears.

Step 4 In the LDAP Configuration area, check the **Enable LDAP** check box as shown in Figure 8-1.

Figure 8-1 LDAP Interface Configuration in NAC Profiler



Step 5 Click **Update Server**.

Step 6 Click the **Configuration** tab and click **Apply Changes**.

The Update NAC Profiler Modules page appears.

Step 7 Click **Update Modules** to enable LDAP to be used by ACS.

You must enable the endpoint profiles that you want to authenticate against the Cisco NAC Profiler. For information on how to do this, see Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication, page 8-32.

For proper Active Response Events you need to configure Active Response Delay time from your Cisco NAC Profiler UI. For this, choose **Configuration > NAC Profiler Modules > Configure Server > Advanced Options > Active Response Delay**.

Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication

For the non-802.1X endpoints that you want to successfully authenticate, you must enable the corresponding endpoint profiles in NAC Profiler for LDAP authentication.

Note If the profile is not enabled for LDAP, the endpoints in the profile will not be authenticated by the Cisco NAC Profiler.

To enable the endpoint profiles for LDAP authentication:

Step 1 Log into your NAC Profiler.

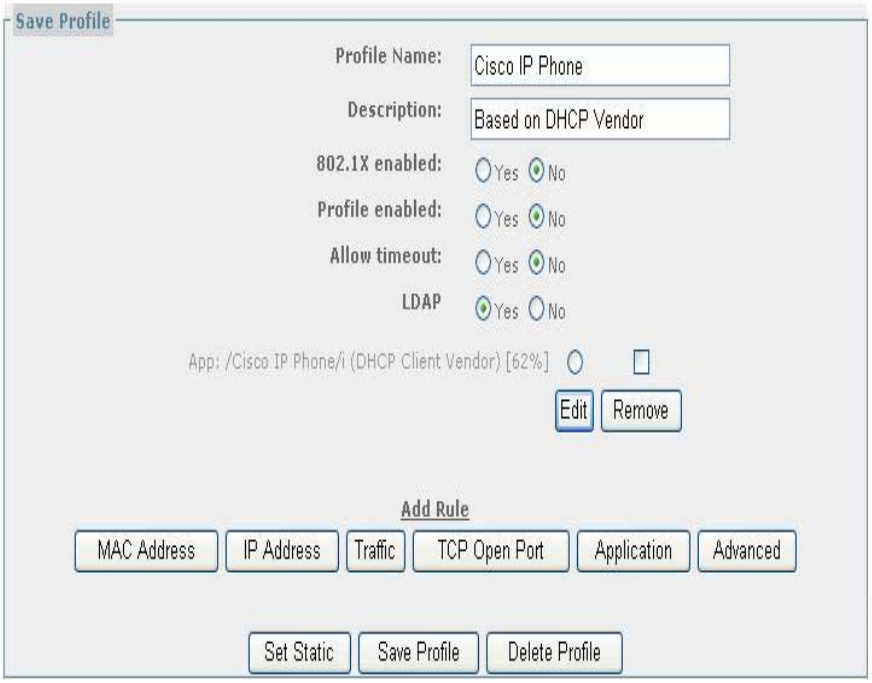
Step 2 Choose **Configuration > Endpoint Profiles > View/Edit Profiles List**.

A list of profiles in a table appears.

Step 3 Click on the name of a profile to edit it.

Step 4 In the Save Profile page, ensure that the LDAP option is enabled by clicking the **Yes** radio button next to it, if it is not already done as shown in Figure 8-2.

Figure 8-2 Configuring Endpoint Profiles in NAC Profiler



Step 5 Click **Save Profile**.

Configuring NAC Profile LDAP Definition in ACS for Use in Identity Policy

After you install ACS, there is a predefined LDAP database definition for NAC Profiler. This predefined database definition for NAC Profiler contains all the required data for establishing an initial connection. The only exception is the host information, which depends on your specific deployment configuration.

The steps below describe how to configure the host information, verify the connection, and use the profile database in policies.

Note Make sure that ACS NAC Profiler is choosen under **Access Policies > Access Services > Default Network Access > Identity**.

Note The **NAC Profiler** template in ACS, available under the LDAP external identity store, works with Cisco NAC Profiler version 2.1.8 and later.

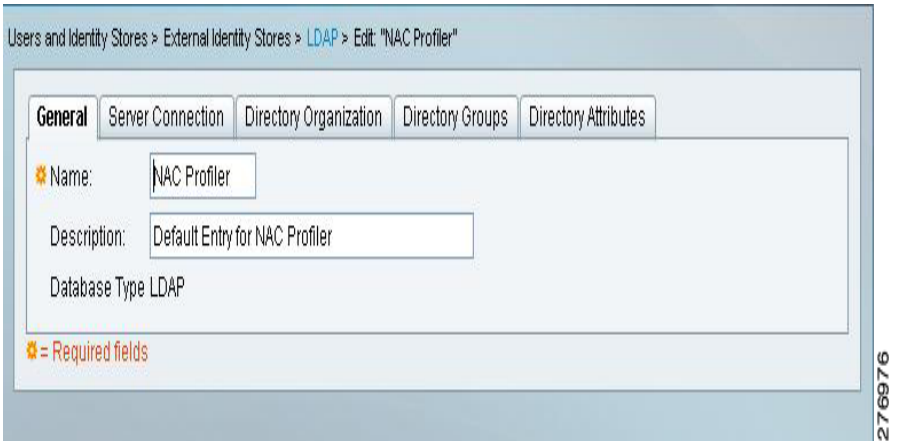
To edit the NAC Profiler template in ACS:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

Step 2 Click on the name of the NAC Profiler template or check the check box next to the NAC Profiler template and click **Edit**.

The Edit NAC Profiler definition page appears as shown in Figure 8-3.

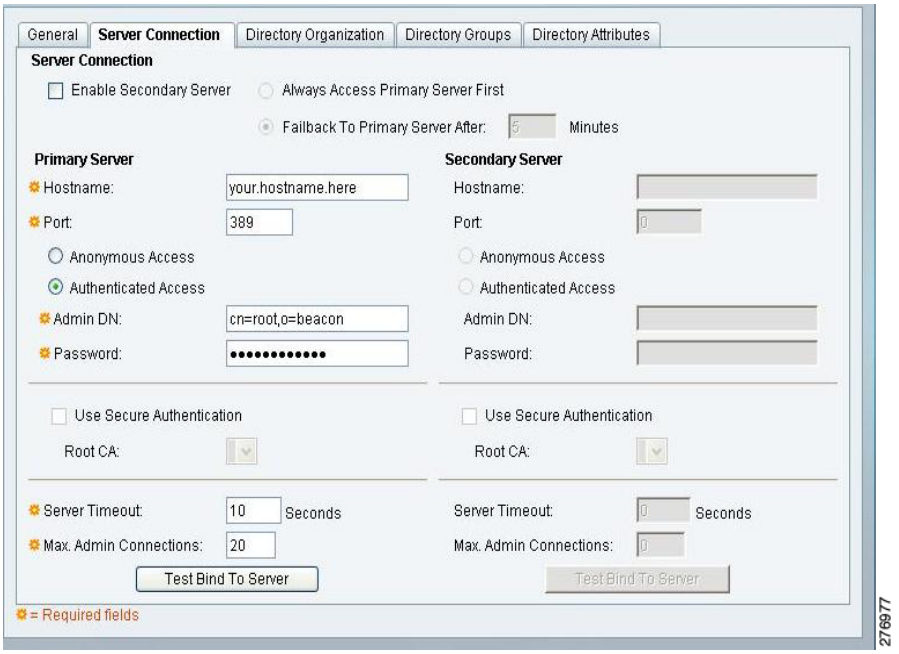
Figure 8-3 Edit NAC Profiler Definition - General Page



Step 3 Click the **Server Connection** tab.

The Edit page appears as shown in Figure 8-4.

Figure 8-4 Edit NAC Profiler Definition - Server Connection Page



Step 4 In the **Primary Server Hostname** field, enter the IP address or fully qualified domain name of the Profiler Server, or the Service IP of the Profiler pair if Profiler is configured for High Availability.

Step 5 Click **Test Bind to Server** to test the connection and verify ACS can communicate with Profiler through LDAP.

A small popup dialog, similar to the one shown in Figure 8-5 appears.

Figure 8-5 Test Bind to Server Dialog Box

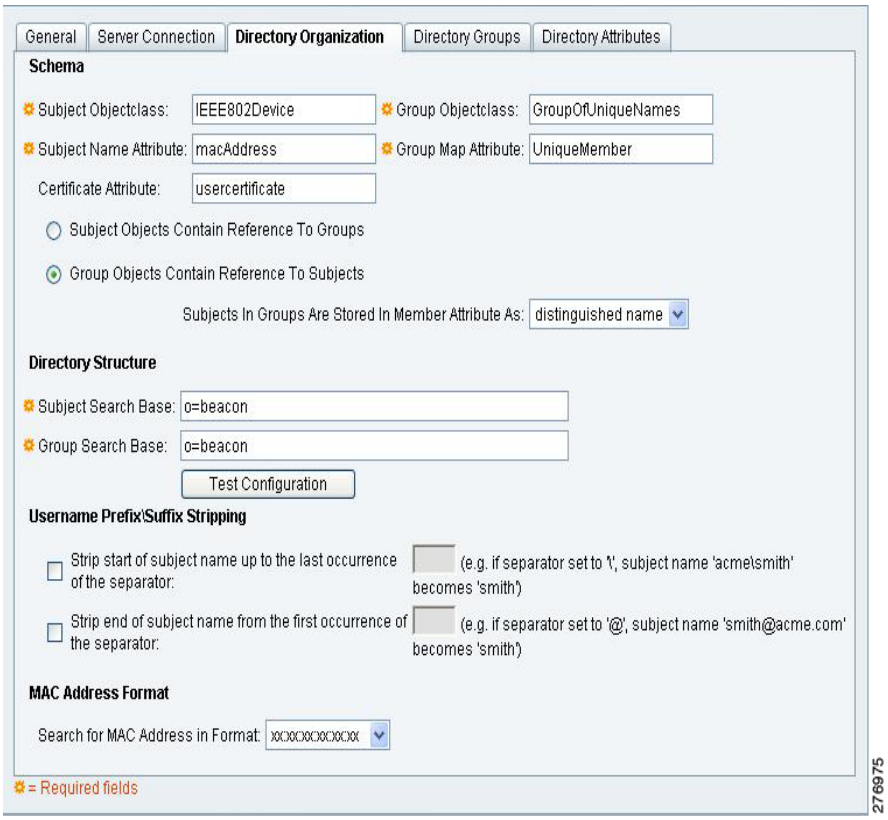
For more information, see Creating External LDAP Identity Stores, page 8-22.

Note The default password for LDAP is *GBSbeacon*. If you want to change this password, refer to the *Cisco NAC Profiler Installation and Configuration Guide* at the following location: http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/310/p_ldap31.html#wp1057155

Step 6 If successful, go to the **Directory Organization** tab.

The Edit page appears as shown in Figure 8-6.

Figure 8-6 Edit NAC Profiler Definition - Directory Organization Page

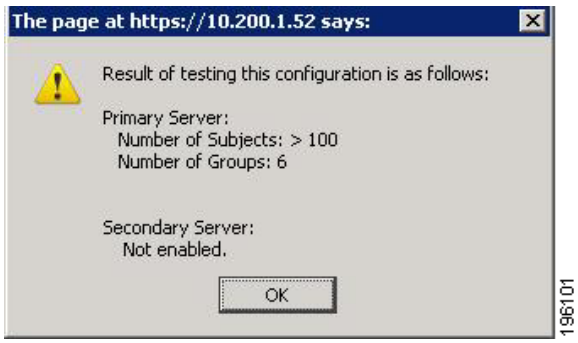


Step 7 Click **Test Configuration**.

A dialog box as shown in Figure 8-7 appears that lists data corresponding to the Profiler. For example:

- Primary Server
- Number of Subjects: 100
- Number of Directory Groups: 6

Figure 8-7 Test Configuration Dialog Box



Number of Subjects—This value maps to the actual subject devices already profiled by the Cisco NAC Profiler (actual devices enabled for Profiler).

After the Profiler receives initial SNMP trap information from the switch, Profiler can poll the switch using SNMP to gather MIB (Management Information Base) information about the switch as well as the connecting endpoint.

After the Profiler has learned about the endpoint (e.g. MAC address, switch port), it adds the endpoint to its database. An endpoint added to the Profiler's database is considered 1 subject.

Number of Directory Groups—This value maps to the actual profiles enabled for LDAP on Profiler. When already running Profiler on your network, default profiles for endpoints are pre-configured.

However, all profiles are not enabled for LDAP, and must be configured as described in Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication, page 8-32. Note that if setting up Profiler for the first time, once the Profiler is up and running, you will see zero groups initially.

Note The subjects and directory groups are listed if they are less than 100 in number. If the number of subjects or directory groups exceed 100, the subjects and directory groups are not listed. Instead, you get a message similar to the following one:

```
More than 100 subjects are found.
```

Step 8 Click the Directory Attributes tab if you want to use the directory attributes of subject records as policy conditions in policy rules. See Viewing LDAP Attributes, page 8-30 for more information.

Step 9 Choose NAC Profiler as the result (Identity Source) of the identity policy. For more information, see Viewing Identity Policies, page 10-21.

As soon as Endpoint is successfully authenticated from ACS server, ACS will do a CoA (Change of Authorization) and change VLAN. For this, you can configure static VLAN mapping in ACS server. For more information, see Specifying Common Attributes in Authorization Profiles, page 9-20.

When Endpoint is successfully authenticated the following message is displayed on the switch.

```
ACCESS-Switch# #show authentication sessions
Interface MAC Address Method Domain Status Session ID
Fa1/0/1 0014.d11b.aa36 mab DATA Authz Success 505050010000004A0B41FD15
```

For more information on features like Event Delivery Method and Active Response, see the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1* at the follwing location: http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/310/p_prof_events31.html

Troubleshooting MAB Authentication with Profiler Integration

Following are the steps to troubleshoot MAB authentication while integrating with NAC Profiler:

Step 1 To verify that the endpoint is successfully authenticated, run the following command on the switch which is conencted to the endpoint devices:

```
ACCESS-Switch# show authentication sessions
```

The following output is displayed:

```
Interface  MAC Address    Method   Domain  Status         Session ID
Fa1/0/1    0014.d11b.aa36 mab      DATA     Authz Success  505050010000004A0B41FD15 reject
```

Step 2 Enable debugging for SNMP, AAA, and 802.1X on the switch.

Step 3 Verify the MAB authentication logs in **Monitoring and Reports Viewer > Troubleshooting**, for failure and success authentications.

Microsoft AD

ACS uses Microsoft Active Directory (AD) as an external identity store to store resources such as, users, machines, groups, and attributes. ACS authenticates these resources against AD.

Supported Authentication Protocols

- EAP-FAST and PEAP—ACS 5.1 supports user and machine authentication and change password against AD using EAP-FAST and PEAP with an inner method of MSCHAPv2 and EAP-GTC.
- PAP—ACS 5.1 supports authenticating against AD using PAP and also allows you to change AD users password.
- MSCHAPv1—ACS 5.1 supports user and machine authentication against AD using MSCHAPv1. You can change AD users password using MSCHAPv1 version 2. ACS does not support MS-CHAP MPPE-Keys of a user, but does support MPPE-Send-Key and MPPE-Recv-Key.

Note ACS 5.1 does not support changing user password against AD using MSCHAPv1 version 1.

- MSCHAPv2—ACS 5.1 supports user and machine authentication against AD using MSCHAPv2. ACS does not support MS-CHAP MPPE-Keys of a user, but does support MPPE-Send-Key and MPPE-Recv-Key.
- EAP-GTC—ACS 5.1 supports user and machine authentication against AD using EAP-GTC.
- EAP-TLS—ACS uses the certificate retrieval option introduced in 5.1 to support user and machine authentication against AD using EAP-TLS.

Changing the password for EAP-FAST and PEAP with inner MSCHAPv2 is also supported.

ACS supports these AD domains:

- Windows Server 2000
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008

ACS machine access restriction (MAR) features use AD to map machine authentication to user authentication and authorization, and sets a the maximal time allowed between machine authentication and an authentication of a user from the same machine. Most commonly, MAR fails authentication of users whose host machine does not successfully authenticate or if the time between machine and user authentication is greater than the specified aging time. You can add MAR as a condition in authentication and authorization rules as required.

While trying to join ACS to the AD domain, ACS and AD must be time-synchronized. Time in ACS is set according to the Network Time Protocol (NTP) server. Both AD and ACS should be synchronized by the same NTP server. If time is not synchronized when you join ACS to the AD domain, ACS displays a clock skew error. Using the command line interface on your appliance, you must configure the NTP

client to work with the same NTP server that the AD domain is synchronized with. Refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/command/reference/acs5_1_cli.html for more information.

Note You have to add a UPN suffix or NETBIOS prefix to the username when authenticating to a domain that the ACS is not joined to, including the child domains.

ACS 5.1 supports certificate authorization.

If there is a firewall between ACS and AD, certain ports need to be opened in order to allow ACS to communicate with AD. The following are the default ports to be opened:

Protocol	Port number
LDAP	389/udp
SMB	445/tcp
KDC	88/(tcp/udp)
Global catalog	3268/tcp
KPASS	464/tcp
NTP	123/udp

Note Dial-in users are not supported by AD in ACS.

This section contains the following topics:

- Machine Authentication, page 8-39
- Attribute Retrieval for Authorization, page 8-40
- Group Retrieval for Authorization, page 8-40
- Certificate Retrieval for EAP-TLS Authentication, page 8-40
- Concurrent Connection Management, page 8-40
- User and Machine Account Restrictions, page 8-40
- Machine Access Restrictions, page 8-41
- Joining ACS to an AD Domain, page 8-43
- Configuring an AD Identity Store, page 8-43
- Selecting an AD Group, page 8-45
- Configuring AD Attributes, page 8-46

Machine Authentication

Machine authentication provides access to network services to only these computers that are listed in Active Directory. This becomes very important for wireless networks because unauthorized users can try to access your wireless access points from outside your office building. Machine authentication happens while starting up a computer or while logging in to a computer. Supplicants, such as Funk Odyssey perform machine authentication periodically while the supplicant is running. If you enable machine

authentication, ACS authenticates the computer before a user authentication request comes in. ACS checks the credentials provided by the computer against the Windows user database. If the credentials match, the computer is given access to the network.

Attribute Retrieval for Authorization

You can configure ACS to retrieve user or machine AD attributes to be used in authorization and group mapping rules. The attributes are mapped to the ACS policy results and determine the authorization level for the user or machine. ACS retrieves user and machine AD attributes after a successful user or machine authentication and can also retrieve the attributes for authorization and group mapping purposes independent of authentication.

Group Retrieval for Authorization

ACS can retrieve user or machine groups from Active Directory after a successful authentication and also retrieve the user or machine group independent of authentication for authorization and group mapping purposes. You can use the AD group data in the authorization and group mapping tables and introduce special conditions to match them against the retrieved groups.

Certificate Retrieval for EAP-TLS Authentication

ACS 5.1 supports certificate retrieval for user or machine authentication that uses EAP-TLS protocol. The user or machine record on AD includes a certificate attribute of binary data type. This can contain one or more certificates. ACS refers to this attribute as userCertificate and does not allow you to configure any other name for this attribute. ACS retrieves this certificate for verifying the identity of the user or machine. The certificate authentication profile determines the field (SAN, CN, or SSN) to be used for retrieving the certificates. After ACS retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, ACS compares the certificates to check if one of them match. When a match is found, ACS grants the user or machine access to the network.

Concurrent Connection Management

After ACS connects to the AD domain, at startup, ACS creates a number of threads to be used by the AD identity store for improved performance. Each thread has its own connection.

User and Machine Account Restrictions

While authenticating or querying a user or a machine, ACS checks for the following:

- Is the user account disabled?
- Is the user locked out?
- Has the user's account expired?
- Is the query run outside of the specified logon hours?

If the user has one of these limitations, the *AD1::IdentityAccessRestricted* attribute on the AD dedicated dictionary is set to indicate that the user has restricted access. You can use this attribute in all policy rules.

Machine Access Restrictions

MAR helps tying the results of machine authentication to user authentication and authorization process. The most common usage of MAR is to fail authentication of users whose host machine does not successfully authenticate. The MAR is effective for all authentication protocols.

MAR functionality is based on the following points:

- As a result of Machine Authentication, the machine's RADIUS `Calling-Station-ID attribute (31)` is cached as an evidence for later reference.
- Administrator can configure the time to live (TTL) of the above cache entries in the AD settings page.
- Administrator can configure whether or not MAR is enabled in the AD settings page. However for MAR to work the following limitations must be taken into account:
  - Machine authentication must be enabled in the authenticating protocol settings
  - The AAA client must send a value in the Internet Engineering Task Force (IETF) RADIUS `Calling-Station-Id attribute (31).`
  - ACS does not replicate the cache of `Calling-Station-Id attribute` values from successful machine authentications.
  - ACS do not persevere the cache of `Calling-Station-Id attribute`. So the content is lost in case you restart ACS or if it crashes. The content is not verified for consistency in case the administrator performs configuration changes that may effect machine authentication.
  - Dialup is not supported for 5.1.
- When user authenticates with either PEAP or EAP-FAST, against AD external ID store then ACS performs an additional action. It searches the cache for the users `Calling-Station-Id`. If it is found then **Was-Machine-Authenticated** attribute is set to true on the session context, otherwise set to false.
- For the above to function correctly, the user authentication request should contain the `Calling-Station-Id`. In case it does not, the **Was-Machine-Authenticated** attribute shall be set to false.
- The administrator can add rules to authorization policies that are based on AD GM attribute and on Machine authentication required attribute. Any rule that contains these two attributes will only apply if the following conditions are met:
  - MAR feature is enabled
  - Machine authentication in the authenticating protocol settings is enabled
  - External ID store is AD
- When a rule such as the one described above is evaluated, the attributes of AD GM and **Was-Machine-Authenticated** are fetched from the session context and checked against the rule's condition. According to the results of this evaluation an authorization result is set.
- Exemption list functionality is supported implicitly (in contrast to ACS 4.x). To exempt a given user group from the MAR the administrator can set a rule such that the column of **AD Group** consists of the group to exempt and the column of **Machine Authentication Required** consists of *No*. See the second rule in the table below for an example.

  For example, the administrator will add rules to the authorization policy as follows:

AD Group	Machine Authentication Required	…	ATZ profile
Engineers	Yes	…	VLAN X
Managers	No	…	VLAN B
…	…	…	DENY ACCESS

The Engineers' rule is an example of MAR rule that only allows engineers access if their machine was successfully authenticated against windows DB.

The Managers' rule is an example of an exemption from MAR.

Joining ACS to an AD Domain

After you configure the AD identity store in ACS through the ACS web interface, you must submit the configuration to join ACS to the AD domain. For more information on how to configure an AD identity store, see Configuring an AD Identity Store, page 8-43.

Note The Windows AD account, which joins ACS to the AD domain, can be placed in its own organizational unit (OU). It resides in its own OU either when the account is created or later on, with a restriction that the appliance name must match the name of the AD account.

Note ACS does not support user authentication in AD when a user name is supplied with an alternative UPN suffix configured in OU level. The authentication works fine if the UPN suffix is configured in domain level.

Related Topic

- Machine Authentication, page B-32

Configuring an AD Identity Store

When you configure an AD identity store, ACS also creates:

- A new dictionary for that store with two attributes: ExternalGroups and another attribute for any attribute retrieved from the Directory Attributes page.
- A new attribute, IdentityAccessRestricted. You can manually create a custom condition for this attribute.
- A custom condition for group mapping from the ExternalGroup attribute; the custom condition name is AD1:ExternalGroups and another custom condition for each attribute selected in the Directory Attributes page (for example, AD1:cn).

You can edit the predefined condition name, and you can create a custom condition from the Custom condition page. See Creating, Duplicating, and Editing a Custom Session Condition, page 9-5.

To authenticate users and join ACS with an AD domain:

Step 1 Select **Users and Identity Stores > External Identity Stores > Active Directory**.

The Active Directory page appears.

Step 2 Modify the fields in the General tab as described in Table 8-10.

Table 8-10 Active Directory: General Page

Option	Description
Connection Details	
Active Directory Domain Name	Name of the AD domain to join ACS to.
Username	Predefined user in AD. AD account required for domain access in ACS should have either of the following: • Add workstations to domain user right in corresponding domain. • Create Computer Objects or Delete Computer Objects permission on corresponding computers container where ACS machine's account is precreated (created before joining ACS to the domain).
Password	Enter the user password.
Test Connection	Click to test the ACS connection with the AD domain for the user, domain, and password identified in the previous fields. A message appears informing you whether the AD server is routable within the network and also authenticates the given AD username and password.
End User Authentication Settings	
Enable password change	Click to allow the password to be changed.
Enable machine authentication	Click to allow machine authentication.
Enable Machine Access Restrictions	Click to ensure that machine authentication results are tied to user authentication and authorization. If you enable this feature, you must set the Aging time.
Aging time (hours) <*time*>	The time after a machine was authenticated that a user can be authenticated from that machine. If this time elapses, user authentication fails. You must set this time if you clicked the Enable Machine Access Restrictions check box.
Connectivity Status	
Joined to Domain	(*Display only.*) After you save the configuration (by clicking **Save Changes**), shows the domain name with which ACS is joined.
Connectivity Status	(*Display only.*) After you save the configuration (by clicking **Save Changes**), shows the connection status of the domain name with which ACS is joined.

Step 3 Click:

- **Save Changes** to save the configuration, join the ACS to the specified AD domain with the configured credentials, and start the AD agent.
- **Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that:
  - There are no policy rules that use custom conditions based on the AD dictionary.
  - The AD is not chosen as the identity source in any of the available access services.
  - There are no identity store sequences with the AD.

The Active Directory configuration is saved. The Active Directory page appears with the new configuration.

Note The Windows AD account, which joins ACS to the AD domain, can be placed in its own Organizational Unit (OU). It resides in its own OU either when the account is created or later on with a restriction that the appliance name must match the name of the AD account.

Note ACS will perform a new join to the AD domain each time the services are restarted.

Note Due to NETBIOS limitations, ACS hostnames must contain less than or equal to 15 characters.

Warning **If ACS has long hostnames whose first 15 characters are the same on more than one appliance, only one appliance can be connected to the domain.**

Related Topics

- Selecting an AD Group, page 8-45
- Configuring AD Attributes, page 8-46

Selecting an AD Group

Use this page to select groups that can then be available for policy conditions.

Note To select groups and attributes from an AD, ACS must be connected to that AD.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Directory Groups** tab.

The Groups page appears. The Selected Directory Groups field lists the AD groups you selected and saved. The AD groups you selected in the External User Groups page are listed and can be available as options in group mapping conditions in rule tables.

Note If you have more groups in other trusted domain or forest that are not displayed, you can use the search filter to narrow down your search results.

Step 2 Click **Select** to see the available AD groups on the domain (and other trusted domains in the same forest).

The External User Groups dialog box appears displaying a list of AD groups in the domain, as well as other trusted domains in the same forest.

Note If you have more groups that are not displayed, use the search filter to refine your search and click **Go**.

Step 3 Enter the AD groups or select them from the list, then click **OK**.

To remove an AD group from the list, click an AD group, then click **Deselect**.

Step 4 Click:

- **Save Changes** to save the configuration.
- **Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

Note Logon authentication may fail on Active Directory when ACS tries to authenticate Users who belong to more than 1015 groups in external identity stores. This is due to the Local Security Authentication (LSA) limitations in Active Directory.

Configuring AD Attributes

Use this page to select attributes that can then be available for policy conditions.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Directory Attributes** tab.

Step 2 Complete the fields in the Active Directory: Attributes page as described in Table 8-11:

Table 8-11 Active Directory: Attributes Page

Option	Description
Name of example Subject to Select Attributes	Enter the name of a user or computer found on the joined domain. You can enter the user's or the computer's CN or distinguished name. **Note** The set of attributes that are displayed belong to the subject that you specify. The set of attributes are different for a user and a computer.
Select	Click to access the Attributes secondary window, which displays the attributes of the name you entered in the previous field.
Attribute Name List—Displays the attributes you selected in the secondary Selected Attributes window.	

Table 8-11 Active Directory: Attributes Page (continued)

Option	Description
Attribute Name	• Do one of the following: – Enter the name of the attribute. – You can also select an attribute from the list, then click **Edit** to edit the attribute. • Click **Add** to add an attribute to the Attribute Name list.
Type	Attribute types associated with the attribute names. Valid options are: • String • Unsigned Integer 32 • IPv4 Address
Default	Specified attribute default value for the selected attribute: • String—Name of the attribute. • Unsigned Integer 32—0. • IPv4 Address—No default set.
Policy Condition Name	Enter the custom condition name for this attribute. For example, if the custom condition name is *AAA*, enter **AAA** in this field and not **AD1:*att_name***.
Select Attributes Secondary Window	Available from the Attributes secondary window only.
Search Filter	Specify a user or machine name. For user names, you can specify distinguished name, SAM, NetBios, or UPN format. For machine names, you can specify one of the following formats: MACHINE$, NETBiosDomain\MACHINE$, host/MACHINE, or host/machine.domain. You can specify non-English letters for user and machine names.
Attribute Name	The name of an attribute of the user or machine name you entered in the previous field.
Attribute Type	The type of attribute.
Attribute Value	The value of an attribute for the specified user or machine.

Step 3 Click:

- **Save Changes** to save the configuration.
- **Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

RSA SecurID Server

ACS supports the RSA SecurID server as an external database. RSA SecurID two-factor authentication consists of the user's personal identification number (PIN) 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.

You can integrate with RSA SecurID authentication technology in any one of the following ways:

- Using the RSA SecurID agent—Users are authenticated with username and passcode through the RSA's native protocol.
- Using the RADIUS protocol—Users are authenticated with username and passcode through the RADIUS protocol.

RSA SecurID token server in ACS 5.1 integrates with the RSA SecurID authentication technology by using the RSA SecurID Agent. ACS 5.1 supports RSA SecurID token server versions 6.x and 7.x.

Configuring RSA SecurID Agents

The RSA SecurID Server administrator can do the following:

- Create an Agent Record (sdconf.rec), page 8-48
- Reset the Node Secret (securid), page 8-48
- Override Automatic Load Balancing, page 8-48
- Manually Intervene to Remove a Down RSA SecurID Server, page 8-49

Create an Agent Record (sdconf.rec)

To configure an RSA SecurID token server in ACS 5.1, the ACS administrator requires the *sdconf.rec* file. The *sdconf.rec* file is a configuration record file that specifies how the RSA agent communicates with the RSA SecurID server realm. In order to create the *sdconf.rec* file, the RSA SecurID server administrator should add the ACS host as an Agent host on the RSA SecurID server and generate a configuration file for this agent host. Make sure that you add the IP address of every ACS server in your network that will be using the RSA server.

Reset the Node Secret (securid)

After the agent initially communicates with the RSA SecurID server, the server provides the agent with a node secret file called securid. Subsequent communication between the server and the agent relies on exchanging the node secret to verify the other's authenticity. At times, you might have to reset the node secret. To reset the node secret:

- The RSA SecurID server administrator must uncheck the Node Secret Created check box on the Agent Host record in the RSA SecurID server.
- The ACS administrator must remove the securid file from ACS.

Override Automatic Load Balancing

RSA SecurID Agent automatically balances the requested loads on the RSA SecurID servers in the realm. However, you do have the option to manually balance the load. You can specify which server each of the agent hosts must use and assign a priority to each server so that the agent host directs authentication requests to some servers more frequently than others. You must specify the priority settings in a text file and save it as sdopts.rec, which you can then upload to ACS.

Manually Intervene to Remove a Down RSA SecurID Server

When an RSA SecurID server is down, the automatic exclusion mechanism does not always work quickly. To speed up this process, you can remove the *sdstatus.12* file from ACS.

Creating and Editing RSA SecurID Token Servers

ACS 5.1 supports RSA SecurID Token Servers for authenticating users for the increased security that one-time passwords provide. RSA SecurID token servers provide two-factor authentication to ensure the authenticity of users. To authenticate users against an RSA identity store, you must first create an RSA SecurID Token Server in ACS and configure the realm, ACS instance, and advanced settings.

ACS 5.1 supports only one RSA realm. You can configure the settings for the RSA realm. A single realm can contain many ACS instances.

Note You must obtain the *sdconf.rec* file from the RSA SecurID server administrator and store it in ACS.

To create or edit an RSA SecurID token server:

Step 1 Select **Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers**.

The RSA SecurID Token Servers page appears.

Step 2 Click **Create**. You can also click the identity store name that you want to modify, or check the box next to the name and click **Edit**.

Step 3 Complete the fields in the RSA Realm Settings tab as described in Table 8-12.

Table 8-12 RSA Realm Settings Tab

Option	Description
General	
Name	Name of the RSA realm.
Description	(Optional) The description of the RSA realm.
Server Connection	
Server Timeout *n* seconds	ACS waits for *n* seconds to connect to the RSA SecurID token server before timing out.
Reauthenticate on Change PIN	Check this check box to reauthenticate on change PIN.
Realm Configuration File	
Import new 'sdconf.rec' file	Click **Browse** to select the *sdconf.rec* file from your machine.

Step 4 Click the ACS Instance Settings tab. See Configuring ACS Instance Settings, page 8-50 for more information.

Step 5 Click the Advanced tab. See Configuring Advanced Options, page 8-52 for more information.

Step 6 Click **Submit** to create an RSA SecurID store.

The RSA SecurID Token Server page appears with the configured servers.

When you first setup the RSA server you will get a message stating that ACS needs to generate a valid RSA key. On the ACS server you will see the following threads to the RSA server.

```
41 : 10.209.2.166 <166>Jun 29 2010 11:59:58: %ASA-6-302015: Built outbound
UDP connection 180194049 for corporate:10.10.10.1/5500 (10.10.10.1/5500)
to server:x.x.x.x/32781 (x.x.x.x/32781)  ----(rsa server)
```

Note Primary ACS server will obtain a Node Secret from an RSA server after first successful RSA authentication is performed via the primary ACS server. Secondary ACS server will obtain a Node Secret from an RSA server after first successful RSA authentication is performed via the secondary ACS server.

Related Topics:

- RSA SecurID Server, page 8-47
- Configuring ACS Instance Settings, page 8-50
- Configuring Advanced Options, page 8-52

Configuring ACS Instance Settings

The ACS Instance Settings tab appears with the current list of ACS instances that are active in the system. You cannot add or delete these entries. However, you can edit the available RSA Realm settings for each of these ACS instances.

.Table 8-13 describes the fields in the ACS Instance Settings tab.

Table 8-13 ACS Instance Settings Tab

Option	Description
ACS Instance	Name of the ACS instance.
Options File	Name of the options file.
securid Backup Status	Status of SecurID backup. This can be one of the following: • Cached • Not cached

You can edit the settings of the ACS instances that are listed on this page. To do this:

Step 1 Check the check box next to the ACS instance that you want to edit and click **Edit**.

The ACS instance settings dialog box appears. This dialog box contains the following tabs:

- RSA Options File—See Editing ACS Instance Settings, page 8-51 for more information.
- Reset Agents Files—See Editing ACS Instance Settings, page 8-51 for more information.

Step 2 Click **OK.**

Related Topics

- RSA SecurID Server, page 8-47
- Creating and Editing RSA SecurID Token Servers, page 8-49

- Editing ACS Instance Settings, page 8-51
- Editing ACS Instance Settings, page 8-51
- Configuring Advanced Options, page 8-52

Editing ACS Instance Settings

You can edit the ACS instance settings to:

- Enable the RSA options file, page 8-51
- Reset Agent Files, page 8-52

Enable the RSA options file

You can enable the RSA options file (*sdopts.rec*) on each ACS instance to control routing priorities for connections between the RSA agent and the RSA servers in the realm.

Table 8-14 describes the fields in the RSA Options File tab.

Table 8-14 RSA Options File Tab

Option	Description
The RSA options file (sdopts.rec) may be enabled on each ACS instance to control the routing priorities for connections between the RSA agent and the RSA servers in the realm. For detailed description of the format of the sdopts.rec, please refer to the RSA Documentation.	
Use the Automatic Load Balancing status maintained by the RSA Agent	Choose this option to use the automatic load balancing status that the RSA agent maintains.
Override the Automatic Load Balancing status with the sdopts.rec file selected below	Choose this option to use the automatic load balancing status that is specified in the sdopts.rec file.
Current File	Lists the sdopts.rec file that is chosen currently.
Timestamp	The time when sdopts.rec file was last modified.
File Size	The size of the sdopts.rec file.
Import new 'sdopts.rec' file	Click Browse to import the new sdopts.rec file from your hard drive.
Note Changes will not take effect until the page which launched this popup is submitted.	

Do one of the following:

- Click **OK** to save the configuration.
- Click the Reset Agent Files tab to reset the secret key information or the status of active and inactive servers in the realm.

Related Topics

- RSA SecurID Server, page 8-47
- Creating and Editing RSA SecurID Token Servers, page 8-49
- Configuring ACS Instance Settings, page 8-50
- Editing ACS Instance Settings, page 8-51
- Configuring Advanced Options, page 8-52

Reset Agent Files

Use this page to reset the following:

- Node Secret key file, to ensure that communication with the RSA servers is encrypted.
- Status of the servers in the realm.

Step 1 Choose either of the following options:

- To reset node secret on the agent host, check the **Remove securid file on submit** check box.

Note If you reset the node secret on the agent host, you must reset the agent host's node secret in the RSA server.

- To reset the status of servers in the realm, check the **Remove sdstatus.12 file on submit** check box.

Step 2 Click **OK**.

Related Topics

- RSA SecurID Server, page 8-47
- Creating and Editing RSA SecurID Token Servers, page 8-49
- Configuring ACS Instance Settings, page 8-50
- Editing ACS Instance Settings, page 8-51
- Configuring Advanced Options, page 8-52

Configuring Advanced Options

Use this page to do the following:

- Define what an access reject from an RSA SecurID token server means to you.
- Enable identity caching—Caching users in RSA is similar to caching users in Radius Token with the logic and the purpose of the caching being the same. The only difference is that in RSA there is no attribute retrieval for users and therefore no caching of attributes. The user who is authenticated is cached, but without any attributes.

To configure advanced options for the RSA realm:

Step 1 Do one of the following:

- Click the Treat Rejects as 'authentication failed' radio button—For ACS to interpret an authentication reject from an RSA SecurdID store as an authentication failure.
- Click the Treat Rejects as 'user not found' radio button—For ACS to interpret an authentication reject from an RSA SecurID store as "user not found."

Step 2 Enable identity caching to allow ACS to process requests that are not authenticated through the RSA server. The results obtained from the last successful authentication are available in the cache for the specified time period.

Step 3 Check the **Enable identity caching** check box.

Step 4 Enter the aging time in minutes. The identity cache stores the results of a successful login only for the time period specified here.

Step 5 Click **Submit**.

Related Topics

- RSA SecurID Server, page 8-47
- Creating and Editing RSA SecurID Token Servers, page 8-49
- Configuring ACS Instance Settings, page 8-50
- Editing ACS Instance Settings, page 8-51
- Editing ACS Instance Settings, page 8-51

RADIUS Identity Stores

Note RADIUS server is a third-party server that supports the RADIUS interface. RADIUS identity store, which is part of ACS, connects to the RADIUS server.

RADIUS servers are servers that come with a standard RADIUS interface built into them and other servers that support the RADUIS interface. ACS 5.1 supports any RADIUS RFC 2865-compliant server as an external identity store. ACS 5.1 supports multiple RADIUS token server identities; for example, the RSA SecurID server and SafeWord server. RADIUS identity stores can work with any RADIUS Token server that is used to authenticate the user. RADIUS identity stores use the UDP port for authentication sessions. The same UDP port is used for all RADIUS communication.

Note For ACS to successfully send RADIUS messages to a RADIUS-enabled server, you must ensure that the gateway devices between the RADIUS-enabled server and ACS allow communication over the UDP port. You can configure the UDP port through the ACS web interface.

This section contains the following topics:

- Supported Authentication Protocols, page 8-53
- Failover, page 8-54
- Password Prompt, page 8-54
- User Group Mapping, page 8-54
- Groups and Attributes Mapping, page 8-54
- RADIUS Identity Store in Identity Sequence, page 8-55
- Authentication Failure Messages, page 8-55
- Username Special Format with Safeword Server, page 8-55
- User Attribute Cache, page 8-56
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-56

Supported Authentication Protocols

ACS supports the following authentication protocols for RADIUS identity stores:

- RADIUS PAP
- TACACS+ ASCII/PAP
- PEAP with inner EAP-GTC
- EAP-FAST with inner EAP-GTC

Failover

ACS 5.1 allows you to configure multiple RADIUS identity stores. Each RADIUS identity store can have primary and secondary RADIUS servers. When ACS is unable to connect to the primary server, it uses the secondary server.

Password Prompt

RADIUS identity stores allow you to configure the password prompt. You can configure the password prompt through the ACS web interface.

User Group Mapping

To provide the per-user group mapping feature available in ACS 4.x, ACS 5.1 uses the attribute retrieval and authorization mechanism for users that are authenticated with a RADIUS identity store. For this, you must configure the RADIUS identity store to return authentication responses that contain the [009\001] cisco-av-pair attribute with the following value: ACS:CiscoSecure-Group-Id=*N*, where *N* can be any ACS group number from 0 through 499 that ACS assigns to the user. Then, this attribute is available in the policy configuration pages of the ACS web interface while creating authorization and group mapping rules.

Groups and Attributes Mapping

You can use the RADIUS attributes retrieved during authentication against the RADIUS identity store in ACS policy conditions for authorization and group mapping. You can select the attributes that you want to use in policy conditions while configuring the RADIUS identity store. These attributes are kept in the RADIUS identity store dedicated dictionary and can be used to define policy conditions.

Note You cannot query the RADIUS server for the requested attributes. You can only configure the RADIUS identity store to return the requested attributes. These attributes are available in the Access-Accept response as part of the attributes list.

You can use the attribute subscription feature of ACS 5.1 to receive RADIUS identity store attributes can on the ACS response to the device. The following RADIUS attributes are returned:

- Attributes that are listed in the RADIUS RFS
- Vendor-specific attributes

The following attribute types are supported:

- String
- Unsigned Integer
- IPv4 Address
- Enumeration

Note If an attribute with multiple values is returned, the value is ignored, and if a default value has been configured, that value is returned. However, this attribute is reported in the customer log as a problematic attribute.

RADIUS Identity Store in Identity Sequence

You can add the RADIUS identity store for authentication sequence in an identity sequence. However, you cannot add the RADIUS identity store for attribute retrieval sequence because you cannot query the RADIUS identity store without authentication. ACS cannot distinguish between different error cases while authenticating with a RADIUS server. RADIUS servers return an Access-Reject message for all error cases. For example, when a user is not found in the RADIUS server, instead of returning a User Unknown status, the RADIUS server returns an Access-Reject message. You can, however, enable the Treat Rejects as Authentication Failure or User Not Found option available in the RADIUS identity store pages of the ACS web interface.

Authentication Failure Messages

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. ACS provides you the option to configure this message through the ACS web interface as either Authentication Failed or Unknown User. However, this option returns an Unknown User message not only for cases where the user is not known, but for all failure cases.

Table 8-15 lists the different failure cases that are possible with RADIUS identity servers.

Table 8-15 Error Handling

Cause of Authentication Failure	Failure Cases
Authentication Failed	• User is unknown. • User attempts to login with wrong passcode. • User logon hours expired.
Process Failed	• RADIUS server is configured incorrectly in ACS. • RADIUS server is unavailable. • RADIUS packet is detected as malformed. • Problem during sending or receiving a packet from the RADIUS server. • Timeout.
Unknown User	Authentication failed and the 'Fail on Reject' option is set to false.

Username Special Format with Safeword Server

Safeword token server supports authentication with the following username format:

Username—Username, OTP

ACS parses the username and converts this to:

Username—Username

Safeword token servers support both the formats. ACS works with various token servers. While configuring a Safeword server, you must check the Safeword Server check box for ACS to parse the username and convert it to the specified format. This conversion is done in the RADIUS token server identity store before the request is sent to the RADIUS token server.

User Attribute Cache

RADIUS token servers, by default, do not support user lookups. However, the user lookup functionality is essential for the following ACS features:

- PEAP session resume—Happens after successful authentication during EAP session establishment
- EAP/FAST fast reconnect—Happens after successful authentication during EAP session establishment
- T+ Authorization—Happens after successful T+ Authentication

ACS 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 ACS nodes in a distributed deployment. You can configure the time to live (TTL) limit for the cache through the ACS web interface. You must enable the identity caching option and set the aging time in minutes. The cache is available in the memory for the specified amount of time.

Creating, Duplicating, and Editing RADIUS Identity Servers

ACS 5.1 supports the RADIUS identity server as an external identity store for the increased security that one-time passwords provide. RADIUS identity servers provide two-factor authentication to ensure the authenticity of the users. To authenticate users against a RADIUS identity store, you must first create the RADIUS identity server in ACS and configure the settings for the RADIUS identity store. ACS 5.1 supports the following authentication protocols:

- RADIUS PAP
- TACACS+ ASCII\PAP
- PEAP with inner EAP-GTC
- EAP-FAST with inner EAP-GTC

For a successful authentication with a RADIUS identity server, ensure that:

- The gateway devices between the RADIUS identity server and ACS allow communication over the UDP port.
- The shared secret that you configure for the RADIUS identity server on the ACS web interface is identical to the shared secret configured on the RADIUS identity server.

To create, duplicate, or edit a RADIUS Identity Server:

Step 1 Choose **Users and Identity Stores > External Identity Stores > RADIUS Identity Servers**.

The RADIUS Identity Servers page appears with a list of RADIUS external identity servers.

Step 2 Click **Create**. You can also:

- Check the check box next to the identity store you want to duplicate, then click **Duplicate**.
- Click the identity store name that you want to modify, or check the box next to the name and click **Edit**.

Step 3 Complete the fields in the General tab. See Configuring General Settings, page 8-57 for a description of the fields in the General tab.

Step 4 You can:

- Click **Submit** to save the RADIUS Identity Server.
- Click the Shell Prompts tab. See Configuring Shell Prompts, page 8-59 for a description of the fields in the Shell Prompts tab.
- Click the Directory Attributes tab. See Configuring Directory Attributes, page 8-59 for a description of the fields in the Directory Attributes tab.
- Click the Advanced tab. See Configuring Advanced Options, page 8-60 for a description of the fields in the Advanced tab.

Step 5 Click **Submit** to save the changes.

Related Topics

- RADIUS Identity Stores, page 8-53
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-56

Configuring General Settings

Table 8-16 describes the fields in the General tab of the RADIUS Identity Servers page.

Table 8-16 RADIUS Identity Server - General Tab

Option	Description
Name	Name of the external RADIUS identity server.
Description	(Optional) A brief description of the RADIUS identity server.
SafeWord Server	Check this check box to enable a two-factor authentication using a SafeWord server.
Server Connection	
Enable Secondary Server	Check this check box to use a secondary RADIUS identity server as a backup server in case the primary RADIUS identity server fails. If you enable the secondary server, you must configure the parameters for the secondary RADIUS identity server and must choose one of the following options: • Always Access Primary Server First—Select this option to ensure that ACS always accesses the primary RADIUS identity server first before the secondary server is accessed. • Failback To Primary Server After *n* Minutes—Select this option to set the number of minutes ACS can use the secondary server for authentication. After this time expires, ACS should again attempt to authenticate using the primary server. The default value is 5 minutes.
Primary Server	

Table 8-16 RADIUS Identity Server - General Tab (continued)

Option	Description
Server IP Address	IP address of the primary RADIUS identity server.
Shared Secret	The shared secret between ACS and the primary RADIUS identity server. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Authentication Port	Port number on which the RADIUS primary server listens. Valid options are from 1 to 65,535. The default value is 1812.
Server Timeout *n* Seconds	The number of seconds, *n*, that ACS waits for a response from the primary RADIUS identity server before it determines that the connection to the primary server has failed. Valid options are from 1 to 300. The default value is 5.
Connection Attempts	Specifies the number of times that ACS should attempt to reconnect before contacting the secondary RADIUS identity server or dropping the connection if no secondary server is configured. Valid options are from 1 to 10. The default value is 3.
Secondary Server	
Server IP Address	IP address of the secondary RADIUS identity server.
Shared Secret	The shared secret between ACS and the secondary RADIUS identity server. The shared secret must be identical to the shared secret that is configured on the RADIUS identity server. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
Authentication Port	Port number on which the RADIUS secondary server listens. Valid options are from 1 to 65,535. The default value is 1812.
Server Timeout *n* Seconds	The number of seconds, *n*, that ACS waits for a response from the secondary RADIUS identity server before it determines that the connection to the secondary server has failed. Valid options are from 1 to 300. The default value is 5.
Connection Attempts	Specifies the number of times that ACS should attempt to reconnect before dropping the request. Valid options are from 1 to 10. The default value is 3.

Related Topics

- RADIUS Identity Stores, page 8-53
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-56
- Configuring Shell Prompts, page 8-59
- Configuring Directory Attributes, page 8-59
- Configuring Advanced Options, page 8-60

Configuring Shell Prompts

For TACACS+ ASCII authentication, ACS must return the password prompt to the user. RADIUS identity server supports this functionality by the password prompt option. ACS can use the prompt that you configure in the Shell Prompts page on the ACS web interface. If the prompt is empty, the user receives the default prompt that is configured under TACACS+ global settings.

When establishing a connection with a RADIUS identity server, the initial request packets may not have the password. You must request a password. You can use this page to define the prompt that is used to request the password. To do this:

Step 1 Enter the text for the prompt in the Prompt field.

Step 2 Do one of the following:

- Click **Submit** to configure the prompt for requesting the password.
- Click the Directory Attributes tab to define a list of attributes that you want to use in policy rule conditions. See Configuring Directory Attributes, page 8-59 for more information.

Related Topics

- RADIUS Identity Stores, page 8-53
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-56
- Configuring General Settings, page 8-57
- Configuring Directory Attributes, page 8-59
- Configuring Advanced Options, page 8-60

Configuring Directory Attributes

When a RADIUS identity server responds to a request, RADIUS attributes are returned along with the response. You can make use of these RADIUS attributes in policy rules. In the Directory Attributes tab, you can specify the RADIUS attributes that you use in policy rule conditions. ACS maintains a separate list of these attributes.

Step 1 Modify the fields in the Directory Attributes tab as described in Table 8-17.

Table 8-17 RADIUS Identity Servers - Directory Attributes Tab

Option	Description
Attribute List	Use this section to create the attracted list to include in policy conditions. As you include each attribute, its name, type, default value, and policy condition name appear in the table. To: • Add a RADIUS attribute, fill in the fields below the table and click **Add**. • Edit a RADIUS attribute, select the appropriate row in the table and click **Edit**. The RADIUS attribute parameters appear in the fields below the table. Edit as required, then click **Replace**.
Dictionary Type	RADIUS dictionary type. Click the drop-down list box to select a RADIUS dictionary type.

Table 8-17 RADIUS Identity Servers - Directory Attributes Tab

Option	Description
RADIUS Attribute	Name of the RADIUS attribute. Click **Select** to choose the RADIUS attribute. This name is composed of two parts: The attribute name and an extension to support AV-pairs if the attribute selected is a Cisco AV-Pair. For example, for an attribute, **cisco-av-pair** with an AV-pair name **some-avpair**, ACS displays **cisco-av-pair.some-avpair**. **Note** IETF and vendor VSA attribute names contain an optional suffix, *-nnn*, where *nnn* is the ID of the attribute.
Type	RADIUS attribute type. Valid options are: • String • Unsigned Integer 32 • IPv4 Address
Default	(Optional) A default value that can be used if the attribute is not available in the response from the RADIUS identity server. This value must be of the specified RADIUS attribute type.
Policy Condition Name	Specify the name of the custom policy condition that uses this attribute.

Step 2 Do one of the following:

- Click **Submit** to save your changes and return to the RADIUS Identity Servers page.
- Click the Advanced tab to configure failure message handling and to enable identity caching. See Configuring Advanced Options, page 8-60 for more information.

Related Topics

- RADIUS Identity Stores, page 8-53
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-56
- Configuring General Settings, page 8-57
- Configuring Shell Prompts, page 8-59
- Configuring Advanced Options, page 8-60

Configuring Advanced Options

In the Advanced tab, you can do the following:

- Define what an access reject from a RADIUS identity server means to you.
- Enable identity caching.

Table 8-18 describes the fields in the Advanced tab of the RADIUS Identity Servers page.

Table 8-18 RADIUS Identity Server - Advanced Tab

Option	Description
This Identity Store does not differentiate between 'authentication failed' and 'user not found' when an authentication attempt is rejected. From the options below, select how such an authentication reject from the Identity Store should be interpreted by ACS for Identity Policy processing and reporting.	
Treat Rejects as 'authentication failed'	Click this option to consider all ambiguous access reject attempts as failed authentications.
Treat Rejects as 'user not found'	Click this option to consider all ambiguous access reject attempts as unknown users.
Identity caching is used to allow processing of requests that do not perform authentication against the server. The cache retains the results and attributes retrieved from the last successful authentication for the subject.	
Enable identity caching	Check this check box to enable identity caching. If you enable identity caching, you must enter the time in minutes for which you want ACS to retain the identity cache.
Aging Time *n* Minutes	Enter the time in minutes for which you want ACS to retain the identity cache. Valid options are from 1 to 1440.

Click **Submit** to save the RADIUS Identity Server.

Related Topics

- RADIUS Identity Stores, page 8-53
- Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-56

Configuring CA Certificates

When a client uses the EAP-TLS protocol to authenticate itself against the ACS server, it sends a client certificate that identifies itself to the server. To verify the identity and correctness of the client certificate, the server must have a preinstalled certificate from the Certificate Authority (CA) that has digitally signed the client certificate. If ACS does not trust the client's CA certificate, then you must install in ACS the entire chain of successively signed CA certificates, all the way to the top-level CA certificate that ACS trusts. CA certificates are also known as trust certificates.

You use the CA options to install digital certificates to support EAP-TLS authentication. ACS uses the X.509 v3 digital certificate standard. ACS also supports manual certificate acquisition and provides the means for managing a certificate trust list (CTL) and certificate revocation lists (CRLs).

Digital certificates do not require the sharing of secrets or stored database credentials. They can be scaled and trusted over large deployments. If managed properly, they can serve as a method of authentication that is stronger and more secure than shared secret systems. Mutual trust requires that ACS have an installed certificate that can be verified by end-user clients. This server certificate may be issued from a CA or, if you choose, may be a self-signed certificate. For more information, see Configuring Local Server Certificates, page 18-14.

Note ACS builds a certificate chain with the CA certificates that you add to it and uses this chain during TLS negotiations. You must add the certificate that signed the server certificate to the CA. You must ensure that the chain is signed correctly and that all the certificates are valid.

If the server certificate and the CA that signed the server certificate are installed on ACS, ACS sends the full certificate chain to the client.

Related Topics

- Adding a Certificate Authority, page 8-62
- Editing a Certificate Authority and Configuring Certificate Revocation Lists, page 8-63
- Deleting a Certificate Authority, page 8-65
- Exporting a Certificate Authority, page 8-65

Adding a Certificate Authority

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Note The supported certificate formats are either DER or PEM.

To add a trusted CA (Certificate Authority) certificate:

Step 1 Select **Users and Identity Stores > Certificate Authorities**.

The Trust Certificate page appears.

Step 2 Click **Add**.

Step 3 Complete the fields in the Certificate File to Import page as described in Table 8-19:

Table 8-19 Certificate Authority Properties Page

Option	Description
Certificate File to Import	
Certificate File	Enter the name of the certificate file. Click **Browse** to navigate to the location on the client machine where the trust certificate is located.
Trust for client with EAP-TLS	Check this box so that ACS will use the certificate trust list for the EAP protocol.
Description	Enter a description of the CA certificate.

Step 4 Click **Submit**.

The new certificate is saved. The Trust Certificate List page appears with the new certificate.

Related Topics

- User Certificate Authentication, page B-6
- Overview of EAP-TLS, page B-6

Editing a Certificate Authority and Configuring Certificate Revocation Lists

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Use this page to edit a trusted CA (Certificate Authority) certificate.

Step 1 Select **Users and Identity Stores > Certificate Authorities.**

The Trust Certificate page appears with a list of configured certificates.

Step 2 Click the name that you want to modify, or check the check box for the Name, and click **Edit**.

Step 3 Complete the fields in the Edit Trust Certificate List Properties Page as described in Table 8-20:

Table 8-20 Edit Certificate Authority Properties Page

Option	Description
Issuer	
Friendly Name	The name that is associated with the certificate.
Description	(Optional) A brief description of the CA certificate.
Issued To	*Display only.* The entity to which the certificate is issued. The name that appears is from the certificate subject.
Issued By	*Display only.* The certification authority that issued the certificate.
Valid from	*Display only.* The start date of the certificate's validity. An X509 certificate is valid only from the start date to the end date (inclusive).
Valid To (Expiration)	*Display only.* The last date of the certificate's validity.
Serial Number	*Display only.* The serial number of the certificate.
Description	Description of the certificate.
Usage	
Trust for client with EAP-TLS	Check this box so that ACS will use the trust list for the TLS related EAP protocols.
Certificate Revocation List Configuration	Use this section to configure the CRL.
Download CRL	Check this box to download the CRL.
CRL Distribution URL	Enter the CRL distribution URL. You can specify a URL that uses HTTP.
Retrieve CRL	ACS attempts to download a CRL from the CA. Toggle the time settings for ACS to retrieve a new CRL from the CA. • Automatically —Obtain the next update time from the CRL file. If unsuccessful, ACS tries to retrieve the CRL periodically after the first failure until it succeeds. • Every—Determines the frequency between retrieval attempts. Enter the amount in units of time.
If Download Failed Wait	Enter the amount of time to attempt to retrieve the CRL, if the retrieval initially failed.
Bypass CRL Verification if CRL is not Received	If unchecked, all the client requests that use the certificate that is signed by the selected CA will be rejected until ACS receives the CRL file. When checked, the client request may be accepted before the CRL is received.
Ignore CRL Expiration	Check this box to check a certificate against an outdated CRL. When checked, ACS continues to use the expired CRL and permits or rejects EAP-TLS authentications according to the contents of the CRL. When unchecked, ACS examines the expiration date of the CRL in the Next Update field in the CRL file. If the CRL has expired, all authentications that use the certificate that is signed by the selected CA are rejected.

Step 4 Click **Submit**.

The Trust Certificate page appears with the edited certificate.

Related Topics

- User Certificate Authentication, page B-6
- Overview of EAP-TLS, page B-6

Deleting a Certificate Authority

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Use this page to delete a trusted CA (Certificate Authority) certificate:

Step 1 Select **Users and Identity Stores > Certificate Authorities**.

The Trust Certificate List page appears with a list of configured certificates.

Step 2 Check one or more check boxes next to the certificates that you want to delete.

Step 3 Click **Delete**.

Step 4 For confirmation, click **Yes**.

The Trust Certificate page appears without the deleted certificate(s).

Related Topic

- Overview of EAP-TLS, page B-6

Exporting a Certificate Authority

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To export a trust certificate:

Step 1 Select **Users and Identity Stores > Certificate Authorities**.

The Trust Certificate List page appears with a list of configured certificates.

Step 2 Check the box next to the certificates that you want to export.

Step 3 Click **Export**.

This operation exports the trusted certificate to the client machine.

Step 4 For confirmation, click **Yes**.

You are prompted to install the exported certificate on your client machine.

Related Topics

- User Certificate Authentication, page B-6
- Overview of EAP-TLS, page B-6

Configuring Certificate Authentication Profiles

The certificate authentication profile defines the X509 certificate information to be used for a certificate-based access request. You can select an attribute from the certificate to be used as the username. You can select a subset of the certificate attributes to populate the username field for the context of the request. The username is then used to identify the user for the remainder of the request, including the identification used in the logs.

You can use the certificate authentication profile to retrieve certificate data to further validate a certificate presented by an LDAP or AD client. The username from the certificate authentication profile is used to query the LDAP or AD identity store. ACS compares the client certificate against all certificates retrieved from the LDAP or AD identity store, one after another, to see if one of them matches. ACS either accepts or rejects the request.

Note For ACS to accept a request, only one certificate from either the LDAP or the AD identity store must match the client certificate.

When ACS processes a certificate-based request for authentication, one of two things happens: the username from the certificate is compared to the username in ACS that is processing the request, or ACS uses the information that is defined in the selected LDAP or AD identity store to validate the certificate information.

You can duplicate a certificate authentication profile to create a new profile that is the same, or similar to, an existing certificate authentication profile. After duplication is complete, you access each profile (original and duplicated) separately, to edit or delete them.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a certificate authentication profile:

Step 1 Select **Users and Identity Stores > Certificate Authentication Profile**.

The Certificate Authentication Profile page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the certificate authentication profile that you want to duplicate, then click **Duplicate**.

- Click the certificate authentication profile that you want to modify, or check the check box next to the name and click **Edit**.

The Certificate Authentication Profile Properties page appears.

Step 3 Complete the fields in the Certificate Authentication Profile Properties page as described in Table 8-21:

Table 8-21 Certificate Authentication Profile Properties Page

Option	Description
General	
Name	Enter the name of the certificate authentication profile.
Description	Enter a description of the certificate authentication profile.
Certificate Definition	
Principal Username X509 Attribute	The available set of principal username attributes for x509 authentication. The selection includes: • Common Name • Subject Alternative Name • Subject Serial Number • Subject • Subject Alternative Name - Other Name • Subject Alternative Name - EMail • Subject Alternative Name - DNS
Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory	Check this check box if you want to validate certificate information for authentication against a selected LDAP or AD identity store. If you select this option, you must enter the name of the LDAP or AD identity store, or click **Select** to select the LDAP or AD identity store from the available list.

Step 4 Click **Submit.** The Certificate Authentication Profile page reappears.

Related Topics

- Viewing Identity Policies, page 10-21
- Configuring Identity Store Sequences, page 8-67
- Creating External LDAP Identity Stores, page 8-22

Configuring Identity Store Sequences

An access service identity policy determines the identity sources that ACS uses for authentication and attribute retrieval. An identity source consists of a single identity store or multiple identity methods. When you use multiple identity methods, you must first define them in an identity store sequence, and then specify the identity store sequence in the identity policy.

An identity store sequence defines the sequence that is used for authentication and attribute retrieval and an optional additional sequence to retrieve additional attributes.

Authentication Sequence

An identity store sequence can contain a definition for certificate-based authentication or password-based authentication or both. If you select to perform authentication based on a certificate, you specify a single Certificate Authentication Profile, which you have already defined in ACS; if you select to perform authentication based on a password, you can define a list of databases to be accessed in sequence. When authentication succeeds, any defined attributes within the database are retrieved. You must have defined the databases in ACS.

Attribute Retrieval Sequence

You can optionally define a list of databases from which to retrieve additional attributes. These databases can be accessed regardless of whether you use password or certificate-based authentication. When you use certificate-based authentication, ACS populates the username field from a certificate attribute and then uses the username to retrieve attributes.

ACS can retrieve attributes for a user, even when:

- The user's password is flagged for a mandatory change.
- The user's account is disabled.

Note When you perform password-based authentication, you can define the same identity database in the authentication list and the attribute retrieval list. However, if the database is used for authentication, it will not be accessed again as part of the attribute retrieval flow.

ACS authenticates a user or host in an identity store only when there is a single match for that user or host. If an external database contains multiple instances of the same user, authentication fails. Similarly, ACS retrieves attributes only when a single match for the user or host exists; otherwise, ACS skips attribute retrieval from that database.

This section contains the following topics:

- Creating, Duplicating, and Editing Identity Store Sequences, page 8-68
- Deleting Identity Store Sequences, page 8-70

Creating, Duplicating, and Editing Identity Store Sequences

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit an identity store sequence:

Step 1 Select **Users and Identity Stores > Identity Store Sequences**.

The Identity Store Sequences page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the sequence that you want to duplicate, then click **Duplicate**.
- Click the sequence name that you want to modify, or check the check box next to the name and click **Edit**.

The Identity Store Sequence Properties page appears as described in Table 8-22.

Table 8-22 Identity Store Sequence Properties Page

Option	Description
General	
Name	Enter the name of the identity store sequence.
Description	Enter a description of the identity store sequence.
Authentication Method List	
Certificate Based	Check this check box to use the certificate-based authentication method. If you choose this option, you must enter the certificate authentication profile. Click **Select** to choose the profile from a list of available profiles.
Password Based	Check this check box to use the password-based authentication method. If you choose this option, you must choose the set of identity stores that ACS will access one after another until a match is found. **Note** If you choose this option, you must select a list of identity stores in the Authentication and Attribute Retrieval Search List area for ACS to access the identity stores one after another.
Authentication and Attribute Retrieval Search List **Note** This section appears only when you check the Password Based option.	
Available	The available set of identity stores to access.
Selected	The selected set of identity stores to access in sequence until first authentication succeeds. Use the Up and Down arrows at the right of the list to define the order of access. ACS automatically retrieves attributes from identity stores that you selected for authentication. You do not need to select the same identity stores for attribute retrieval.
Additional Attribute Retrieval Search List	
Available	The available set of additional identity stores for attribute retrieval.
Selected	(Optional) The selected set of additional identity stores for attribute retrieval. Use the Up and Down arrows at the right of the list to define the order of access. ACS automatically retrieves attributes from identity stores that you selected for authentication. You do not need to select the same identity stores for attribute retrieval.
Internal User/Host Advanced Option	
If internal user/host not found or disabled then exit sequence and treat as "User Not Found"	Check this check box for ACS to treat the failed authentication as User Not Found when a match is not found.

Step 3 Click **Submit**. The Identity Store Sequences page reappears.

Related Topics

- Performing Bulk Operations for Network Resources and Users, page 7-8
- Viewing Identity Policies, page 10-21
- Managing Internal Identity Stores, page 8-4
- Managing External Identity Stores, page 8-18
- Configuring Certificate Authentication Profiles, page 8-66
- Deleting Identity Store Sequences, page 8-70

Deleting Identity Store Sequences

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To delete an identity store sequence:

Step 1 Select **Users and Identity Stores > Identity Store Sequences**.

The Identity Store Sequences page appears with a list of your configured identity store sequences.

Step 2 Check one or more check boxes next to the identity store sequences that you want to delete.

Step 3 Click **Delete**.

The following error message appears:

Are you sure you want to delete the selected item/items?

Step 4 Click **OK**.

The Identity Store Sequences page appears, without the deleted identity store sequence(s) listed.

Related Topics

- Performing Bulk Operations for Network Resources and Users, page 7-8
- Viewing Identity Policies, page 10-21
- Managing Internal Identity Stores, page 8-4
- Managing External Identity Stores, page 8-18
- Configuring Certificate Authentication Profiles, page 8-66
- Creating, Duplicating, and Editing Identity Store Sequences, page 8-68

CHAPTER 9

Managing Policy Elements

A policy defines the authentication and authorization processing of clients that attempt to access the ACS network. A client can be a user, a network device, or a user associated with a network device.

Policies are sets of rules. Rules contain policy elements, which are sets of conditions and results that are organized in rule tables. See Chapter 3, "ACS 5.x Policy Model" for more information on policy design and how it is implemented in ACS.

Before you configure your policy rules, you must create the policy elements, which are the conditions and results to use in those policies. After you create the policy elements, you can use them in policy rules. See Chapter 10, "Managing Access Policies" for more information on managing services, policies, and policy rules.

These topics contain.

- Managing Policy Conditions, page 9-1
- Managing Authorizations and Permissions, page 9-18
- Creating, Duplicating, and Editing Downloadable ACLs, page 9-32

Note When Cisco TrustSec license is installed, you can also configure Security Groups and Security Group Access Control Lists (SGACLs), which you can then use in TrustSec authorization policies. For information about configuring security groups for TrustSec, see Creating Security Groups, page 4-23.

Managing Policy Conditions

You can configure the following items as conditions in a rule table:

- Request/Protocol Attributes—ACS retrieves these attributes from the authentication request that the user issues.
- Identity Attributes—These attributes are related to the identity of the user performing a request. These attributes can be retrieved from the user definition in the internal identity store or from user definitions that are stored in external repositories, such as LDAP and AD.
- Identity Groups—ACS maintains a single identity group hierarchy that is used for all types of users and hosts. Each internal user or host definition can include an association to a single identity group within the hierarchy. You can map users and hosts to identity groups by using the group mapping policy. You can include identity groups in conditions to configure common policy conditions for all users in the group. For more information about creating identity groups, see Managing Identity Attributes, page 8-7.

- Network Device Groups (NDGs)—Devices issuing requests are included in one or more of up to 12 device hierarchies. You can include hierarchy elements in policy conditions. For more information about creating NDGs, see Network Device Groups, page 7-1.
- Date and Time Conditions—You can create named conditions that define specific time intervals across specific days of the week. You can also associate expiry dates with date and time conditions.

  A date and time condition is a condition that takes the current date and time and effectively returns either true or false to indicate whether or not the condition is met. There are two components within the date and time condition:

  - Enable Duration—You have the option to limit the duration during which the condition is enabled by specifying an optional start time, end time, or both. This component allows creation of rules with limited time durations that effectively expire. If the condition is not enabled, then this component of the date and time condition returns false.
  - Time Intervals—On the ACS web interface, you see a grid of time that shows the days of the week and the hours within each day. Each cell in the grid represents one hour. You can either set or clear the cells. If the date and time when a request is processed falls at a time when the corresponding time interval is set, then this component of the date and time condition returns true.

  Both components of the date and time condition are considered while processing a request. The date and time condition is evaluated as true only if both components return a true value.
- Network Conditions—You can create filters of the following types to restrict access to the network:
  - End Station Filters—Based on end stations that initiate and terminate the connection. End stations may be identified by IP address, MAC address, calling line identification (CLI), or dialed number identification service (DNIS) fields obtained from the request.
  - Network Device Filters—Based on the AAA client that processes the request. A network device can be identified by its IP address, by the device name that is defined in the network device repository, or by the NDG.
  - Device Port Filters—Network device definition might be supplemented by the device port that the end station is associated with.

  Each network device condition defines a list of objects that can then be included in policy conditions, resulting in a set of definitions that are matched against those presented in the request. The operator that you use in the condition can be either *match,* in which case the value presented must match at least one entry within the network condition, or *no matches,* in which case it should not match any entry in the set of objects that is present in the filter.

You can include Protocol and Identity attributes in a condition by defining them in custom conditions or in compound conditions.

You define compound conditions in the policy rule properties page and not as a separate named condition. See Configuring Compound Conditions, page 10-42.

Custom conditions and Date and Time conditions are called session conditions.

This section contains the following topics:

- Creating, Duplicating, and Editing a Date and Time Condition, page 9-3
- Creating, Duplicating, and Editing a Custom Session Condition, page 9-5
- Deleting a Session Condition, page 9-6
- Managing Network Conditions, page 9-7

See Chapter 3, “ACS 5.x Policy Model” for information about additional conditions that you can use in policy rules, although they are not configurable.

Creating, Duplicating, and Editing a Date and Time Condition

Create date and time conditions to specify time intervals and durations. For example, you can define shifts over a specific holiday period. When ACS processes a rule with a date and time condition, the condition is compared to the date and time information of the ACS instance that is processing the request. Clients that are associated with this condition are subject to it for the duration of their session.

Note The time on the ACS server is used when making policy decisions. Therefore, ensure that you configure date and time conditions that correspond to the time zone in which your ACS server resides. Your time zone may be different from that of the ACS server.

You can duplicate a session condition to create a new session condition that is the same, or similar to, an existing session condition. After duplication is complete, you access each session condition (original and duplicated) separately to edit or delete them.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a date and time condition:

Step 1 Select **Policy Elements > Session Conditions > Date and Time**.

The Date and Time Conditions page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the condition you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the condition that you want to modify and click **Edit**.

The Date and Time Properties page appears.

Step 3 Enter valid configuration data in the required fields as described in Table 9-1:

Table 9-1 Date and Time Properties Page

Option	Description
General	
Name	Enter a name for the date and time condition.
Description	Enter a description, such as specific days and times of the date and time condition.
Duration	

Table 9-1 Date and Time Properties Page (continued)

Option	Description
Start	Click one of the following options: • **Start Immediately**—Specifies that the rules associated with this condition are valid, starting at the current date. • **Start On**—Specify a start date by clicking the calendar icon next to the associated field to choose a specific start date, at which the condition becomes active (at the beginning of the day, indicated by the time 00:00:00 on a 24-hour clock). **Note** You can specify time in the *hh*:*mm* format.
End	Click one of the following options: • **No End Date**—Specifies that the rules associated with this date and time condition are always active, after the indicated start date. • **End By**—Specify an end date by clicking the calendar icon next to the associated field to choose a specific end date, at which the date and time condition becomes inactive (at the end of the day, indicated by the time 23:59:59 on a 24-hour clock) **Note** You can specify time in the *hh*:*mm* format.
Days and Time	
Days and Time section grid	Each square in the Days and Time grid is equal to one hour. Select a grid square to make the corresponding time active; rules associated with this condition are valid during this time. A green (or darkened) grid square indicates an active hour. **Note** Ensure that you configure date and time conditions that correspond to the time zone in which your ACS server resides. Your time zone may be different from that of the ACS server. For example, you may receive an error message if you configure a date and time condition that is an hour ahead of your current time, but that is already in the past with respect to the time zone of your ACS server.
Select All	Click to set all squares in the grid to the active state. Rules associated with this condition are always valid.
Clear All	Click to set all squares in the grid to the inactive state. Rules associated with this condition are always invalid.
Undo All	Click to remove your latest changes for the active and inactive day and time selections for the date and time group.

Note To add date and time conditions to a policy, you must first customize the rule table. See Customizing a Policy, page 10-5.

Step 4 Click **Submit**.

The date and time condition is saved. The Date and Time Conditions page appears with the new date and time condition that you created or duplicated.

Related Topics

- Creating, Duplicating, and Editing a Custom Session Condition, page 9-5
- Deleting a Session Condition, page 9-6
- Configuring Access Service Policies, page 10-20

Creating, Duplicating, and Editing a Custom Session Condition

The protocol and identity dictionaries contain a large number of attributes. To use any of these attributes as a condition in a policy rule, you must first create a custom condition for the attribute. In this way, you define a smaller subset of attributes to use in policy conditions, and present a smaller focused list from which to choose condition types for rule tables.

Note You can also include protocol and identity attributes within compound conditions. See Configuring Compound Conditions, page 10-42 for more information on compound conditions.

To create a custom condition, you must select a specific protocol (RADIUS or TACACS+) or identity attribute from one of the dictionaries, and name the custom condition. See Configuring Global System Options, page 18-1 for more information on protocol and identity dictionaries.

When you create a custom condition that includes identity or RADIUS attributes, you can also include the definition of the attributes. You can thus easily view any existing custom conditions associated with a particular attribute.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a custom session condition:

Step 1 Select **Policy Elements > Session Conditions > Custom**.

The Custom Conditions page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the condition you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the condition that you want to modify and click **Edit**.

The Custom Condition Properties page appears.

Step 3 Enter valid configuration data in the required fields as shown in Table 9-2:

Table 9-2 Policy Custom Condition Properties Page

Option	Description
General	
Name	Name of the custom condition.

Table 9-2 Policy Custom Condition Properties Page (continued)

Option	Description
Description	Description of the custom condition.
Condition	
Dictionary	Choose a specific protocol or identity dictionary from the drop-down list box.
Attribute	Click **Select** to display the list of external identity store dictionaries based on the selection you made in the Dictionary field. Select the attribute that you want to associate with the custom condition, then click **OK**. If you are editing a custom condition that is in use in a policy, you cannot edit the attribute that it references.

Note To add custom conditions to a policy, you must first customize the rule table. See Customizing a Policy, page 10-5.

Step 4 Click **Submit**.

The new custom session condition is saved. The Custom Condition page appears with the new custom session condition. Clients that are associated with this condition are subject to it for the duration of their session.

Related Topics

- Creating, Duplicating, and Editing a Date and Time Condition, page 9-3
- Deleting a Session Condition, page 9-6
- Configuring Access Service Policies, page 10-20

Deleting a Session Condition

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To delete a session condition:

Step 1 Select **Policy Elements** > **Session Conditions** > **<*session condition*>**, where <*session condition*> is Date and Time or Custom.

The Session Condition page appears.

Step 2 Check one or more check boxes next to the session conditions that you want to delete and click **Delete**.

The following message appears:

Are you sure you want to delete the selected item/items?

Step 3 Click **OK**.

The Session Condition page appears without the deleted custom session conditions.

Related Topics

- Creating, Duplicating, and Editing a Date and Time Condition, page 9-3
- Creating, Duplicating, and Editing a Custom Session Condition, page 9-5

Managing Network Conditions

Filters are reusable network conditions that you create for end stations, network devices, and network device ports. Filters enable ACS 5.1 to do the following:

- Decide whether or not to grant network access to users and devices.
- Decide on the identity store, service, and so on to be used in policies.

After you create a filter with a name, you can reuse this filter multiple times across various rules and policies by referring to its name.

Note The filters in ACS 5.1 are similar to the NARs in ACS 4.x. In ACS 4.x, the NARs were based on either the user or user group. In 5.1, the filters are independent conditions that you can reuse across various rules and policies.

ACS offers three types of filters:

- End Station Filter—Filters end stations, such as a laptop or printer that initiates a connection based on the end station's IP address, MAC address, CLID number, or DNIS number.

  The end station identifier can be the IP address, MAC address, or any other string that uniquely identifies the end station. It is a protocol-agnostic attribute of type string that contains a copy of the end station identifier:

  - In a RADIUS request, this identifier is available in Attribute 31 (Calling-Station-Id).
  - In a TACACS request, ACS obtains this identifier from the remote address field of the start request (of every phase). It takes the remote address value before the slash (/) separator, if it is present; otherwise, it takes the entire remote address value.

  The end station IPv4 is an IPv4 version of the end station identifier. The end station MAC is a normalized MAC address of the end station identifier.

- Device Filter—Filters a network device (AAA client) that acts as a Policy Enforcement Point (PEP) to the end station based on the network device's IP address or name, or the network device group that it belongs to.

  The device identifier can be the IP address or name of the device, or it can be based on the network device group to which the device belongs.

  The IP address is a protocol-agnostic attribute of type IPv4 that contains a copy of the device IP address obtained from the request:

  - In a RADIUS request, if Attribute 4 (NAS-IP-Address) is present, ACS obtains the IP address from Attribute 4; otherwise, if Attribute 32 (NAS-Identifier) is present, ACS obtains the IP address from Attribute 32, or it obtains the IP address from the packet that it receives.
  - In a TACACS request, the IP address is obtained from the packet that ACS receives.

The device name is an attribute of type string that contains a copy of the device name derived from the ACS repository.

The device dictionary (the NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes, in turn, contain the groups that the current device is related to.

- Device Port Filter—Filters the physical port of the device that the end station is connected to. Filtering is based on the device's IP address, name, NDG it belongs to, and port.

  The device port identifier is an attribute of type string:

  - In a RADIUS request, if Attribute 5 (NAS-Port) is present in the request, ACS obtains the value from Attribute 5; or, if Attribute 87 (NAS-Port-Id) is present in the request, ACS obtains the request from Attribute 87.
  - In a TACACS request, ACS obtains this identifier from the port field of the start request (of every phase).

  The device name is an attribute of type string that contains a copy of the device name derived from the ACS repository.

  The device dictionary (the NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes, in turn, contain the groups that the current device is related to.

You can create, duplicate, and edit these filters. You can also do a bulk import of the contents within a filter from a .csv file and export the filters from ACS to a .csv file. See Importing Network Conditions, page 9-8 for more information on how to do a bulk import of network conditions.

This section contains the following topics:

- Importing Network Conditions, page 9-8
- Exporting Network Conditions, page 9-9
- Creating, Duplicating, and Editing End Station Filters, page 9-10
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Creating, Duplicating, and Editing Device Port Filters, page 9-15

Importing Network Conditions

You can use the bulk import function to import the contents from the following network conditions:

- End station filters
- Device filters
- Device port filters

For bulk import, you must download the .csv file template from ACS, add the records that you want to import to the .csv file, and save it to your hard drive. Use the Download Template function to ensure that your .csv file adheres to the requirements. The .csv templates for end station filters, device filters, and device port filters are specific to their type; for example, you cannot use a downloaded template accessed from the End Station Filters page to import device filters or device port filters. Within the .csv file, you must adhere to these requirements:

- Do not alter the contents of the first record (the first line, or row, of the .csv file).
- Use only one line for each record.

- Do not imbed new-line characters in any fields.
- For non-English languages, encode the .csv file in utf-8 encoding, or save it with a font that supports Unicode.

Note The import process does not add filters to the existing list of filters in ACS, but instead replaces the existing list. When you import records from a .csv file, it replaces the existing filter configuration in ACS and replaces it with the filter configuration from the .csv file.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Click the **Replace from File** button on the End Station Filter, Device Filter, or Device Port Filter page of the web interface.

The Replace from File dialog box appears.

Step 2 Click **Download Template** to download the .csv file template if you do not have it.

Step 3 Click **Browse** to navigate to your .csv file.

Step 4 Click **Start Replace** to start the bulk import process.

The import progress is shown on the same page. You can monitor the bulk import progress. Data transfer failures of any records within your .csv file are displayed.

Step 5 Click **Close** to close the Import Progress window.

Note You can submit only one .csv file to the system at one time. If an import is under way, an additional import cannot succeed until the original import is complete.

Timesaver Instead of downloading the template and creating an import file, you can use the export file of the particular filter, update the information in that file, save it, and reuse it as your import file.

Exporting Network Conditions

ACS 5.1 offers you a bulk export function to export the filter configuration data in the form of a .csv file. You can export the following filter configurations:

- End Station Filters
- Device Filters
- Device Port Filters

From the create, edit, or duplicate page of any of the filters, click **Export to File** to save the filter configuration as a .csv file on your local hard drive.

Creating, Duplicating, and Editing End Station Filters

Use the End Station Filters page to create, duplicate, and edit end station filters. To do this:

Step 1 Choose **Policy Elements > Session Conditions > Network Conditions > End Station Filters**.

The End Station Filters page appears with a list of end station filters that you have configured.

Step 2 Click **Create**. You can also:

- Check the check box next to the end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the end station filter that you want to edit, then click **Edit**.
- Click **Export** to save a list of end station filters in a .csv file. For more information, see Exporting Network Conditions, page 9-9.
- Click **Replace from File** to perform a bulk import of end station filters from a .csv import file. For more information, see Importing Network Conditions, page 9-8.

Step 3 Enter the values for the following fields:

- Name—Name of the end station filter.
- Description—A description of the end station filter.

Step 4 Edit the fields in one or more of the following tabs:

- IP Address—See Defining IP Address-Based End Station Filters, page 9-10 for a description of the fields in this tab.
- MAC Address—See Defining MAC Address-Based End Station Filters, page 9-11 for a description of the fields in this tab.
- CLI/DNIS—See Defining CLI or DNIS-Based End Station Filters, page 9-12 for a description of the fields in this tab.

Note To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- Managing Network Conditions, page 9-7
- Importing Network Conditions, page 9-8
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Creating, Duplicating, and Editing Device Port Filters, page 9-15

Defining IP Address-Based End Station Filters

You can create, duplicate, and edit the IP addresses of end stations that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.

- Check the check box next to the IP-based end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the IP-based end station filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Choose either of the following:

- Single IP Address—If you choose this option, you must enter a valid IPv4 address of the format *x.x.x.x*, where *x* can be any number from 0 to 255.
- IP Range(s)—If you choose this option, you must enter a valid IPv4 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value is 32.

Step 3 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing End Station Filters, page 9-10
- Defining MAC Address-Based End Station Filters, page 9-11
- Defining CLI or DNIS-Based End Station Filters, page 9-12

Defining MAC Address-Based End Station Filters

You can create, duplicate, and edit the MAC addresses of end stations or destinations that you want to permit or deny access to. To do this:

Step 1 From the MAC Address tab, do one of the following:

- Click **Create**.
- Check the check box next to the MAC address-based end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the MAC address-based end station filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Check the **End Station MAC** check box to enter the MAC address of the end station. You can optionally set this field to ANY to refer to any MAC address.

Step 3 Check the **Destination MAC** check box to enter the MAC address of the destination machine. You can optionally set this field to ANY to refer to any MAC address.

Note You must enter the MAC address in one of the following formats: *xxxxxxxxxxxx*, *xx-xx-xx-xx-xx-xx*, *xx:xx:xx:xx:xx:xx*, or *xxxx.xxxx.xxxx*, where x can be any number from 0 to 9 or A through F. You cannot use wildcard characters for MAC address.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing End Station Filters, page 9-10
- Defining IP Address-Based End Station Filters, page 9-10
- Defining CLI or DNIS-Based End Station Filters, page 9-12

Defining CLI or DNIS-Based End Station Filters

You can create, duplicate, and edit the CLI and DNIS number of the end stations or destinations that you want to permit or deny access to. To do this:

Step 1 From the CLI/DNIS tab, do one of the following:

- Click **Create**.
- Check the check box next to the CLI or DNIS-based end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the CLI or DNIS-based end station filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Check the **CLI** check box to enter the CLI number of the end station. You can optionally set this field to ANY to refer to any CLI number.

Step 3 Check the **DNIS** check box to enter the DNIS number of the destination machine. You can optionally set this field to ANY to refer to any DNIS number.

Note You can use ? and * wildcard characters to refer to any single character or a series of one or more successive characters respectively.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing End Station Filters, page 9-10
- Defining IP Address-Based End Station Filters, page 9-10
- Defining MAC Address-Based End Station Filters, page 9-11

Creating, Duplicating, and Editing Device Filters

Use the Device Filters page to create, duplicate, and edit device filters. To do this:

Step 1 Choose **Policy Elements > Session Conditions > Network Conditions > Device Filters**.

The Device Filters page appears with a list of device filters that you have configured.

Step 2 Click **Create**. You can also:

- Check the check box next to the device filter that you want to duplicate, then click **Duplicate**.

- Check the check box next to the device filter that you want to edit, then click **Edit**.
- Click **Export** to save a list of device filters in a .csv file. For more information, see Exporting Network Conditions, page 9-9.
- Click **Replace from File** to perform a bulk import of device filters from a .csv import file. For more information, see Importing Network Conditions, page 9-8.

Step 3 Enter the values for the following fields:

- Name—Name of the device filter.
- Description—A description of the device filter.

Step 4 Edit the fields in any or all of the following tabs:

- IP Address—See Defining IP Address-Based Device Filters, page 9-13 for a description of the fields in this tab.
- Device Name—See Defining Name-Based Device Filters, page 9-14 for a description of the fields in this tab.
- Network Device Group—See Defining NDG-Based Device Filters, page 9-14 for a description of the fields in this tab.

Note To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- Managing Network Conditions, page 9-7
- Importing Network Conditions, page 9-8
- Creating, Duplicating, and Editing End Station Filters, page 9-10
- Creating, Duplicating, and Editing Device Port Filters, page 9-15

Defining IP Address-Based Device Filters

You can create, duplicate, and edit the IP addresses of network devices that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.
- Check the check box next to the IP-based device filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the IP-based device filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Choose either of the following:

- Single IP Address—If you choose this option, you must enter a valid IPv4 address of the format *x*.*x*.*x*.*x*, where *x* can be any number from 0 to 255.
- IP Range(s)—If you choose this option, you must enter a valid IPv4 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value is 32.

Step 3 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Defining Name-Based Device Filters, page 9-14
- Defining NDG-Based Device Filters, page 9-14

Defining Name-Based Device Filters

You can create, duplicate, and edit the name of the network device that you want to permit or deny access to. To do this:

Step 1 From the Device Name tab, do one of the following:

- Click **Create**.
- Check the check box next to the name-based device filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the name-based device filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Click **Select** to choose the network device that you want to filter.

Step 3 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Defining IP Address-Based Device Filters, page 9-13
- Defining NDG-Based Device Filters, page 9-14

Defining NDG-Based Device Filters

You can create, duplicate, and edit the name of the network device group type that you want to permit or deny access to. To do this:

Step 1 From the Network Device Group tab, do one of the following:

a. Click **Create**.

b. Check the check box next to the NDG-based device filter that you want to duplicate, then click **Duplicate**.

c. Check the check box next to the NDG-based device filter that you want to edit, then click **Edit**.

   A dialog box appears.

Step 2 Click **Select** to choose the network device group type that you want to filter.

Step 3 Click **Select** to choose the network device group value that you want to filter.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Defining IP Address-Based Device Filters, page 9-13
- Defining Name-Based Device Filters, page 9-14

Creating, Duplicating, and Editing Device Port Filters

Use the Device Port Filters page to create, duplicate, and edit device port filters. To do this:

Step 1 Choose **Policy Elements > Session Conditions > Network Conditions > Device Port Filters**.

The Device Port Filters page appears with a list of device port filters that you have configured.

Step 2 Click **Create**. You can also:

- Check the check box next to the device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the device port filter that you want to edit, then click **Edit**.
- Click **Export** to save a list of device port filters in a .csv file. For more information, see Exporting Network Conditions, page 9-9.
- Click **Replace from File** to perform a bulk import of device port filters from a .csv import file. For more information, see Importing Network Conditions, page 9-8.

Step 3 Enter the values for the following fields:

- Name—Name of the device port filter.
- Description—A description of the device port filter.

Step 4 Edit the fields in any or all of the following tabs:

- IP Address—See Defining IP Address-Based Device Port Filters, page 9-16 for a description of the fields in this tab.
- Device Name—See Defining NDG-Based Device Port Filters, page 9-17 for a description of the fields in this tab.
- Network Device Group—See Defining NDG-Based Device Port Filters, page 9-17 for a description of the fields in this tab.

Note To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- Managing Network Conditions, page 9-7
- Importing Network Conditions, page 9-8
- Creating, Duplicating, and Editing End Station Filters, page 9-10
- Creating, Duplicating, and Editing Device Filters, page 9-12

Defining IP Address-Based Device Port Filters

You can create, duplicate, and edit the IP addresses of the network device ports that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.
- Check the check box next to the IP-based device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the IP-based device port filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Choose either of the following:

- Single IP Address—If you choose this option, you must enter a valid IPv4 address of the format *x*.*x*.*x*.*x*, where *x* can be any number from 0 to 255.
- IP Range(s)—If you choose this option, you must enter a valid IPv4 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value is 32.

Step 3 Check the **Port** check box and enter the port number. This field is of type string and can contain numbers or characters. You can use the following wildcard characters:

- ?—match a single character
- *—match a set of characters

For example, the string "p*1*" would match any word that starts with the letter "p" and contains the number 1, such as port1, port15, and so on.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing Device Port Filters, page 9-15
- Defining Name-Based Device Port Filters, page 9-16
- Defining NDG-Based Device Port Filters, page 9-17

Defining Name-Based Device Port Filters

You can create, duplicate, and edit the name of the network device and the port to which you want to permit or deny access. To do this:

Step 1 From the Device Name tab, do one of the following:

- Click **Create**.

- Check the check box next to the name-based device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the name-based device port filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Click **Select** to choose the network device that you want to filter.

Step 3 Check the **Port** check box and enter the port number.

Step 4 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing Device Port Filters, page 9-15
- Defining IP Address-Based Device Port Filters, page 9-16
- Defining NDG-Based Device Port Filters, page 9-17

Defining NDG-Based Device Port Filters

You can create, duplicate, and edit the network device group type and the port to which you want to permit or deny access. To do this:

Step 1 From the Network Device Group tab, do one of the following:

- Click **Create**.
- Check the check box next to the NDG-based device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box next to the NDG-based device port filter that you want to edit, then click **Edit**.

  A dialog box appears.

Step 2 Click **Select** to choose the network device group type that you want to filter.

Step 3 Click **Select** to choose the network device group value that you want to filter.

Step 4 Check the **Port** check box and enter the port number.

Step 5 Click **OK**.

Related Topics

- Managing Network Conditions, page 9-7
- Creating, Duplicating, and Editing Device Filters, page 9-12
- Defining IP Address-Based Device Filters, page 9-13
- Defining Name-Based Device Filters, page 9-14

Managing Authorizations and Permissions

You define authorizations and permissions to determine the results associated with a specific policy rule.

You can define:

- Authorization profiles for network access authorization (for RADIUS).
- Shell profiles for TACACS+ shell sessions and command sets for device administration.
- Downloadable ACLs.
- Security groups and security group ACLs for Cisco TrustSec. See ACS and Cisco TrustSec, page 4-22, for information on configuring these policy elements.

These topics describe how to manage authorizations and permissions:

- Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18
- Creating and Editing Security Groups, page 9-24
- Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24
- Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-29
- Creating, Duplicating, and Editing Downloadable ACLs, page 9-32
- Deleting an Authorizations and Permissions Policy Element, page 9-33
- Configuring Security Group Access Control Lists, page 9-33

Creating, Duplicating, and Editing Authorization Profiles for Network Access

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

An authorization profile defines the set of attributes and values that the Access-Accept response returns. You can specify:

- Common data, such as VLAN information, URL for redirect, and more. This information is automatically converted to the raw RADIUS parameter information.
- RADIUS authorization parameters—You can select any RADIUS attribute and specify the corresponding value to return.

You can duplicate an authorization profile to create a new authorization profile that is the same, or similar to, an existing authorization profile. After duplication is complete, you access each authorization profile (original and duplicated) separately to edit or delete them.

After you create authorization profiles, you can use them as results in network access session authorization policies.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit an authorization profile:

Step 1 Select **Policy Elements > Authorization and Permissions > Network Access > Authorization Profile**.

The Authorization Profiles page appears with the fields described in Table 9-3:

Table 9-3 Authorization Profiles Page

Option	Description
Name	A list of existing network access authorization definitions.
Description	*Display only.* The description of the network access authorization definition.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the authorization profile that you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**.

The Authorization Profile Properties page appears.

Step 3 Enter valid configuration data in the required fields in each tab. See:

- Specifying Authorization Profiles, page 9-19
- Specifying Common Attributes in Authorization Profiles, page 9-20
- Specifying RADIUS Attributes in Authorization Profiles, page 9-22

Step 4 Click **Submit**.

The authorization profile is saved. The Authorization Profiles page appears with the authorization profile that you created or duplicated.

Specifying Authorization Profiles

Use this tab to configure the name and description for a network access authorization profile.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:

- **Create** to create a new network access authorization definition.
- **Duplicate** to duplicate a network access authorization definition.
- **Edit** to edit a network access authorization definition.

Step 2 Complete the required fields of the Authorization Profile: General page as shown in Table 9-4:

Table 9-4 Authorization Profile: General Page

Option	Description
Name	The name of the network access authorization definition.
Description	The description of the network access authorization definition.

Step 3 Click one of the following:

- **Submit** to save your changes and return to the Authorization Profiles page.
- The **Common Tasks** tab to configure common tasks for the authorization profile; see Specifying Common Attributes in Authorization Profiles, page 9-20.
- The **RADIUS Attributes** tab to configure RADIUS attributes for the authorization profile; see Specifying RADIUS Attributes in Authorization Profiles, page 9-22.

Specifying Common Attributes in Authorization Profiles

Use this tab to specify common RADIUS attributes to include in a network access authorization profile. ACS converts the specified values to the required RADIUS attribute-value pairs and displays them in the RADIUS attributes tab.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:

- **Create** to create a new network access authorization definition, then click the **Common Tasks** tab.
- **Duplicate** to duplicate a network access authorization definition, then click the **Common Tasks** tab.
- **Edit** to edit a network access authorization definition, then click the **Common Tasks** tab.

Step 2 Complete the required fields of the Authorization Profile: Common Tasks page as shown in Table 9-5:

Table 9-5 Authorization Profile: Common Tasks Page

Option	Description
ACLS	
Downloadable ACL Name	Includes a defined downloadable ACL. See Creating, Duplicating, and Editing Downloadable ACLs, page 9-32 for information about defining a downloadable ACL.
Filter-ID ACL	Includes an ACL Filter ID.
Proxy ACL	Includes a proxy ACL.
Voice VLAN	
Permission to Join	Select **Static**. A value for this parameter is displayed.
VLAN	
VLAN ID/Name	Includes a VLAN assignment.
Reauthentication	
Reauthentication Timer	Select whether to use a session timeout value. If you select **Static**, you must enter a value in the Seconds field. If you select **Dynamic**, you must select the dynamic parameters.
Maintain Connectivity during Reauthentication	Click **Yes** to ensure connectivity is maintained while reauthentication is performed. By default, **Yes** is selected. This field is enabled only if you define the Reauthentication Timer.
QoS	
Input Policy Map	Includes a QoS input policy map.
Output Policy Map	Includes a QoS output policy map.
802.1X-REV	
LinkSec Security Policy	If you select **Static**, you must select a value for the 802.1X-REV LinkSec security policy. Valid options are: • must-not-secure • should-secure • must-secure
URL Redirect When a URL is defined for Redirect an ACL must also be defined	
URL for Redirect	Includes a URL redirect.
URL Redirect ACL	Includes the name of the access control list (ACL) for URL redirection. When you define a URL redirect, you must also define an ACL for the URL redirection.

Specifying RADIUS Attributes in Authorization Profiles

Use this tab to configure which RADIUS attributes to include in the Access-Accept packet for an authorization profile. This tab also displays the RADIUS attribute parameters that you choose in the Common Tasks tab.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:

- **Create** to create a new network access authorization definition, then click the **RADIUS Attributes** tab.
- Check the check box next to the authentication profile that you want to duplicate, click **Duplicate**, and then click the **RADIUS Attributes** tab.
- Check the check box next to the authentication profile that you want to duplicate, click **Edit**, and then click the **RADIUS Attributes** tab.

Step 2 Complete the required fields of the Authorization Profile: RADIUS Attributes page as shown in Table 9-6:

Table 9-6 Authorization Profile: RADIUS Attributes Page

Option	Description
Common Tasks Attributes	Displays the names, values, and types for the attributes that you defined in the Common Tasks tab.
Manually Entered	Use this section to define RADIUS attributes to include in the authorization profile. As you define each attribute, its name, value, and type appear in the table. To: • Add a RADIUS attribute, fill in the fields below the table and click **Add**. • Edit a RADIUS attribute, select the appropriate row in the table and click **Edit**. The RADIUS parameters appear in the fields below the table. Edit as required, then click **Replace**.
Dictionary Type	Choose the dictionary that contains the RADIUS attribute you want to use.

Table 9-6 Authorization Profile: RADIUS Attributes Page (continued)

Option	Description
RADIUS Attribute	The name of the RADIUS attribute. Click **Select** to choose a RADIUS attribute from the specified dictionary. You must manually add VPN attributes to the authorization profile to authenticate VPN devices in your network. ACS can work with different Layer 2 and Layer 3 protocols, such as: • IPSec—Operates at Layer 3; no mandatory attributes need to be configured in the ACS authorization profile, but you can configure optional attributes. • L2TP—For L2TP tunneling, you must configure ACS with: – CVPN3000/ASA/PIX7.x-Tunneling Protocols—This attribute specifies the type of tunneling to be used. – CVPN3000/ASA/PIX7.x-L2TP-Encryption—This attribute, when set, enables VPN3000 to communicate to the client the type of Microsoft Point-to-Point Encryption (MPPE) key that must be used, either the MSCHAPv1 or MSCHAPv2 authentication method. • PPTP—For PPTP tunneling, you must configure ACS with: – CVPN3000/ASA/PIX7.x-Tunneling Protocols—This attribute specifies the type of tunneling to be used. – CVPN3000/ASA/PIX7.x-PPTP-Encryption—This attribute, when set, enables VPN3000 to communicate to the client the type of Microsoft Point-to-Point Encryption (MPPE) key that must be used, either the MSCHAPv1 or MSCHAPv2 authentication method.
Attribute Type	The client vendor type of the attribute, from which ACS allows access requests. For a description of the attribute types, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients.
Attribute Value	The value of the attribute. Click **Select** for a list of attribute values. For a description of the attribute values, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients. For tunneled protocols, ACS provides for attribute values with specific tags to the device within the access response according to RFC 2868. If you choose Tagged Enum or Tagged String as the RADIUS Attribute type, the Tag field appears. For the tag value, enter a number that ACS will use to group attributes belonging to the same tunnel. For the Tagged Enum attribute type: • Choose an appropriate attribute value. • Enter an appropriate tag value (0–31). For the Tagged String attribute type: • Enter an appropriate string attribute value (up to 256 characters). • Enter an appropriate tag value (0–31).

Step 3 To configure:

- Basic information of an authorization profile; see Specifying Authorization Profiles, page 9-19.
- Common tasks for an authorization profile; see Specifying Common Attributes in Authorization Profiles, page 9-20.

Creating and Editing Security Groups

Use this page to view names and details of security groups and security group tags (SGTs), and to open pages to create, duplicate, and edit security groups.

When you create a security group, ACS generates a unique SGT. Network devices can query ACS for SGT information. The network device uses the SGT to tag, or paint, packets at ingress, so that the packets can be filtered at Egress according to the Egress policy. See Egress Policy Matrix Page, page 10-47, for information on configuring an Egress policy.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Policy Elements > Authorizations and Permissions > Network Access > Security Groups**.

The Security Groups page appears as described in Table 9-7:

Table 9-7 Security Groups Page

Option	Description
Name	The name of the security group.
SGT (Dec / Hex)	Representation of the security group tag in decimal and hexadecimal format.
Description	The description of the security group.

Step 2 Click:

- **Create** to create a new security group.
- **Duplicate** to duplicate a security group.
- **Edit** to edit a security group.

Step 3 Enter the required information in the Name and Description fields, then click **Submit**.

Related Topic

- Creating Security Groups, page 4-23

Creating, Duplicating, and Editing a Shell Profile for Device Administration

You can configure Cisco IOS shell profile and command set authorization. Shell profiles and command sets are combined for authorization purposes. Shell profile authorization provides decisions for the following capabilities for the user requesting authorization and is enforced for the duration of a user's session:

- Privilege level.
- General capabilities, such as device administration and network access.

Shell profile definitions are split into two components:

- Common tasks
- Custom attributes

The Common Tasks tab allows you to select and configure the frequently used attributes for the profile. The attributes that are included here are those defined by the TACACS protocol draft specification that are specifically relevant to the shell service. However, the values can be used in the authorization of requests from other services.

The Custom Attributes tab allows you to configure additional attributes. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. Custom attributes can be defined for nonshell services.

For a description of the attributes that you specify in shell profiles, see Cisco IOS documentation for the specific release of Cisco IOS software that is running on your AAA clients.

After you create shell profiles and command sets, you can use them in authorization and permissions within rule tables.

You can duplicate a shell profile if you want to create a new shell profile that is the same, or similar to, an existing shell profile.

After duplication is complete, you access each shell profile (original and duplicated) separately to edit or delete them.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a shell profile:

Step 1 Select **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**.

The Shell Profiles page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the shell profile that you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**.

The Shell Profile Properties page General tab appears.

Step 3 Enter valid configuration data in the required fields in each tab. As a minimum configuration, you must enter a unique name for the shell profile; all other fields are optional. See:

- Defining General Shell Profile Properties, page 9-26
- Defining Common Tasks, page 9-27
- Defining Custom Attributes, page 9-28

Step 4 Click **Submit**.

The shell profile is saved. The Shell Profiles page appears with the shell profile that you created or duplicated.

Related Topics

- Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18
- Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-29
- Deleting an Authorizations and Permissions Policy Element, page 9-33
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Defining General Shell Profile Properties

Use this page to define a shell profile's general properties.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, then do one of the following:

- Click **Create**.
- Check the check box next to the shell profile that you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**.

Step 2 Complete the Shell Profile: General fields as described in Table 9-8:

Table 9-8 Shell Profile: General Page

Option	Description
Name	The name of the shell profile.
Description	(Optional) The description of the shell profile.

Step 3 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **Common Tasks** tab to configure privilege levels for the authorization profile; see Defining Common Tasks, page 9-27.
- The **Custom Attributes** tab to configure RADIUS attributes for the authorization profile; see Defining Custom Attributes, page 9-28.

Related Topics

- Defining Common Tasks, page 9-27

- Defining Custom Attributes, page 9-28

Defining Common Tasks

Use this page to define a shell profile's privilege level and attributes. The attributes are defined by the TACACS+ protocol.

For a description of the attributes, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, then click:

- **Create** to create a new shell profile, then click **Common Tasks**.
- **Duplicate** to duplicate a shell profile, then click **Common Tasks**.
- **Edit** to edit a shell profile, then click **Common Tasks**.

Step 2 Complete the Shell Profile: Common Tasks page as described in Table 9-9:

Table 9-9 Shell Profile: Common Tasks

Option	Description
Privilege Level	
Default Privilege	(Optional) Enables the initial privilege level assignment that you allow for a client, through shell authorization. If disabled, the setting is not interpreted in authorization and permissions.
	The **Default Privilege Level** specifies the default (initial) privilege level for the shell profile. If you select the Enable Default Privilege option, you can select the default privilege level; the valid options are 0 to 15.
Maximum Privilege	(Optional) Enables the maximum privilege level assignment for which you allow a client after the initial shell authorization.
	The **Maximum Privilege Level** specifies the maximum privilege level for the shell profile. If you select the Enable Change of Privilege Level option, you can select the maximum privilege level; the valid options are 0 to 15. **Note** If you choose both default and privilege level assignments, the default privilege level assignment must be equal to or lower than the maximum privilege level assignment.
Shell Attributes	
Note Choose Not in Use for the options provided below if you do not want to enable them.	
Access Control List	(Optional) Choose Static and specify the name of the access control list to enable it. The name of the access control list can be up to 27 characters, and cannot contain a hyphen (-), left bracket ([), right bracket, (]) forward slash (/), back slash (\), apostrophe (‘), left angle bracket (<), or right angle bracket (>).
Auto Command	(Optional) Choose Static and specify the command to enable it.

Table 9-9 Shell Profile: Common Tasks

Option	Description
No Callback Verify	(Optional) Choose Static and specify whether or not you want callback verification. Valid options are: • true—Specifies that callback verification is not needed. • false—Specifies that callback verification is needed.
No Escape	(Optional) Choose Static and specify whether or not you want escape prevention. Valid options are: • true—Specifies that escape prevention is enabled. • false—Specifies that escape prevention is not enabled.
No Hang Up	(Optional) Choose Static and specify whether or not you want no hangup. Valid options are: • true—Specifies no hangups are allowed. • false—Specifies that hangups are allowed.
Timeout	(Optional) Choose Static to enable and specify, in minutes, the duration of the allowed timeout in the value field. The valid range is from 0 to 999.
Idle Time	(Optional) Choose Static to enable and specify, in minutes, the duration of the allowed idle time in the value field. The valid range is from 0 to 999.
Callback Line	(Optional) Choose Static to enable and specify the callback phone line in the value field.
Callback Rotary	(Optional) Choose Static to enable and specify the callback rotary phone line in the value field.

Step 3 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **General** tab to configure the name and description for the authorization profile; see Defining General Shell Profile Properties, page 9-26.
- The **Custom Attributes** tab to configure Custom Attributes for the authorization profile; see Defining Custom Attributes, page 9-28.

Related Topics

- Defining Custom Attributes, page 9-28
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Defining Custom Attributes

Use this tab to define custom attributes for the shell profile. This tab also displays the Common Tasks Attributes that you have chosen in the Common Tasks tab.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Edit the fields in the Custom Attributes tab as described in Table 9-10:

Table 9-10 Shell Profile: Custom Attributes Page

Option	Description
Common Tasks Attributes	Displays the names, requirements, and values for the Common Tasks Attributes that you have defined in the Common Tasks tab.
Manually Entered	Use this section to define custom attributes to include in the authorization profile. As you define each attribute, its name, requirement, and value appear in the table. To: • Add a custom attribute, fill in the fields below the table and click **Add**. • Edit a custom attribute, select the appropriate row in the table and click **Edit**. The custom attribute parameters appear in the fields below the table. Edit as required, then click **Replace**.
Attribute	Name of the custom attribute.
Requirement	Choose whether this custom attribute is Mandatory or Optional.
Value	Value of the custom attribute.

Step 2 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **General** tab to configure the name and description for the authorization profile; see Defining General Shell Profile Properties, page 9-26.
- The **Common Tasks** tab to configure the shell profile's privilege level and attributes for the authorization profile; see Defining Common Tasks, page 9-27.

Related Topics

- Defining General Shell Profile Properties, page 9-26
- Defining Common Tasks, page 9-27

Creating, Duplicating, and Editing Command Sets for Device Administration

Command sets provide decisions for allowed commands and arguments for device administration. You can specify command sets as results in a device configuration authorization policy. Shell profiles and command sets are combined for authorization purposes, and are enforced for the duration of a user's session.

You can duplicate a command set if you want to create a new command set that is the same, or similar to, an existing command set. After duplication is complete, you access each command set (original and duplicated) separately to edit or delete them.

After you create command sets, you can use them in authorizations and permissions within rule tables. A rule can contain multiple command sets. See Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24.

Note Command sets support TACACS+ protocol attributes only.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a new command set:

Step 1 Select **Policy Elements > Authorization and Permissions > Device Administration > Command Sets**.

The Command Sets page appears.

Step 2 Do one of the following:

- Click **Create**. The Command Set Properties page appears.
- Check the check box next to the command set that you want to duplicate and click **Duplicate**. The Command Set Properties page appears.
- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**. The Command Set Properties page appears.
- Click **File Operations** to perform any of the following functions:
  - Add—Choose this option to add command sets from the import file to ACS.
  - Update—Choose this option to replace the list of command sets in ACS with the list of command sets in the import file.
  - Delete—Choose this option to delete the command sets listed in the import file from ACS.

  See Performing Bulk Operations for Network Resources and Users, page 7-8 for a detailed description of the bulk operations.
- Click **Export** to export the command sets from ACS to your local hard disk.

  A dialog box appears, prompting you to enter an encryption password to securely export the command sets:
  - Check the **Password** check box and enter the password to encrypt the file during the export process, then click **Start Export**.
  - Click **Start Export** to export the command sets without any encryption.

Step 3 Enter valid configuration data in the required fields. As a minimum configuration, you must enter a unique name for the command set; all other fields are optional. You can define commands and arguments; you can also add commands and arguments from other command sets.

See Table 9-11 for a description of the fields in the Command Set Properties page.

Table 9-11 Command Set Properties Page

Field	Description
Name	The name of the command set.
Description	(Optional) The description of the command set.
Permit any command that is not in the table below	Check to allow all commands that are requested, unless they are explicitly denied in the Grant table. Uncheck to allow only commands that are explicitly allowed in the Grant table.

Table 9-11 Command Set Properties Page (continued)

Field	Description
Command Set table	Use this section to define commands to include in the authorization profile. As you define each command, its details appear in the table. To: • Add a command, fill in the fields below the table and click **Add**. • Edit a command, select the appropriate row in the table, and click **Edit**. The command parameters appear in the fields below the table. Edit as required, then click **Replace**. The order of commands in the Command Set table is important; policy rule table processing depends on which command and argument are matched first to make a decision on policy result choice. Use the control buttons at the right of the Command Set table to order your commands.
Grant	Choose the permission level of the associated command. Options are: • Permit—The associated command and arguments are automatically granted. • Deny—The associated command and arguments are automatically denied. • Deny Always—The associated command and arguments are always denied.
Command	Enter the command name. This field is not case sensitive. You can use the asterisk (*) to represent zero (0) or more characters in the command name, and you can use the question mark (?) to represent a single character in a command name. Examples of valid command name entries: • SHOW • sH* • sho? • Sh*?
Arguments (field)	Enter the argument associated with the command name. This field is not case sensitive. **Note** ACS 5.1 uses standard UNIX-type regular expressions.
Select Command/ Arguments from Command Set	To add a command from another command set: 1. Choose the command set. 2. Click **Select** to open a page that lists the available commands and arguments. 3. Choose a command and click **OK**.

Step 4 Click **Submit**.

The command set is saved. The Command Sets page appears with the command set that you created or duplicated.

Related Topics

- Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18
- Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24
- Deleting an Authorizations and Permissions Policy Element, page 9-33
- Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-24

Creating, Duplicating, and Editing Downloadable ACLs

You can define downloadable ACLs 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 downloadable ACLs 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 downloadable ACL if you want to create a new downloadable ACL that is the same, or similar to, an existing downloadable ACL.

After duplication is complete, you access each downloadable ACL (original and duplicated) separately to edit or delete them.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate or edit a downloadable ACL:

Step 1 Select **Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs**.

The Downloadable ACLs page appears.

Step 2 Do one of the following:

- Click **Create**. The Downloadable ACL Properties page appears.
- Check the check box next to the downloadable ACL that you want to duplicate and click **Duplicate**. The Downloadable ACL Properties page appears.
- Click the name that you want to modify; or, check the check box next to the name that you want to modify and click **Edit**. The Downloadable ACL Properties page appears.
- Click **File Operations** to perform any of the following functions:
  - Add—Choose this option to add ACLs from the import file to ACS.
  - Update—Choose this option to replace the list of ACLs in ACS with the list of ACLs in the import file.
  - Delete—Choose this option to delete the ACLs listed in the import file from ACS.

  See Performing Bulk Operations for Network Resources and Users, page 7-8 for a detailed description of the bulk operations.
- Click **Export** to export the DACLs from ACS to your local hard disk.

  A dialog box appears, prompting you to enter an encryption password to securely export the DACLs:
  - Check the **Password** check box and enter the password to encrypt the file during the export process, then click **Start Export**.
  - Click **Start Export** to export the DACLs without any encryption.

Step 3 Enter valid configuration data in the required fields as shown in Table 9-12, and define one or more ACLs by using standard ACL syntax.

Table 9-12 Downloadable ACL Properties Page

Option	Description
Name	The name of the DACL.
Description	The description of the DACL.
Downloadable ACL Content	Define the ACL content. Use standard ACL command syntax and semantics. The ACL definitions comprise one or more ACL commands; each ACL command must occupy a separate line. For detailed ACL definition information, see the command reference section of your device configuration guide.

Step 4 Click **Submit**.

The downloadable ACL is saved. The Downloadable ACLs page appears with the downloadable ACL that you created or duplicated.

Related Topics

- Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Deleting an Authorizations and Permissions Policy Element, page 9-33

Deleting an Authorizations and Permissions Policy Element

To delete an authorizations and permissions policy element:

Step 1 Select **Policy Elements** > **Authorization and Permissions;** then, navigate to the required option.

The corresponding page appears.

Step 2 Check one or more check boxes next to the items that you want to delete and click **Delete**.

The following message appears:

Are you sure you want to delete the selected item/items?

Step 3 Click **OK**.

The page appears without the deleted object.

Configuring Security Group Access Control Lists

Security group access control lists (SGACLs) are applied at Egress, based on the source and destination SGTs. Use this page to view, create, duplicate and edit SGACLs. When you modify the name or content of an SGACL, ACS updates its generation ID. When the generation ID of an SGACL changes, the relevant TrustSec network devices reload the content of the SGACL.

Note SGACLs are also called role-based ACLs (RBACLs).

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Policy Elements > Authorizations and Permissions > Named Permissions Objects > Security Group ACLs**.

The Security Group Access Control Lists page appears with the fields described in Table 9-13:

Table 9-13 Security Group Access Control Lists Page

Option	Description
Name	The name of the SGACL.
Description	The description of the SGACL.

Step 2 Click one of the following options:

- **Create** to create a new SGACL.
- **Duplicate** to duplicate an SGACL.
- **Edit** to edit an SGACL.

Step 3 Complete the fields in the Security Group Access Control Lists Properties page as described in Table 9-14:

Table 9-14 Security Group Access Control List Properties Page

Option	Description
General	
Name	The name of the SGACL. You cannot use spaces, hyphens (-), question marks (?), or exclamation marks (!) in the name. After you create an SGACL, its generation ID appears.
Generation ID	*Display only.* ACS updates the generation ID of the SGACL if you change the: • Name of the SGACL. • Content of the SGACL (the ACEs). Changing the SGACL description does not affect the generation ID.
Description	The description of the SGACL.
Security Group ACL Content	Enter the ACL content. Ensure that the ACL definition is syntactically and semantically valid.

Step 4 Click **Submit**.

TACACS+ Command Sets

ACS recognizes that an authorization request is specifically a command administration request by examining the following rules:

- The service attribute, which must be shell for command authorization
- The command attribute length is not zero

Within the context of a given access service, the device administration rule table is then used to select the appropriate command sets. The contents of the command and command-argument attributes are then processed against the command sets to determine whether they are valid.

The TACACS+ Command Set Definition

A Command Set defines the set of commands, and command arguments that are permitted. It can be called as a matching process. The Command Sets and their interpretations are defined as follows.

- Command set =<Unmatched Command Flag> + <Command List>
- Unmatched Command Flag =[Permit | Deny-Always | Deny-If-Not-Otherwise-Permitted]
- Command List ={Command}*
- Command = Command String + <Unmatched Argument Flag> + <Argument List>
- Arg List = [Permit | Deny-Always | Deny-If-Not-Otherwise-Permitted] + Argument String
- Unmatched Arg Flag = [Permit | Deny-Always | Deny-If-Not-Otherwise-Permitted]

{}* means a list in {} with zero or more entries of the object defined inside the {}. It means that a command list may have zero or more commands.

The command list is ordered. There is a logical significance in the position of the command in the list.

In the management interfaces, *Deny-If-Not-Otherwise-Permitted* is treated as Deny.

Evaluation of Command Based Administration

After the access service is selected, the incoming request is tested against the set of conditions in the rule table.

This results in one or more rules being selected. You can configure the rule table to work as a first-matched-result, whereby the first row whose conditions match is used to obtain the corresponding result, or a multi-matched-result, whereby all rows whose conditions match are used to obtain a set of results. The first matched table is equivalent to a multi-matched table where a single row has matching conditions.

For every row whose conditions match, there is a list of command sets. The command from the request is now processed against this total collection of command sets that result from the rule table. This is a three-level hierarchy of matching process:

- Level 1—Specifies exactly how it is possible to determine whether an incoming command matches an individual entry in a command set list.
- Level 2—Specifies the logic of how the results of matching individual entries in a command set list determine the outcome of matching a single complete command set.

- Level 3—Specifies the logic of how the outcome of the matching process for each single command set within total collection of command sets that result from the rule table are resolved to determine the final outcome.

Level 1: Match Logic for a Single Command Definition in a Command Set

You can determine whether an incoming command matches an individual entry in a command set list. Each entry in the command set is essentially composed of a list of commands and command arguments.

For example, if the input is:

```
<command> + <argument1>…<argument n>
```

The procedure to match the logic is:

Step 1 Go over the command set list to detect matching commands. A command is matched using simple wildcard matching. Wildcard matching permits:

- Case insensitivity
- Any character in the command set may be a '?' which will match any character in the request, though the character must exist.
- Any character in the command set may be a '*' which can match zero or more characters in the requested command.

Table 9-15 shows some examples of command set request matches.

Table 9-15 Examples of Command Set request Matches

Request	Command Set	Matches	Comment
show	show	Yes	Trivial case
show	SHOW	Yes	Case insensitive
show	Sh??	Yes	? matched any character
show	Sho??	No	Second ? intersects with character that doesn't exist.
show	S*	Yes	* matches any character
show	S*w	Yes	* matches the characters ‘ho’
show	S*p	No	The 'p' does not correspond.
show	S*?	Yes	The matching login knows that * should leave a character unmatched for ? to correspond with.

Step 2 For each matching command, validate the arguments.

If there is a valid command in the command set that has matched then match of the arguments is examined. The command set will include a space-delimited set of arguments for each command.

For example:

```
Show interface[1-4] port[1-9]:tty*
```

This command has two arguments:

- Argument 1: interface[1-4]
- Argument 2: port[1-9]:tty*

The command arguments in the request are taken in the position-significant order that they appear in the packet. Every argument in the command definition must be matched by an argument in the request. The matching process is selected to be unix regular expression, for backwards compatibility with previous version of ACS 4.x. If all the arguments in the command definition match the arguments in the request, then this command/argument is said to be matched. Any extraneous arguments in the request are ignored.

Each command/argument list combination is assigned a grant type, this is effectively the result if the command matched. The grant type may be one of the following:

- permit
- deny
- deny always

This result is then used for resolving the response.

Level 2: Match Logic for a Command Set

After you have a set of command lines in a command set that is determined in the first level of processing, the next step for command processing is to match the requested command and argument.

To match the requested command and argument, the following two factors are considered:

- The permission attached to the command.
- The order of the matched commands in the list.

There are three possible permissions, one of which must be attached to a command. They are presented here in the decreasing order of precedence:

- Deny Always (Overrides, independent of order).
- Deny/Permit (Resolved by first Match)

The list of matched commands in a command set is examined.

If any of the items are *Deny Always* then the result of the command set is *Commandset-Deny Always.*

Otherwise, the result of the command set is the first match, using *first* to be defined by the order configured by the administrator. If the first match is *Deny*, then the result of the complete command set is *Commandset-Deny.* If the first match is a permit, then the result of the complete command set is *Commandset-Permit*.

Level 3: Match Logic for the Combined Set of Command Sets

The final stage is to resolve these results for all the command sets selected, into a single Permit or Deny to return as a response to the query. The logic for this is to take the unordered results from all the enabled command sets:

Any *Commandset-DenyAlways* results in an overall Deny.

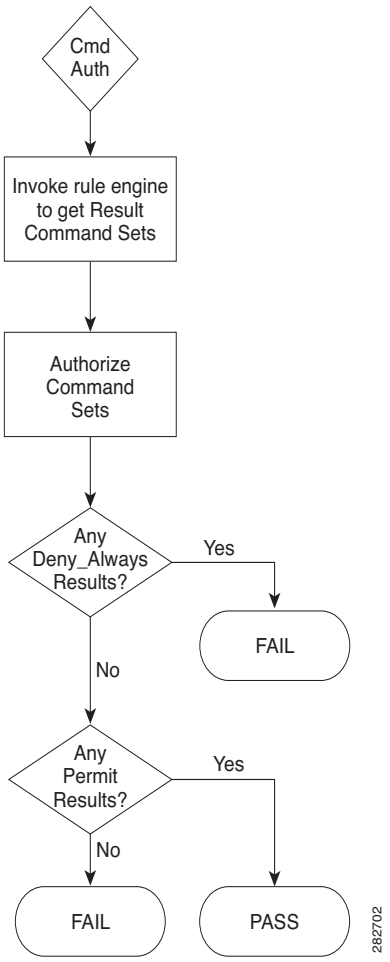
If there is no *Commandset-DenyAlways*, then a command is permitted if any of the command sets respond with a *Commandset-Permit* result.

If neither of the previous two conditions are met, then the result is a Deny.

At this point the *Commandset-Permit* is interpreted to have a higher precedence than *Commandset-Deny.*

Figure 9-1 shows the flow chart of the match logic behind combined command sets.

Figure 9-1 Match Logic For Combined Command Sets



CHAPTER 10

Managing Access Policies

In ACS 5.1, policy drives all activities. Policies consist mainly of rules that determine the action of the policy. You create access services to define authentication and authorization policies for requests. A global service selection policy contains rules that determine which access service processes an incoming request.

For a basic workflow for configuring policies and all their elements, see Flows for Configuring Services and Policies, page 3-18. In general, before you can configure policy rules, you must configure all the elements that you will need, such as identities, conditions, and authorizations and permissions.

For information about:

- Managing identities, see Chapter 8, "Managing Users and Identity Stores."
- Configuring conditions, see Managing Policy Elements, page 9-1.
- Configuring authorizations and permissions, see Configuring System Operations, page 17-1.

This section contains the following topics:

- Policy Creation Flow, page 10-1
- Customizing a Policy, page 10-5
- Configuring the Service Selection Policy, page 10-6
- Configuring Access Services, page 10-11
- Configuring Access Service Policies, page 10-20
- Configuring Compound Conditions, page 10-42
- TrustSec Access Control Pages, page 10-46

For information about creating Egress and NDAC policies for Cisco TrustSec, see Configuring an NDAC Policy, page 4-24.

Policy Creation Flow

Policy creation depends on your network configuration and the degree of refinement that you want to bring to individual policies. The endpoint of policy creation is the access service that runs as the result of the service selection policy. Each policy is rule driven.

In short, you must determine the:

- Details of your network configuration.
- Access services that implement your policies.
- Rules that define the conditions under which an access service can run.

This section contains the following topics:

- Network Definition and Policy Goals, page 10-2
- Policy Elements in the Policy Creation Flow, page 10-3
- Access Service Policy Creation, page 10-4
- Service Selection Policy Creation, page 10-4

Network Definition and Policy Goals

The first step in creating a policy is to determine the devices and users for which the policy should apply. Then you can start to configure your policy elements.

For basic policy creation, you can rely on the order of the drawers in the left navigation pane of the web interface. The order of the drawers is helpful because some policy elements are dependent on other policy elements. If you use the policy drawers in order, you initially avoid having to go backward to define elements that your current drawer requires.

For example, you might want to create a simple device administration policy from these elements in your network configuration:

- Devices—Routers and switches.
- Users—Network engineers.
- Device Groups—Group devices by location and separately by device type.
- Identity groups—Group network engineers by location and separately by access level.

The results of the policy apply to the administrative staff at each site:

- Full access to devices at their site.
- Read-only access to all other devices.
- Full access to everything for a supervisor.

The policy itself applies to network operations and the administrators who will have privileges within the device administration policy. The users (network engineers) are stored in the internal identity store.

The policy results are the authorizations and permissions applied in response to the access request. These authorizations and permissions are also configured as policy elements.

Policy Creation Flow—Next Steps

- Policy Elements in the Policy Creation Flow, page 10-3
- Access Service Policy Creation, page 10-4
- Service Selection Policy Creation, page 10-4

Policy Elements in the Policy Creation Flow

The web interface provides these defaults for defining device groups and identity groups:

- All Locations
- All Device Types
- All Groups

The locations, device types, and identity groups that you create are children of these defaults.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create the building blocks for a basic device administration policy:

Step 1 Create network resources. In the Network Resources drawer, create:

a. Device groups for Locations, such as All Locations > East, West, HQ.

b. Device groups for device types, such as All Device Types > Router, Switch.

c. AAA clients (clients for AAA switches and routers, address for each, and protocol for each), such as EAST-ACCESS-SWITCH, HQ-CORE-SWITCH, or WEST-WAN-ROUTER.

Step 2 Create users and identity stores. In the Users and Identity Stores drawer, create:

a. Identity groups (Network Operations and Supervisor).

b. Specific users and association to identity groups (Names, Identity Group, Password, and more).

Step 3 Create authorizations and permissions for device administration. In the Policy Elements drawer, create:

a. Specific privileges (in Shell Profiles), such as full access or read only.

b. Command Sets that allow or deny access (in Command Sets).

For this policy, you now have the following building blocks:

- Network Device Groups (NDGs), such as:
  - Locations—East, HQ, West.
  - Device Types—Router, Switch.
- Identity groups, such as:
  - Network Operations Sites—East, HQ, West.
  - Access levels—Full Access.
- Devices—Routers and switches that have been assigned to network device groups.
- Users—Network engineers in the internal identity store that have been assigned to identity groups.

- Shell Profiles—Privileges that can apply to each administrator, such as:
  - Full privileges.
  - Read only privileges.
- Command Sets—Allow or deny authorization to each administrator.

Policy Creation Flow—Previous Step

- Network Definition and Policy Goals, page 10-2

Policy Creation Flow—Next Steps

- Access Service Policy Creation, page 10-4
- Service Selection Policy Creation, page 10-4

Access Service Policy Creation

After you create the basic elements, you can create an access policy that includes identity groups and privileges. For example, you can create an access service for device administration, called NetOps, which contains authorization and authentication policies that use this data:

- Users in the Supervisor identity group—Full privileges to all devices at all locations.
- User in the East, HQ, West identity groups—Full privileges to devices in the corresponding East, HQ, West device groups.
- If no match—Deny access.

Policy Creation Flow—Previous Steps

- Network Definition and Policy Goals, page 10-2
- Policy Elements in the Policy Creation Flow, page 10-3

Policy Creation Flow—Next Step

- Service Selection Policy Creation, page 10-4

Service Selection Policy Creation

ACS provides support for various access use cases; for example, device administration, wireless access, network access control, and so on. You can create access policies for each of these use cases. Your service selection policy determines which access policy applies to an incoming request.

For example, you can create a service selection rule to apply the NetOps access service to any access request that uses the TACAC+ protocol.

Policy Creation Flow—Previous Steps

- Network Definition and Policy Goals, page 10-2
- Policy Elements in the Policy Creation Flow, page 10-3
- Access Service Policy Creation, page 10-4

Customizing a Policy

ACS policy rules contain conditions and results. Before you begin to define rules for a policy, you must configure which types of conditions that policy will contain. This step is called customizing your policy. The condition types that you choose appear on the Policy page. You can apply only those types of conditions that appear on the Policy page. For information about policy conditions, see Managing Policy Conditions, page 9-1.

By default, a Policy page displays a single condition column for compound expressions. For information on compound conditions, see Configuring Compound Conditions, page 10-42.

Note If you have implemented TrustSec functionality, you can also customize results for authorization policies.

Caution If you have already defined rules, be certain that a rule is not using any condition that you remove when customizing conditions. Removing a condition column removes all configured conditions that exist for that column.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To customize a policy:

Step 1 Open the Policy page that you want to customize. For:

- The service selection policy, choose **Access Policies > Service Selection Policy**.
- An access service policy, choose **Access Policies > Access Services > *<service>* > *<policy>***, where *<service>* is the name of the access service, and *<policy>* is the name of the policy that you want to customize.

Step 2 In the Policy page, click **Customize**.

A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions.

Note Identity-related attributes are not available as conditions in a service selection policy.

Step 3 Move conditions between the Available and Selected list boxes.

Step 4 Click **OK**, and the selected conditions now appear under the Conditions column.

Step 5 Click **Save Changes**.

Configuring a Policy—Next Steps

- Configuring the Service Selection Policy, page 10-6
- Configuring Access Service Policies, page 10-20

Configuring the Service Selection Policy

The service selection policy determines which access service processes incoming requests. You can configure a simple policy, which applies the same access service to all requests; or, you can configure a rule-based service selection policy.

In the rule-based policy, each service selection rule contains one or more conditions and a result, which is the access service to apply to an incoming request. You can create, duplicate, edit, and delete rules within the service selection policy, and you can enable and disable them.

This section contains the following topics:

- Configuring a Simple Service Selection Policy, page 10-6
- Creating, Duplicating, and Editing Service Selection Rules, page 10-8

Note If you create and save a simple policy, and then change to a rule-based policy, the simple policy becomes the default rule of the rule-based policy. If you have saved a rule-based policy and then change to a simple policy, you will lose all your rules except for the default rule. ACS automatically uses the default rule as the simple policy.

Configuring a Simple Service Selection Policy

A simple service selection policy applies the same access service to all requests.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To configure a simple service selection policy:

Step 1 Select **Access Policies > Service Selection Policy**.

By default, the Simple Service Selection Policy page appears.

Step 2 Select an access service to apply; or, choose **Deny Access**.

Step 3 Click **Save Changes** to save the policy.

Service Selection Policy Page

Use this page to configure a simple or rule-based policy to determine which service to apply to incoming requests.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To display this page, choose **Access Policies > Service Selection**.

If you have already configured the service selection policy, the corresponding Simple Policy page (see Table 10-1) or Rule-based Policy page (see Table 10-2) opens; otherwise, the Simple Policy page opens by default.

Table 10-1 Simple Service Selection Policy Page

Option	Description
Policy type	Defines the type of policy: • Select one result—The results apply to all requests. • Rule-based result selection—Configuration rules apply different results depending on the request.
Service Selection Policy	The access service to apply to all requests. The default is Deny Access.

Table 10-2 Rule-based Service Selection Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Select one result—Results apply to all requests. • Rule-based result selection—Configuration rules apply different results depending on the request.
Status	The current status of the rule that drives service selection. The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor Only—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	The rule name.
Conditions	The conditions that determine the scope of the service. This column displays all current conditions in subcolumns. **Note** You cannot use identity-based conditions in a service selection rule.
Results	The service that runs as a result of the evaluation of the rule.
Hit Count	The number of times that the rule is matched. Click **Hit Count** to refresh and reset this column.

Table 10-2 Rule-based Service Selection Policy Page (continued)

Option	Description
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

To configure a rule-based service selection policy, see these topics:

- Creating, Duplicating, and Editing Service Selection Rules, page 10-8
- Deleting Service Selection Rules, page 10-11

After you configure your service selection policy, you can continue to configure your access service policies. See Configuring Access Service Policies, page 10-20.

Creating, Duplicating, and Editing Service Selection Rules

Create service selection rules to determine which access service processes incoming requests. The Default Rule provides a default access service in cases where no rules are matched or defined.

When you create rules, remember that the order of the rules is important. When ACS encounters a match as it processes the request of a client that tries to access the ACS network, all further processing stops and the associated result of that match is found. No further rules are considered after a match is found.

You can duplicate a service selection rule to create a new rule that is the same, or very similar to, an existing rule. The duplicate rule name is based on the original rule with parentheses to indicate duplication; for example, Rule-1(1). After duplication is complete, you access each rule (original and duplicated) separately. You cannot duplicate the Default rule.

You can edit all values of service selection rules; you can edit the specified access service in the Default rule.

Note To configure a simple policy to apply the same access service to all requests, see Configuring a Simple Service Selection Policy, page 10-6.

Before You Begin

- Configure the conditions that you want to use in the service selection policy. See Managing Policy Conditions, page 9-1.

Note Identity-related attributes are not available as conditions in a service selection policy.

- Create the access services that you want to use in the service selection policy. See Creating, Duplicating, and Editing Access Services, page 10-13. You do not need to configure policies in the access service before configuring the service selection policy.
- Configure the types of conditions to use in the policy rules. See Customizing a Policy, page 10-5, for more information.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit a service selection policy rule:

Step 1 Select **Access Policies > Service Selection Policy**. If you:

- Previously created a rule-based policy, the Rule-Based Service Selection Policy page appears with a list of configured rules.
- Have not created a rule-based policy, the Simple Service Selection Policy page appears. Click **Rule-Based**.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the rule that you want to duplicate; then click **Duplicate**.
- Click the rule name that you want to modify; or, check the check box next to the name and click **Edit**.

The Rule page appears.

Step 3 Enter or modify values:

- User-defined rules—You can edit any value. Ensure that you include at least one condition. If you are duplicating a rule, you must change the rule name.
- The Default Rule—You can change only the access service.

See Table 10-3 for field descriptions:

Table 10-3 Service Selection Rule Properties Page

Option	Description
General	
Name	The name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.

Table 10-3 Service Selection Rule Properties Page (continued)

Option	Description
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor Only—The rule is active but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Conditions	
<condition(s)>	The conditions that you can configure for the rule. By default, the compound condition appears. Click **Customize** in the Policy page to change the conditions that appear. The default value for each condition is *ANY*. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-42.
Results	
Service	The name of the access service that runs as a result of the evaluation of the rule.

Step 4 Click **OK.** The Service Selection Policy page appears with the rule that you configured.

Step 5 Click **Save Changes**.

Related Topics

- Configuring Access Services, page 10-11
- Deleting Service Selection Rules, page 10-11

Displaying Hit Counts

Use this page to reset and refresh the Hit Count display on the Rule-based Policy page.

To display this page, click **Hit Count** on the Rule-based Policy page.

Table 10-4 Hit Count Page

Option	Description
Hit Counts Reset	
Last time hit counts were reset for this policy	Displays the date and time of the last hit count reset for this policy.
Reset hit counts display for this policy	Click **Reset** to reset the hit counts display to zero (0) for all rules on the Policy page.

Table 10-4 Hit Count Page (continued)

Option	Description
Hit Counts Collection	
Hit counts are collected every:	Displays the interval between hit count collections.
Last time hit counts were collected for this policy:	Displays the date and time of the last hit count update for this policy.
Refresh hit counts display for this policy	Click **Refresh** to refresh the hit count display in the Policy page with updated hit counts for all rules. The previous hit counts are deleted. **Note** When a TACACS+ authentication request succeeds, the hit counts of the corresponding identity policy rule and authorization policy rule both increase by 1.

Deleting Service Selection Rules

Note You cannot delete the Default service selection rule.

To delete a service selection rule:

Step 1 Select **Access Policies > Service Selection Policy**.

The Service Selection Policy page appears, with a list of configured rules.

Step 2 Check one or more check boxes next to the rules that you want to delete.

Step 3 Click **Delete**.

The Service Selection Rules page appears without the deleted rule(s).

Step 4 Click **Save Changes** to save the new configuration.

Configuring Access Services

Access services contain the authentication and authorization policies for requests. You can create separate access services for different use cases; for example, device administration, wireless network access, and so on.

When you create an access service, you define the type of policies and policy structures that it contains; for example, policies for device administration or network access.

Note You must create access services before you define service selection rules, although you do not need to define the policies in the services.

This section contains the following topics:

- Creating, Duplicating, and Editing Access Services, page 10-13
- Deleting an Access Service, page 10-20

After you create an access service, you can use it in the service selection policy. See Configuring the Service Selection Policy, page 10-6.

You can customize and modify the policies in the access service. See Configuring Access Service Policies, page 10-20.

Related Topic

- Creating, Duplicating, and Editing Access Services, page 10-13

Editing Default Access Services

ACS 5.1 is preconfigured with two default access services, one for device administration and another for network access. You can edit these access services.

To edit the default access service:

Step 1 Choose one of the following:

- **Access Policies > Access Services > Default Device Admin**
- **Access Policies > Access Services > Default Network Access**

The Default <*Service*> Access Service Edit page appears.

Step 2 Edit the fields in the Default <*Service*> Access Service page.

Table 10-5 describes the fields in the General tab.

Table 10-5 Default Access Service - General Page

Option	Description
General	
Name	Name of the access service.
Description	Description of the access service.
Service Type	(Display only) Type of service, device administration, or network access.
Policy Structure	
Identity	Check to include an identity policy in the access service, to define the identity store or stores that ACS uses for authentication and attribute retrieval.
Group Mapping	Check to include a group mapping policy in the access service, to map groups and attributes that are retrieved from external identity stores to the identity groups in ACS.
Authorization	Check to include an authorization policy in the access service, to apply: • Authorization profiles for network access services. • Shell profiles and command sets for device administration services.

Step 3 Edit the fields in the Allowed Protocols tab as described in Table 10-7.

Step 4 Click **Submit** to save the changes you have made to the default access service.

Creating, Duplicating, and Editing Access Services

Access services contain the authentication and authorization policies for requests.

When you create an access service, you define:

- Policy structure—The types of policies the service will contain. You can define these according to a service template, an existing service, or a use case.

  A service can contain:

  - An Identity policy—Defines which identity store to use for authentication.
  - A group mapping policy—Defines the identity group to which to map.
  - An Authorization policy—For network access, this policy defines which session authorization profile to apply; for device administration, it defines which shell profile or command set to apply.
- Allowed protocols—Specifies which authentication protocols are allowed for this access service, and provides additional information about how ACS uses them for authentication.

Use a service template to define an access service with policies that are customized to use specific condition types. See Configuring Access Services Templates, page 10-19 for information about the service templates.

Duplicate an access service to create a new access service with rules that are the same, or very similar to, an existing access service. After duplication is complete, you access each service (original and duplicated) separately.

Note To replicate a service policy structure without duplicating the source service's rules, create a new access service based on an existing service.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, or edit an access service:

Step 1 Select **Access Policies > Access Services**.

The Access Services page appears with a list of configured services.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the access service that you want to duplicate; then click **Duplicate**.
- Click the access service name that you want to modify; or, check the check box next to the name and click **Edit**.
- Click the access service name in the left navigation tab.

The Access Service Properties General page appears.

Step 3 If you are creating a new access service:

a. Define the name and policy structure of the access service.

b. Click **Next** to proceed to the Allowed Protocols page.

c. Click **Finish** to save the new access service.

Step 4 If you are duplicating or editing an access service:

a. Modify fields in the Properties page tabs as required. You can add policies, but you cannot remove existing policies.

b. Click **Submit** to save changes.

For information about valid field options, see:

- Configuring General Access Service Properties, page 10-14
- Configuring Access Service Allowed Protocols, page 10-16
- Configuring Access Services Templates, page 10-19

The access service configuration is saved. The Access Services page appears with the new configuration.

Related Topics

- Deleting an Access Service, page 10-20
- Configuring Access Service Policies, page 10-20
- Configuring the Service Selection Policy, page 10-6

Configuring General Access Service Properties

Access service definitions contain general and allowed protocol information. When you duplicate and edit services, the Access Service properties page contains tabs.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Access Policies > Access Services**, then click **Create**, **Duplicate**, or **Edit**.

Step 2 Complete the fields as described in Table 10-6:

Table 10-6 Access Service Properties—General Page

Option	Description
General	
Name	The name of the access service. If you are duplicating a service, you must enter a unique name as a minimum configuration; all other fields are optional.
Description	The description of the access service.
Access Service Policy Structure	
Based on service template	Creates an access service containing policies based on a predefined template. This option is available only for service creation.

Table 10-6 Access Service Properties—General Page (continued)

Option	Description
Based on existing service	Creates an access service containing policies based on an existing access service. The new access service does not include the existing service's policy rules. This option is available only for service creation.To replicate a service, including its policy rules, duplicate an existing access service.
User selected service type	Provides you the option to select the access service type. The available options are Network Access, Device Administration, and RADIUS Proxy. The list of policies you can configure depends on your choice of access service type.
User Selected Service Type—Network Access and Device Administration	
Policy Structure	
Identity	Check to include an identity policy in the access service to define the identity store or stores that ACS uses for authentication and attribute retrieval.
Group Mapping	Check to include a group mapping policy in the access service to map groups and attributes that are retrieved from external identity stores to ACS identity groups.
Authorization	Check to include an authorization policy in the access service to apply: • Authorization profiles for network access services. • Shell profiles and command sets for device administration services.
User Selected Service Type—RADIUS Proxy	
Select the set of External RADIUS servers to be used for proxy. You can also determine the order in which these servers will be used.	
Available External RADIUS Servers	The list of available external RADIUS servers. Select the external RADIUS servers to be used for proxy and move them to the Selected External RADIUS Servers list.
Selected External RADIUS Servers	The list of selected external RADIUS servers.
Advanced Options	
Accounting	
Remote Accounting	Check to enable remote accounting.
Local Accounting	Check to enable local accounting.
Username Prefix\Suffix Stripping	
Strip start of subject name up to the last occurrence of the separator	Check to strip the username from the prefix. For example, if the subject name is acme\smith and the separator is \, the username becomes smith.
Strip end of subject name from the first occurrence of the separator	Check to strip the username from the suffix. For example, if the subject name is smith@acme.com and the separator is @, the username becomes smith.

Step 3 Click **Next** to configure the allowed protocols. See Configuring Access Service Allowed Protocols, page 10-16.

Related Topic

- Configuring Access Service Allowed Protocols, page 10-16
- Configuring Access Services Templates, page 10-19

Configuring Access Service Allowed Protocols

The allowed protocols are the second part of access service creation. Access service definitions contain general and allowed protocol information. When you duplicate and edit services, the Access Service properties page contains tabs.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Access Policies > Access Services**, then click:

- **Create** to create a new access service, then click the **Allowed Protocols** tab.
- **Duplicate** to duplicate an access service, then click the **Allowed Protocols** tab.
- **Edit** to edit an access service, then click the **Allowed Protocols** tab.

Step 2 Complete the fields as shown in Table 10-7:

Table 10-7 Access Service Properties—Allowed Protocols Page

Option	Description
Process Host Lookup	Check to configure ACS 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 for ACS to ignore the Host Lookup request and use the original value of the system UserName attribute for authentication and authorization. When unchecked, message processing is according to the protocol (for example, PAP).
Authentication Protocols	
Allow PAP/ASCII	Enables PAP/ASCII. PAP uses clear-text passwords (that is, unencrypted passwords) and is the least secure authentication protocol. When you check **Allow PAP/ASCII**, you can check **Detect PAP as Host Lookup** to configure ACS to detect this type of request as a Host Lookup (instead of PAP) request in the network access service.
Allow CHAP	Enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with the Windows Active Directory.
Allow MS-CHAPv1	Enables MS-CHAPv1.
Allow MSCHAPv2	Enables MSCHAPv2.
Allow EAP-MD5	Enables EAP-based Message Digest 5 hashed authentication. When you check **Allow EAP-MD5**, you can check **Detect EAP-MD5 as Host Lookup** to configure ACS to detect this type of request as a Host Lookup (instead of EAP-MD5) request in the network access service.

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Allow EAP-TLS	Enables the EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how ACS verifies 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 ACS 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. See Configuring Local Server Certificates, page 18-14 for more information.
Allow LEAP	Enables LEAP authentication.
Allow PEAP	Enables the PEAP authentication protocol and PEAP settings. The default inner method is MSCHAPv2. When you check **Allow PEAP**, you can configure the following PEAP inner methods: • Allow EAP-MSCHAPv2—Check to use EAP-MSCHAPv2 as the inner method. – Allow Password Change—Check for ACS to support password changes. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-GTC—Check to use EAP-GTC as the inner method. – Allow Password Change—Check for ACS to support password changes. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1 to 3.
Allow EAP-FAST	Enables the EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MSCHAPv2. When you check **Allow EAP-FAST**, you can configure EAP-FAST inner methods: • Allow EAP-MSCHAPv2 – Allow Password Change—Check for ACS to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1-3. • Allow EAP-GTC – Allow Password Change—Check for ACS to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1-3. • Use PACs—Choose to configure ACS to provision authorization PACs for EAP-FAST clients. Additional PAC Options appear. • Don't use PACs—Choose to configure ACS to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and ACS responds with a Success-TLV without a PAC. When you choose this option, you can configure ACS to perform machine authentication.

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Allow EAP-FAST (continued)	**PAC Options** • 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 one (1) day. • Proactive PAC Update When: <*n*%> of PAC TTL is Left—The Update value ensures that the client has a valid PAC. ACS initiates 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. (Default: 10%) • Allow Anonymous In-band PAC Provisioning—Check for ACS to establish a secure anonymous TLS handshake with the client and provision it with a so-called PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. **Note** To enable Anonymous PAC Provisioning, you must choose both the inner methods, EAP-MSCHAPv2 and EAP-GTC. • Allow Authenticated In-band PAC Provisioning—ACS uses Secure Socket Layer (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 ACS. When you check this option, you can configure ACS to return an Access-Accept message to the client after successful authenticated PAC provisioning. • Allow Machine Authentication—Check for ACS 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 administrator (out-of-band). When ACS receives a valid machine PAC from the end-user client, the machine identity details are extracted from the PAC and verified in the ACS external identity store. After these details are correctly verified, no further authentication is performed. **Note** ACS 5.1 only supports Active Directory as an external identity store for machine authentication. When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When ACS 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 for ACS to provision authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled). Uncheck this option: – If you do not want ACS 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 ACS receives an expired authorization PAC, it performs phase two EAP-FAST authentication.

Step 3 Click **Finish** to save your changes to the access service.

To enable an access service, you must add it to the service selection policy.

Configuring Access Services Templates

Use a service template to define an access service with policies that are customized to use specific condition types.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 In the Configuring General Access Service Properties, page 10-14, choose **Based on service template** and click **Select**.

Step 2 Complete the fields as described in Table 10-8:

Table 10-8 Access Services Templates

Template Name	Access Service Type	Protocols	Policies	Conditions	Results
Device Admin - Simple	Device Administration	PAP/ASCII	Identity	None - Simple	Internal users
			Authorization	Identity group, NDG:Location, NDG:Device Type, Time and Date	Shell profile
Device Admin - Command Auth	Device Administration	PAP/ASCII	Identity	None - Simple	Internal users
			Authorization	Identity group, NDG:Location, NDG: Time and Date	Command sets
Network Access - Simple	Network Access	PEAP, EAP-FAST	Identity	None - Simple	Internal users
			Authorization	NDG:Location, Time and date	Authorization profiles
Network Access - MAC Authentication Bypass	Network Access	Process Host Lookup, PAP/ASCII (detect PAP as host lookup) and EAP-MD5 (detect EAP-MD5 as host lookup)	Identity	None - Simple	Internal users
			Authorization	Use case	Authorization profiles

Deleting an Access Service

To delete an access service:

Step 1 Select **Access Policies > Access Services**.

The Access Services page appears with a list of configured services.

Step 2 Check one or more check boxes next to the access services that you want to delete.

Step 3 Click **Delete**; then click **OK** in the confirmation message.

The Access Policies page appears without the deleted access service(s).

Related Topic

- Creating, Duplicating, and Editing Access Services, page 10-13

Configuring Access Service Policies

You configure access service policies after you create the access service:

- Viewing Identity Policies, page 10-21
- Configuring Identity Policy Rule Properties, page 10-24
- Configuring a Group Mapping Policy, page 10-26
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

You can configure simple policies to apply to the same result to all incoming requests; or, you can create rule-based policies.

Note If you create and save a simple policy, and then change to a rule-based policy, the simple policy becomes the default rule of the rule-based policy. If you have saved a rule-based policy and then change to a simple policy, you will lose all your rules except for the default rule. ACS automatically uses the default rule as the simple policy.

Before you begin to configure policy rules, you must:

- Configure the policy conditions and results. See Managing Policy Conditions, page 9-1.
- Select the types of conditions and results that the policy rules apply. See Customizing a Policy, page 10-5.

For information about configuring policy rules, see:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Viewing Identity Policies

The identity policy in an access service defines the identity source that ACS uses for authentication and attribute retrieval. ACS can use the retrieved attributes in subsequent policies.

The identity source for:

- Password-based authentication can be a single identity store, or an identity store sequence.
- Certificate-based authentication can be a certificate authentication profile, or an identity store sequence.

An identity store sequence defines the sequence that is used for authentication and an optional additional sequence to retrieve attributes. See Configuring Identity Store Sequences, page 8-67.

If you created an access service that includes an identity policy, you can configure and modify this policy. You can configure a simple policy, which applies the same identity source for authentication of all requests; or, you can configure a rule-based identity policy.

In the rule-based policy, each rule contains one or more conditions and a result, which is the identity source to use for authentication. You can create, duplicate, edit, and delete rules within the identity policy; and you can enable and disable them.

Caution If you switch between the simple policy and the rule-based policy pages, you will lose your previously saved policy.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To configure a simple identity policy:

Step 1 Select **Access Policies > Access Services > <*service*> > Identity**, where <*service*> is the name of the access service.

By default, the Simple Identity Policy page appears with the fields described in Table 10-9:

Table 10-9 Simple Identity Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the result to apply to all requests. • Rule-based—Configure rules to apply different results, depending on the request. **Note** If you switch between policy types, you will lose your previously saved policy configuration.
Identity Source	The identity source to apply to all requests. The default is Deny Access. For: • Password-based authentication, choose a single identity store, or an identity store sequence. • Certificate-based authentication, choose a certificate authentication profile, or an identity store sequence. The identity store sequence defines the sequence that is used for authentication and an optional additional sequence to retrieve attributes. See Configuring Identity Store Sequences, page 8-67.
Advanced options	Specifies whether to reject or drop the request, or continue with authentication for these options: • If authentication failed—Default is reject. • If user not found—Default is reject. • If process failed—Default is drop. **Note** Due to restrictions on the underlying protocol, ACS cannot always continue processing when the Continue option is chosen. ACS can continue when authentication fails for PAP/ASCII, EAP-TLS, or Host Lookup. For all other authentication protocols, the request will be dropped even if you choose the Continue option.

Step 2 Select an identity source for authentication; or, choose **Deny Access**.

Step 3 You can configure additional advanced options. See Configuring Identity Policy Rule Properties, page 10-24.

Step 4 Click **Save Changes** to save the policy.

Viewing Rules-Based Identity Policies

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Select **Access Policies > Access Services > <*service*> > Identity**, where <*service*> is the name of the access service.

By default, the Simple Identity Policy page appears with the fields described in Table 10-9. If configured, the Rules-Based Identity Policy page appears with the fields described in Table 10-10:

Table 10-10 Rule-based Identity Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the results to apply to all requests. • Rule-based—Configure rules to apply different results depending on the request. **Caution** If you switch between policy types, you will lose your previously saved policy configuration.
Status	The current status of the rule. The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Name	The rule name.
Conditions	The conditions that determine the scope of the policy. This column displays all current conditions in subcolumns.
Results	The identity source that is used for authentication as a result of the evaluation of the rule.
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

To configure a rule-based policy, see these topics:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

For information about configuring an identity policy for Host Lookup requests, see Configuring an Authorization Policy for Host Lookup Requests, page 4-18.

Related Topics

- Configuring a Group Mapping Policy, page 10-26
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Configuring Identity Policy Rule Properties

You can create, duplicate, or edit an identity policy rule to determine the identity databases that are used to authenticate the client and retrieve attributes for the client.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 To display this page, choose **Access Policies > Access Services > <*service*> > Identity, then do one of the following:**

- **Click Create**.
- **Check a rule check box**, **and click Duplicate**.
- **Click a rule name or check a rule check box, then click Edit**.

Step 2 Complete the fields as shown in the Identity Rule Properties page described in Table 10-11:

Table 10-11 Identity Rule Properties Page

Option	Description
General	
Rule Name	The name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Rule Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Conditions	
<*condition(s)*>	The conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is *ANY*. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-42.
Results	
Identity Source	The identity source to apply to requests. The default is Deny Access. For: • Password-based authentication, choose a single identity store, or an identity store sequence. • Certificate-based authentication, choose a certificate authentication profile, or an identity store sequence. The identity store sequence defines the sequence that is used for authentication and attribute retrieval and an optional sequence to retrieve additional attributes. See Configuring Identity Store Sequences, page 8-67.
Advanced options	Specifies whether to reject or drop the request, or continue with authentication for these options: • If authentication failed—Default is reject. • If user not found—Default is reject. • If process failed—Default is drop. **Note** Due to restrictions on the underlying protocol, ACS cannot always continue processing when the Continue option is chosen. ACS can continue when authentication fails for PAP/ASCII, EAP-TLS or Host Lookup. For all other authentication protocols, the request is dropped even if you choose the Continue option.

Configuring a Group Mapping Policy

Configure a group mapping policy to map groups and attributes that are retrieved from external identity stores to ACS identity groups. When ACS processes a request for a user or host, this policy retrieves the relevant identity group which can be used in authorization policy rules.

If you created an access service that includes a group mapping policy, you can configure and modify this policy. You can configure a simple policy, which applies the same identity group to all requests; or, you can configure a rule-based policy.

In the rule-based policy, each rule contains one or more conditions and a result. The conditions can be based only on attributes or groups retrieved from external attribute stores, and the result is an identity group within the identity group hierarchy. You can create, duplicate, edit, and delete rules within the policy; and you can enable and disable them.

Caution If you switch between the simple policy and the rule-based policy pages, you will lose your previously saved policy.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To configure a simple group mapping policy:

Step 1 Select **Access Policies > Access Services > <*service*> > Group Mapping**, where <*service*> is the name of the access service.

By default, the Simple Group Mapping Policy page appears. See Table 10-12 for field descriptions.

See Table 10-13 for Rule-Based Group Mapping Policy page field descriptions.

Table 10-12 Simple Group Mapping Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the results to apply to all requests. • Rule-based—Configure rules to apply different results depending on the request. **Caution** If you switch between policy types, you will lose your previously saved policy configuration.
Identity Group	The identity group to which attributes and groups from all requests are mapped.

Table 10-13 Rule-based Group Mapping Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the results to apply to all requests. • Rule-based—Configure rules to apply different results depending on the request. **Caution** If you switch between policy types, you will lose your previously saved policy configuration.
Status	The current status of the rule. The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	The rule name.
Conditions	The conditions that determine the scope of the policy. This column displays all current conditions in subcolumns.
Results	The identity group that is used as a result of the evaluation of the rule.
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Step 2 Select an identity group.

Step 3 Click **Save Changes** to save the policy.

To configure a rule-based policy, see these topics:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40

- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Related Topics

- Viewing Identity Policies, page 10-21
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Configuring Group Mapping Policy Rule Properties

Use this page to create, duplicate, or edit a group mapping policy rule to define the mapping of attributes and groups that are retrieved from external databases to ACS identity groups.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Access Policies > Access Services > <*service*> > Group Mapping, then do one of the following:**

- **Click Create**.
- **Check a rule check box, and click Duplicate**.
- **Click a rule name or check a rule check box, then click Edit**.

Step 2 Complete the fields as described in Table 10-14:

Table 10-14 Group Mapping Rule Properties Page

Option	Description
General	
Rule Name	The name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Rule Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
<*condition(s)*>	The conditions that you can configure for the rule. By default, the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-42.
Results	
Identity Group	The identity group to which attributes and groups from requests are mapped.

Configuring a Session Authorization Policy for Network Access

When you create an access service for network access authorization, it creates a Session Authorization policy. You can then add and modify rules to this policy to determine the access permissions for the client session.

You can create a standalone authorization policy for an access service, which is a standard first-match rule table. You can also create an authorization policy with an exception policy. See Configuring Authorization Exception Policies, page 10-36. When a request matches an exception rule, the policy exception rule result is always applied.

The rules can contain any conditions and multiple results:

- Authorization profile—Defines the user-defined attributes and, optionally, the downloadable ACL that the Access-Accept message should return.
- Security Group Tag (SGT)—If you have installed Cisco TrustSec, the authorization rules can define which SGT to apply to the request.

For information about how ACS processes rules with multiple authorization profiles, see Processing Rules with Multiple Authorization Profiles, page 3-16.

To configure an authorization policy, see these topics:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

For information about creating an authorization policy for:

- Host Lookup requests, see ACS and Cisco TrustSec, page 4-22.
- TrustSec support, see Creating an Endpoint Admission Control Policy, page 4-25.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Access Policies > Access Services > <*service*> > Authorization**.

Step 2 Complete the fields as described in Table 10-15:

Table 10-15 Network Access Authorization Policy Page

Option	Description
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	The name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:<*name*>	Network device group. The two predefined NDGs are Location and Device Type.
Condition Name	The conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	
Shell Profile	Displays the authorization profile that will be applied when the corresponding rule is matched. When you enable the TrustSec feature, you can customize rule results; a rule can determine the access permission of an endpoint, the security group of that endpoint, or both. The columns that appear reflect the customization settings.
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. When you enable the TrustSec feature, you can also choose the set of rule results; only session authorization profiles, only security groups, or both. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Configuring Network Access Authorization Rule Properties

Use this page to create, duplicate, and edit the rules to determine access permissions in a network access service.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Access Policies > Access Services > <*service*> > Authorization**, and click **Create, Edit,** or **Duplicate**.

Step 2 Complete the fields as described in Table 10-16:

Table 10-16 Network Access Authorization Rule Properties Page

Option	Description
General	
Name	The name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
<*condition(s)*>	The conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-42.
Results	
Authorization Profiles	A list of available and selected profiles. You can choose multiple authorization profiles to apply to a request. See Processing Rules with Multiple Authorization Profiles, page 3-16 for information about the importance of authorization profile order when resolving conflicts.
Security Group	(TrustSec only) The security group to apply. **Note** When you enable TrustSec, you can customize the results options to display only session authorization profiles, only security groups, or both.

Configuring Device Administration Authorization Policies

A device administration authorization policy determines the authorizations and permissions for network administrators.

You create an authorization policy during access service creation. See Configuring General Access Service Properties, page 10-14 for details of the Access Service Create page.

Use this page to:

- View rules.
- Delete rules.
- Open pages that enable you to create, duplicate, edit, and customize rules.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Select **Access Policies > Access Services > <*service*> > Authorization**.

The Device Administration Authorization Policy page appears as described in Table 10-17.

Table 10-17 Device Administration Authorization Policy Page

Option	Description
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	The name of the rule.
Conditions	The conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the shell profiles and command sets that will be applied when the corresponding rule is matched. You can customize rule results; a rule can apply shell profiles, or command sets, or both. The columns that appear reflect the customization settings.
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.

Table 10-17 Device Administration Authorization Policy Page (continued)

Option	Description
Customize button	Opens the Customize page in which you choose the types of conditions and results to use in policy rules. The Conditions and Results columns reflect your customized settings. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Configuring Device Administration Authorization Rule Properties

Use this page to create, duplicate, and edit the rules to determine authorizations and permissions in a device administration access service.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Select **Access Policies > Access Services > <*service*> > Authorization**, and click **Create, Edit,** or **Duplicate**.

The Device Administration Authorization Rule Properties page appears as described in Table 10-18.

Table 10-18 Device Administration Authorization Rule Properties Page

Option	Description
General	
Name	The name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
<*condition(s)*>	The conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-42.

Table 10-18 Device Administration Authorization Rule Properties Page (continued)

Option	Description
Results	
Shell Profiles	The shell profile to apply for the rule.
Command Sets	A list of available and selected command sets. You can choose multiple command sets to apply.

Configuring Device Administration Authorization Exception Policies

You can create a device administration authorization exception policy for a defined authorization policy. Results from the exception rules always override authorization policy rules.

Use this page to:

- View exception rules.
- Delete exception rules.
- Open pages that create, duplicate, edit, and customize exception rules.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Select **Access Policies > Access Services > <*service*> > Authorization,** and click **Device Administration Authorization Exception Policy**.

The Device Administration Authorization Exception Policy page appears as described in Table 10-19.

Table 10-19 Device Administration Authorization Exception Policy Page

Option	Description
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	The name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:<*name*>	Network device group. The two predefined NDGs are Location and Device Type.
Condition Name	The conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.

Table 10-19 Device Administration Authorization Exception Policy Page (continued)

Option	Description
Results	Displays the shell profile and command sets that will be applied when the corresponding rule is matched. You can customize rule results; a rule can determine the shell profile, the command sets, or both. The columns that appear reflect the customization settings.
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions and results as in the corresponding authorization policy. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Configuring Shell/Command Authorization Policies for Device Administration

When you create an access service and select a service policy structure for Device Administration, ACS automatically creates a shell/command authorization policy. You can then create and modify policy rules.

The web interface supports the creation of multiple command sets for device administration. With this capability, you can maintain a smaller number of basic command sets. You can then choose the command sets in combination as rule results, rather than maintaining all the combinations themselves in individual command sets.

You can also create an authorization policy with an exception policy, which can override the standard policy results. See Configuring Authorization Exception Policies, page 10-36.

For information about how ACS processes rules with multiple command sets, see Processing Rules with Multiple Command Sets, page 3-10.

To configure rules, see:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Configuring Authorization Exception Policies

An authorization policy can include exception policies. In general, exceptions are temporary policies; for example, to grant provisional access to visitors or increase the level of access to specific users. Use exception policies to react efficiently to changing circumstances and events.

The results from the exception rules always override the standard authorization policy rules.

You create exception policies in a separate rule table from the main authorization policy table. You do not need to use the same policy conditions in the exception policy as you used in the corresponding standard authorization policy.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To access the exception policy rules page:

Step 1 Select **Access Policies > Service Selection Policy <*service*> > <*authorization policy*>**, where <*service*> is the name of the access service, and <*authorization policy*> is the session authorization or shell/command set authorization policy.

Step 2 In the Rule-Based Policy page, click the **Exception Policy** link above the rules table.

The Exception Policy table appears with the fields described in Table 10-20:

Table 10-20 Network Access Authorization Exception Policy Page

Option	Description
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	The name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:<*name*>	Network device group. The two predefined NDGs are Location and Device Type.
Condition Name	The conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the authorization profile that will be applied when the corresponding rule is matched. When you enable the TrustSec feature, you can customize rule results; a rule can determine the access permission of an endpoint, the security group of that endpoint, or both. The columns that appear reflect the customization settings.
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions as in the corresponding authorization policy. When you enable the TrustSec feature, you can also choose the set of rule results; only session authorization profiles, only security groups, or both. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

To configure rules, see:

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Related Topics

- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Creating Policy Rules

When you create rules, remember that the order of the rules is important. When ACS encounters a match as it processes the request of a client that tries to access the ACS network, all further processing stops and the associated result of that match is found. No further rules are considered after a match is found.

The Default Rule provides a default policy in cases where no rules are matched or defined. You can edit the result of a default rule.

Before You Begin

- Configure the policy conditions and results. See Managing Policy Conditions, page 9-1.
- Select the types of conditions and results that the policy rules apply. See Customizing a Policy, page 10-5.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create a new policy rule:

Step 1 Select **Access Policies > Service Selection Policy *<service>* > *<policy>***, where <*service*> is the name of the access service, and <*policy*> is the type of policy. If you:

- Previously created a rule-based policy, the Rule-Based Policy page appears, with a list of configured rules.
- Have not created a rule-based policy, the Simple Policy page appears. Click **Rule-Based**.

Step 2 In the Rule-Based Policy page, click **Create**.

The Rule page appears.

Step 3 Define the rule.

Step 4 Click **OK**, and the Policy page appears with the new rule.

Step 5 Click **Save Changes** to save the new rule.

To configure a simple policy to use the same result for all requests that an access service processes, see:

- Viewing Identity Policies, page 10-21
- Configuring a Group Mapping Policy, page 10-26
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring a Session Authorization Policy for Network Access, page 10-29
- Configuring Shell/Command Authorization Policies for Device Administration, page 10-36

Related Topics

- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Duplicating a Rule

You can duplicate a rule if you want to create a new rule that is the same, or very similar to, an existing rule. The duplicate rule name is based on the original rule with parentheses to indicate duplication; for example, Rule-1(1).

After duplication is complete, you access each rule (original and duplicated) separately.

Note You cannot duplicate the Default rule.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To duplicate a rule:

Step 1 Select **Access Policies > Service Selection Policy > *<service>* > *<policy>***, where <*service*> is the name of the access service, and <*policy*> is the type of policy.

The Policy page appears with a list of configured rules.

Step 2 Check the check box next to the rule that you want to duplicate. You cannot duplicate the Default Rule.

Step 3 Click **Duplicate**.

The Rule page appears.

Step 4 Change the name of the rule and complete the other applicable field options.

Step 5 Click **OK**, and the Policy page appears with the new rule.

Step 6 Click **Save Changes** to save the new rule.

Related Topics

- Creating Policy Rules, page 10-39
- Editing Policy Rules, page 10-40
- Deleting Policy Rules, page 10-41

Editing Policy Rules

You can edit all values of policy rules; you can also edit the result in the Default rule.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To edit a rule:

Step 1 Select **Access Policies > Service Selection Policy > <*service*> > <*policy*>**, where <*service*> is the name of the access service, and <*policy*> is the type of policy.

The Policy page appears, with a list of configured rules.

Step 2 Click the rule name that you want to modify; or, check the check box for the Name and click **Edit**.

The Rule page appears.

Step 3 Edit the appropriate values.

Step 4 Click **OK**, and the Policy page appears with the edited rule.

Step 5 Click **Save Changes** to save the new configuration.

Related Topics

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Deleting Policy Rules, page 10-41

Deleting Policy Rules

Note You cannot delete the Default rule.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To delete a policy rule:

Step 1 Select **Access Policies > Service Selection Policy > <*service*> > <*policy*>**, where <*service*> is the name of the access service, and <*policy*> is the type of policy.

The Policy page appears, with a list of configured rules.

Step 2 Check one or more check boxes next to the rules that you want to delete.

Step 3 Click **Delete**.

The Policy page appears without the deleted rule(s).

Step 4 Click **Save Changes** to save the new configuration.

Related Topics

- Creating Policy Rules, page 10-39
- Duplicating a Rule, page 10-40
- Editing Policy Rules, page 10-40

Configuring Compound Conditions

Use compound conditions to define a set of conditions based on any attributes allowed in simple policy conditions. You define compound conditions in a policy rule page; you cannot define them as separate condition objects.

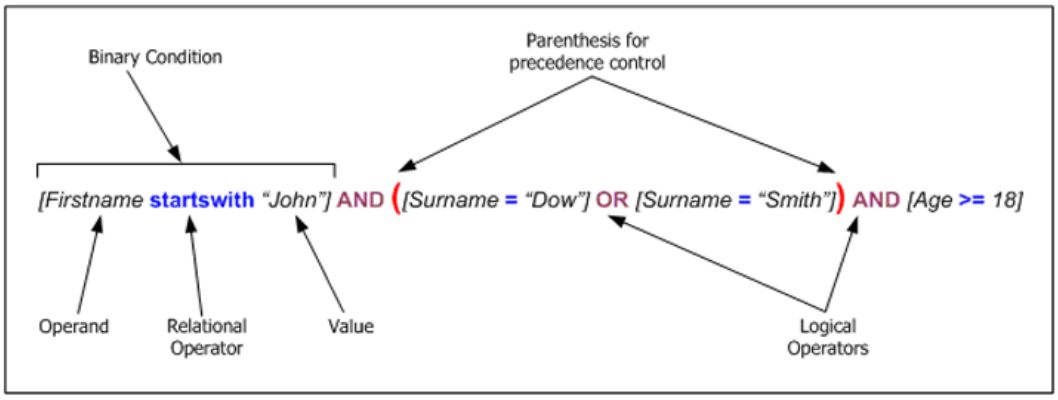
This section contains the following topics:

- Compound Condition Building Blocks, page 10-42
- Types of Compound Conditions, page 10-43
- Using the Compound Expression Builder, page 10-45

Compound Condition Building Blocks

Figure 10-1 shows the building blocks of a compound condition.

Figure 10-1 Building Blocks of a Compound Condition



- **Operands**—Any attribute or condition type, such as Protocol/Request Attributes, Identity Attributes, Identity Groups, Network Device Groups (NDGs), Date/Time, and Custom or Standard Conditions.
- **Relational Operators**—Operators that specify the relation between an operand and a value; for example, equals (=), or does not match. The operators that you can use in any condition vary according to the type of operand.
- **Binary condition**—A binary condition defines the relation between a specified operand and value; for example, [username = "Smith"].

- **Logical Operators**—The logical operators operate on or between binary conditions. The supported logical operators are AND and OR.
- **Precedence Control**—You can alter the precedence of logical operators by using parentheses. Nested parentheses provide administrator control of precedence. The natural precedence of logical operators, that is, without parenthesis intervention, is NOT, AND, OR, where NOT has the highest precedence and OR the lowest.

Related Topics

- Types of Compound Conditions, page 10-43
- Using the Compound Expression Builder, page 10-45

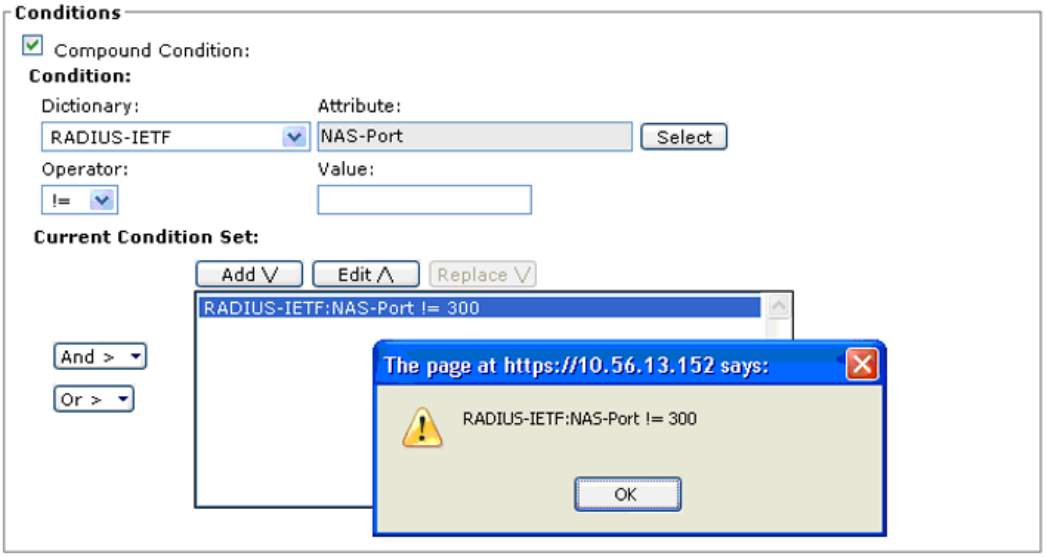
Types of Compound Conditions

You can create three types of compound conditions:

Atomic Condition

Consists of a single predicate and is the only entry in the list. Because all simple conditions in a rule table, except for NDGs, assume the equals (=) operation between the attribute and value, the atomic condition is used to choose an operator other than equals (=). See Figure 10-2 for an example.

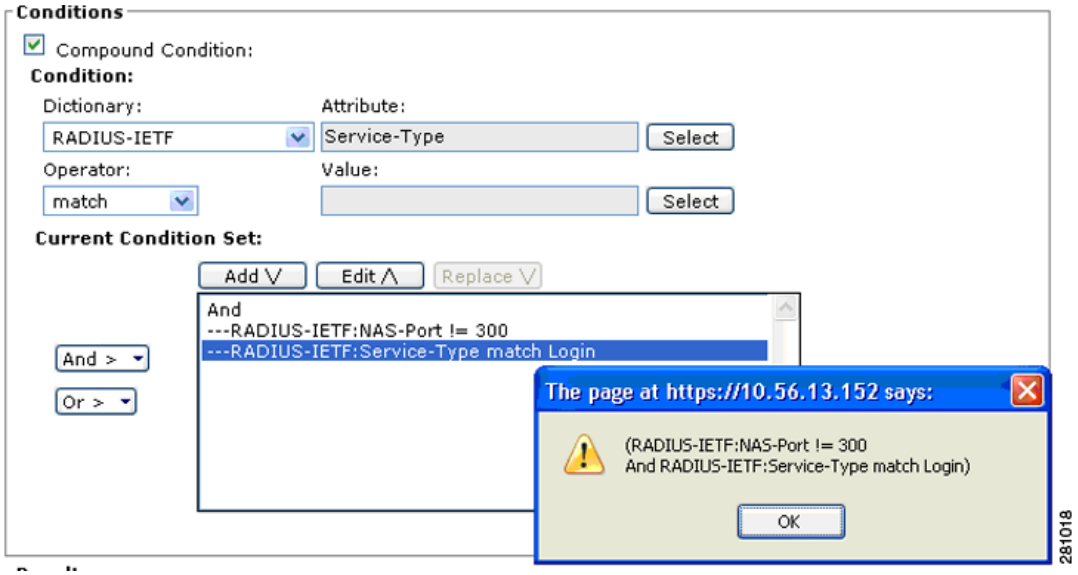
Figure 10-2 Compound Expression - Atomic Condition



Single Nested Compound Condition

Consists of a single operator followed by a set of predicates (>=2). The operator is applied between each of the predicates. See Figure 10-3 for an example. The preview window displays parentheses [()] to indicate precedence of logical operators.

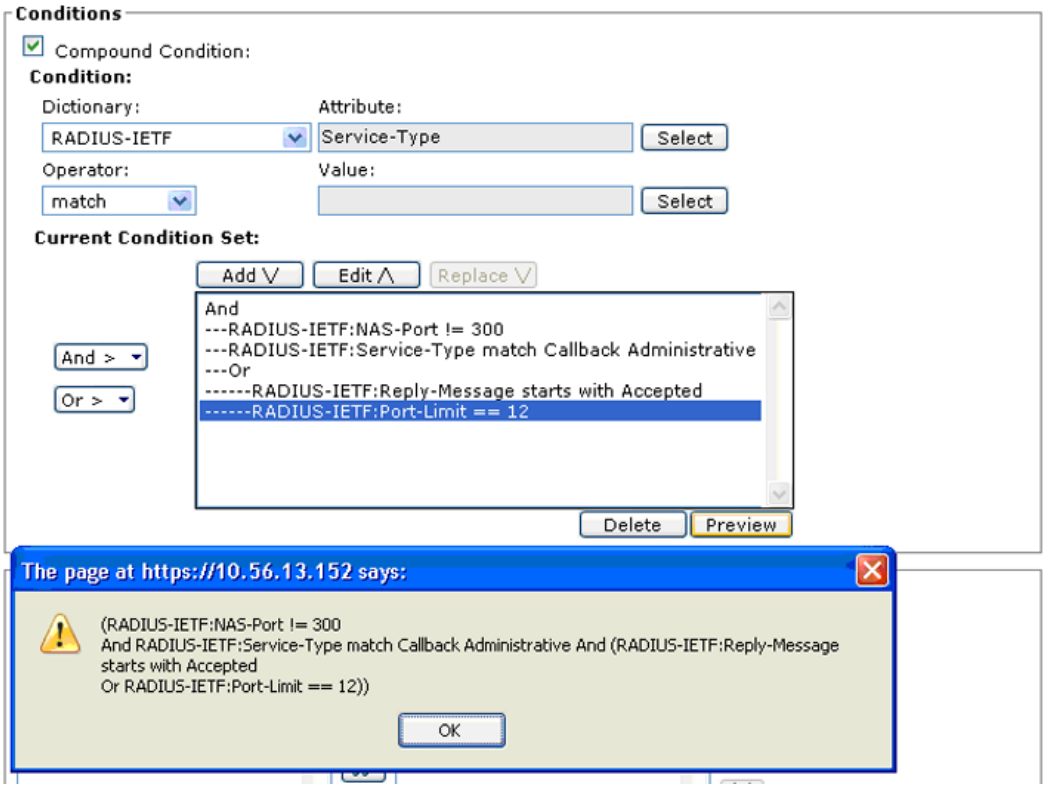
Figure 10-3 Single Nested Compound Expression



Multiple Nested Compound Condition

You can extend the simple nested compound condition by replacing any predicate in the condition with another simple nested compound condition. See Figure 10-4 for an example. The preview window displays parentheses [()] to indicate precedence of logical operators.

Figure 10-4 Multiple Nested Compound Expression



Related Topics

- Compound Condition Building Blocks, page 10-42
- Using the Compound Expression Builder, page 10-45

Using the Compound Expression Builder

You construct compound conditions by using the expression builder in Rule Properties pages. The expression builder contains two sections: a predicate builder to create primary conditions and controls for managing the expression.

In the first section, you define the primary conditions; choose the dictionary and attribute to define the operand, then choose the operator, and specify a value for the condition. Use the second section to organize the order of conditions and the logical operators that operate on or between binary conditions.

Table 10-21 describes the fields in the compound expression builder.

Table 10-21 Expression Builder Fields

Field	Description
Condition	Use this section to define the primary conditions.
Dictionary	**Specifies the dictionary from which to take the operand. These available options depend on the policy that you are defining. For example, when you define a service selection policy, the Identity dictionaries are not available.**

Table 10-21 Expression Builder Fields (continued)

Field	Description
Attribute	**Specifies the attribute that is the operand of the condition. The available attributes depend on the dictionary that you chose.**
Operator	**The relational operator content is dynamically determined according to the choice in the preceding operand field.**
Value	**The condition value. The type of this field depends on the type of condition or attribute.**
Current Condition Set	Use this section to organize the order of conditions and the logical operators that operate on or between binary conditions.
Condition list	Displays a list of defined binary conditions for the compound conditions and their associated logical operators.
Add	**After you define a binary condition, click Add to add it to the Condition list.**
Edit	**To edit a binary condition, select the condition in the Condition list and click Edit. The condition properties appear in the Condition fields. Modify the condition as required, then click Replace.**
Replace	**Click to replace the selected condition with the condition currently defined in the Condition fields.**
And Or	**Specifies the logical operator on a selected condition, or between the selected condition and the one above it. Click the appropriate operator, and click Insert to add the operator as a separate line; click the operator and click Replace, to replace the selected line.**
Delete	Click to delete the selected binary condition or operator from the condition list.
Preview	Click to display the current expression in corresponding parenthesis representation. The rule table displays the parenthesis representation after the compound expression is created.

Related Topics

- Compound Condition Building Blocks, page 10-42
- Types of Compound Conditions, page 10-43

TrustSec Access Control Pages

This section contains the following topics:

- Egress Policy Matrix Page, page 10-47
- Editing a Cell in the Egress Policy Matrix, page 10-47
- Defining a Default Policy for Egress Policy Page, page 10-48
- NDAC Policy Page, page 10-49
- NDAC Policy Properties Page, page 10-51
- Network Device Access EAP-FAST Settings Page, page 10-52

Egress Policy Matrix Page

The Egress policy, also known as an SGACL policy, determines which SGACLs to apply at the Egress points of the network, based on the source and destination SGTs. ACS presents the Egress policy as a matrix; it displays all the security groups in the source and destination axes. Each cell in the matrix can contain a set of ACLs to apply to the corresponding source and destination SGTs.

The network devices add the default policy to the specific policies that you defined for the cells. For empty cells, only the default policy applies.

Use the Egress policy matrix to view, define, and edit the sets of ACLs to apply to the corresponding source and destination SGTs.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To display this page, choose **Access Policies > TrustSec Access Control > Egress Policy**.

Table 10-22 Egress Policy Matrix Page

Option	Description
Destination Security Group	Column header displaying all destination security groups.
Source Security Group	Row header displaying all source security groups.
Cells	Contain the SGACLs to apply to the corresponding source and destination security group.
Edit	Click a cell, then click Edit to open the Edit dialog box for that cell. See Editing a Cell in the Egress Policy Matrix, page 10-47.
Default Policy	Click to open a dialog box to define the default Egress policy. See Defining a Default Policy for Egress Policy Page, page 10-48.
Set Matrix View	To change the Egress policy matrix display, choose an option, then click **Go**: • All—Clears all the rows and columns in the Egress policy matrix. • Customize View—Launches a window where you can customize source and destination security groups corresponding to the selected cell.

Related Topic

- Creating an Egress Policy, page 4-26

Editing a Cell in the Egress Policy Matrix

Use this page to configure the policy for the selected cell. You can configure the SGACLs to apply to the corresponding source and destination security group.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To display this page, choose **Access Policies > TrustSec Access Control > Egress Policy**, select a cell, then click **Edit**.

Table 10-23 Edit Cell Page

Option	Description
Configure Security Groups	*Display only.* Displays the source and destination security group name for the selected cell.
General	A description for the cell policy.
ACLs	Move the SGACLs that you want to apply to the corresponding source and destination security group from the Available list to the Selected list. To specify the order of the list of SGACLs, use the Up (^) and Down (v) arrows.

Related Topic

- Creating an Egress Policy, page 4-26

Defining a Default Policy for Egress Policy Page

Use this page to define the default Egress policy. The network devices add the default policy to the specific policies defined for the cells. For empty cells, only the default policy applies.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To display this page, choose **Access Policies > TrustSec Access Control > Egress Policy**, then click **Default Policy**.

Table 10-24 Default Policy Page

Option	Description
ACLs	Move the SGACLs that you want to apply to the corresponding source and destination security group from the Available list to the Selected list. To specify the order of the list of SGACLs, use the Up (^) and Down (v) arrows. Select Permit All or Deny All as a final catch-all rule.

Related Topics

- Creating an Egress Policy, page 4-26
- Creating a Default Policy, page 4-27

NDAC Policy Page

The Network Device Admission Control (NDAC) policy determines the SGT for network devices in a TrustSec environment. The NDAC policy handles:

- Peer authorization requests from one device about its neighbor.
- Environment requests (a device is collecting information about itself).

The policy returns the same SGT for a specific device, regardless of the request type.

Note You do not add an NDAC policy to an access service; it is implemented by default. However, for endpoint admission control, you must define an access service and session authorization policy. See Configuring Network Access Authorization Rule Properties, page 10-32, for information about creating a session authorization policy.

Use this page to configure a simple policy that assigns the same security group to all devices, or configure a rule-based policy.

To display this page, choose **Access Policies > TrustSec Access Control > Network Device Access > Authentication Policy**.

If you have already configured an NDAC policy, the corresponding Simple Policy page or Rule-based Policy page opens; otherwise, the Simple Policy page opens by default.

Simple Policy Page

Use this page to define a simple NDAC policy.

Table 10-25 Simple NDAC Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies that the result applies to all requests. • Rule-based—Configure rules to apply different results depending on the request. **Note** If you switch between policy types, you will lose your previously saved policy configuration.
Security Group	Select the security group to assign to devices. The default is Unknown.

Rule-Based Policy Page

Use this page for a rule-based policy to:

- View rules.
- Delete rules.
- Open pages that create, duplicate, edit, and customize rules.

Table 10-26 Rule-Based NDAC Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the result to apply to all requests. • Rule-based—Configure rules to apply different results depending on the request. **Note** If you switch between policy types, you will lose your previously saved policy configuration.
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	The name of the rule. The Default Rule is available for conditions for which: • Enabled rules are not matched. • Rules are not defined. Click a link to edit or duplicate a rule. You can edit the Default Rule but you cannot delete, disable, or duplicate it.
Conditions	The conditions that you can use to define policy rules. To change the display of rule conditions, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the security group assigned to the device when it matches the corresponding condition.
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions as in the corresponding authorization policy. ⚠ **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.

Related Topics:

- Configuring an NDAC Policy, page 4-24
- NDAC Policy Properties Page, page 10-51

NDAC Policy Properties Page

Use this page to create, duplicate, and edit rules to determine the SGT for a device.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To display this page, choose **Access Policies > TrustSec Access Control > Network Device Access > Authentication Policy**, then click **Create, Edit,** or **Duplicate**.

Note For endpoint admission control, you must define an access service and session authorization policy. See Configuring Network Access Authorization Rule Properties, page 10-32 for information about creating a session authorization policy.

Table 10-27 NDAC Policy Properties Page

Option	Description
General	
Name	The name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
<condition(s)>	The conditions that you can configure for the rule. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then enter the value. If compound expression conditions are available, when you check Compound Expression, an expression builder appears. For more information, see Configuring Compound Conditions, page 10-42. To change the list of conditions for the policy, click the Customize button in the NDAC Policy Page, page 10-49.
Results	
Security Group	Select the security group to assign to the device when it matches the corresponding conditions.

Related Topics:

- Configuring an NDAC Policy, page 4-24
- NDAC Policy Page, page 10-49

Network Device Access EAP-FAST Settings Page

Use this page to configure parameters for the EAP-FAST protocol that the NDAC policy uses.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To display this page, choose **Access Policies > TrustSec Access Control > Network Device Access.**

Table 10-28 Network Device Access EAP-FAST Settings Page

Option	Description
EAP-FAST Settings	
Tunnel PAC Time To Live	The time to live (TTL), or duration, of a PAC before it expires and requires replacing.
Proactive PAC Update When % of PAC TTL is Left	The percentage of PAC TTL remaining when you should update the PAC.

Related Topics:

- Configuring an NDAC Policy, page 4-24
- Configuring EAP-FAST Settings for TrustSec, page 4-24
- NDAC Policy Page, page 10-49

CHAPTER 11

Monitoring and Reporting in ACS

The Monitoring and Reports drawer appears in the primary web interface window and contains the Launch Monitoring & Report Viewer option.

The Monitoring & Report Viewer provides monitoring, reporting, and troubleshooting capabilities for the ACS servers in your network. You can extract consolidated log, configuration, and diagnostic data from one or more ACS servers for advanced reporting and troubleshooting purposes.

You can configure the network access devices (NADs) in your network to send syslog messages to the Monitoring & Report Viewer. To do this, you must configure the logging port on the NAD to UDP 20514. For example, to enable a NAD in your network to send syslog messages to the Monitoring & Report Viewer, you must enter the following commands on the NAD through the CLI configuration mode:

1. **logging monitor informational**
2. **logging origin-id ip**
3. **logging host** *ip* **transport udp port 20514—**where *ip* is the IP address of the Log Collector in your network.
4. **epm logging**

The following types of syslog messages are supported by ACS Monitoring and Reports Viewer:

- AUTHMGR-5-START
- AUTHMGR-5-SUCCESS
- AUTHMGR-5-FAIL
- AUTHMGR-5-SECURITY_VIOLATION
- AUTHMGR-7-FAILOVER
- AUTHMGR-7-NOMOREMETHODS
- AUTHMGR-7-RESULT
- DOT1X-5-SUCCESS
- DOT1X-5-FAIL
- MAB-5-SUCCESS
- MAB-5-FAIL
- RADIUS-4-RADIUS_DEAD
- RADIUS-4-RADIUS_ALIVE
- EPM-6-POLICY_APP_SUCCESS
- EPM-4-POLICY_APP_FAILURE

- AUTHMGR-SP-5-VLANASSIGN
- AUTHMGR-5-VLANASSIGN
- DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND

Click **Launch Monitoring & Report Viewer** to open the Monitoring and Reports Viewer in a secondary web interface window, which contains these drawers:

- Monitoring and Reports
- Monitoring Configuration. (See Managing System Operations and Configuration in the Monitoring & Report Viewer, page 15-1.)

The Monitoring and Reports drawer provides the following functionality:

- Dashboard—Provides a high-level summary, updated in real time, of the ACS servers in the deployment, the authentication activity, and a summary of authentications against each identity store. See Dashboard Pages, page 11-3.
- Alarms—You can define thresholds to represent acceptable system performance. Measurements are taken on an ongoing basis and compared against these thresholds. If the thresholds are exceeded, alarms are generated. See Understanding Alarms, page 12-1.
- Reports— A rich set of reports are available. See Managing Reports.
- Troubleshooting— Provides tools to assist in troubleshooting the ACS system, including tests for system connectivity and a tool to download support bundles. See Troubleshooting ACS with the Monitoring & Report Viewer.
- Support for non-English characters (UTF-8)—You can have non-English characters in:
  - Syslog messages—Configurable attribute value, user name, and ACS named configuration objects
  - GUI input fields
  - Query pages
  - Reports and Interactive Viewer
  - Alarms
  - Dashboard lookup
  - Failure reason text

Note In Monitoring and Reports drawer pages, you can use the page area's down arrow (v) to hide an area's content, and the right arrow (>) to show its content.

Related Topic

- Authentication Records and Details, page 11-2

Authentication Records and Details

A primary source of information for reports are the authentication records. Reports are provided that analyze these records according to multiple categories such as the Access Service used for the request, the user or host referenced in the request, the device making the request, etc. ACS provides summaries of the authentications per instance in each category, and administrators can get additional details.

Within each authentication record there is an option to view the details of the authentication record. The details contain the following information:

- Authentication Details—Full details of the authentication, which includes details from the request, the service, policies and rules selected for the requests, and the results returned in the response.
- Authentication Result—The contents of the result response.
- Steps—Lists the sequence of steps performed when processing the request.

The authentication details information is very helpful when trying to understand why a specific successful response was returned, or to track the steps performed when a failed response was returned.

Dashboard Pages

When you launch the Monitoring & Report Viewer, the Dashboard appears in a secondary web interface window.

ACS 5.1 provides a new customizable dashboard that contains tabs and portlets, where the Monitoring & Report Viewer consolidates your favorite queries, recent alarms and reports, and health status of ACS instances. Each of these tabs can have multiple portlets with each portlet containing an application of your choice. You can select an application from the list the list of available applications. By default, the Monitoring & Report Viewer provides the following tabs and applications in the Dashboard:

Note These tabs are customizable, and you can modify or delete the following tabs.

- General—The General tab lists the following:
  - Five most recent alarms—When you click the name of the alarm, a dialog box appears with the details and the status of the alarm. You can update the information in the Status tab of this dialog box to track the alarm. See Table 12-5 for a description of the fields in the Status tab.
  - Favorite reports—The favorite reports are displayed in alphabetical order. To view a report, click the name of the report. You can view this report in the Interactive Viewer. You can customize this list to include your favorite reports and can quickly launch them from the dashboard.
- Troubleshooting—The Troubleshooting tab contains the following panes:
  - Live Authentications—View live authentications for the day. You can filter the records that appear in this pane.
  - My Links—You can add your favorite links to this pane.
  - NAD Show Command—You can run any show command on any NAD device from this pane. To run a NAD show command, you must:

    Enter the IP address of the NAD (Required).

    Enter the username and password for the NAD.

    Choose the protocol, Telnet or SSHv2 (Required).

    Enter the port number. The default is 23 (Required).

    Enter the enable password.

    Check the Use Console Server check box if you want to use the console server.

    Enter the IP address of the console server—This field is required if you check the Use Console Server check box.

Enter the show command that you want to execute on the NAD (Required).

When the Monitoring & Report Viewer executes the NAD show command, it might sometimes prompt you for additional details. See Table 14-5 for a description of the fields in the Progress Details page. After you click **Done** , you can click **Show Results Summary** to view the result as shown in Table 14-6.

- Authentication Lookup—You can use this portlet to run an authentication report with default parameters, find authentication records for a user or MAC address, and run user or endpoint summary report for a user or end point respectively. For more information on the Authentication Lookup Portlet, see Working with Authentication Lookup Portlet, page 11-5.

- Authentication Trends—The Authentication Trends tab contains the following panes:
  - Authentication Trend—Provides a graphical and tabular representation of the authentication trend for up to the past 30 days. In the graphical representation, the time is plotted on the X-axis and the authentications are plotted on the Y-axis. The tabular representation provides the number of passed, failed, and dropped authentications for each day. The button at the lower-right corner of the chart ( )allows you to toggle between the two views.
  - Top <N> Authentications—Provides a graphical representation of the top <N> authentications. Time is plotted on the X-axis and authentications are plotted on the Y-axis.
  - Authentication Snapshot—Provides a snapshot of authentications in the graphical and tabular formats for up to the past 30 days. In the graphical representation, the field based on which the records are grouped together is plotted on the X-axis and the authentications are plotted on the Y-axis. The tabular representation provides the Category; Pass Count; Daily, Weekly, or Monthly Pass Count; Fail Count; and Daily, Weekly, or Monthly Fail Count. The button at the lower-right corner of the chart ( ) allows you to toggle between the two views.
- ACS Health—The ACS Health tab provides the system and AAA health of ACS instances. This information is available in a tabular format.
  - System status is determined by the following parameters—CPU utilization, memory utilization, disk input/output utilization, and disk usage for /opt and /local disk.
  - AAA status is determined by RADIUS and TACACS+ latency

  Hovering the mouse over the legend (Critical, Warning, Healthy) provides the criteria that determines the status of the ACS instance. For a detailed graphical representation of the ACS instance health, click the name of the ACS instance. The ACS health summary report appears. You can view this report in the Interactive Viewer.

You can configure the tabs in the Dashboard to suit your needs. See Configuring Tabs in the Dashboard, page 11-6 for more information on how to configure tabs in the Dashboard and add applications to the tabs.

Related Topics

- Working with Portlets, page 11-4
- Configuring Tabs in the Dashboard, page 11-6
- Adding Applications to Tabs, page 11-7

Working with Portlets

A portlet is a small, self-contained window within a dashboard that displays information in the form of real-time charts, tabular reports, and so on. Each tab in the Dashboard consists of one or more portlets. Figure 11-1 shows two portlets from the General tab.

Figure 11-1 Portlets

Top 5 Alarms and My Favorite Reports appear in separate windows. You can edit each of these portlets separately.

To edit a portlet, click the edit button ( ) at the upper-right corner of the window. The Monitoring & Report Viewer allows you to customize the information in the portlets to suit your needs. You can add, edit, and delete tabs; edit application settings in portlets; and delete portlets.

Working with Authentication Lookup Portlet

The Authentication Lookup Portlet contains the following fields:

- Username/MAC Address—(Required for summary reports) Username of the user or the MAC address in aa-bb-cc-dd-ee-ff format. The Monitoring & Report Viewer does not accept MAC address in any other format.
- View—Choose Authentication to run an authentication report or Summary for a summary report.
- Time Range—Depending on the View option that you choose, the Time Range drop-down list box is populated. Choose the time range for which you want to generate the report.
- Start Date—(Enabled when you choose the Custom time range option) Choose the start date.
- End Date—(Enabled when you choose the Custom time range option) Choose the end date.
- Protocol—Choose either RADIUS or TACACS+ from the Protocol drop-down list box. The protocol is not taken into account for endpoint summary reports.

Related Topic

- Dashboard Pages, page 11-3
- Running Authentication Lookup Report, page 11-6

Running Authentication Lookup Report

When you run an Authentication Lookup report, consider the following:

- If you have provided the Username or MAC Address value in the format aa-bb-cc-dd-ee-ff, an authentication report is run for this MAC address.
- If you have provided the Username or MAC Address value in any other format, the value is considered an username and authentication report is run for that user.
- If the Username or MAC Address field is empty, an authentication report with default parameters is run for the chosen protocol and time range (similar to running a RADIUS or TACACS Authentication report in the catalog pages).
- If you provide a valid MAC Address value for the Username or MAC Address field and choose the Summary View option, an endpoint summary report is run. Irrespective of the protocol that you choose, an endpoint summary report is always run for the RADIUS protocol.

If the MAC Address value that you provide is not in the prescribed format, it is assumed to be a username and a user authentication summary report is run for the chosen time range and protocol.

Configuring Tabs in the Dashboard

This section describes how to configure tabs in the Dashboard and add applications to it. This section contains:

- Adding Tabs to the Dashboard, page 11-6
- Renaming Tabs in the Dashboard, page 11-7
- Changing the Dashboard Layout, page 11-7
- Deleting Tabs from the Dashboard, page 11-8

Adding Tabs to the Dashboard

The Monitoring & Report Viewer Dashboard allows you to customize the tabs in the dashboard and the applications that are available from them. To add tabs to the Dashboard:

Step 1 From the Monitoring & Report Viewer, choose **Monitoring and Reports > Dashboard**.

The Dashboard page appears.

Step 2 Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.

Step 3 Click **Add New Page**.

Step 4 Enter the name of the tab that you want to create in the Add New Page text box.

Step 5 Click **Add Page**.

A new tab of your choice is created. You can add the applications that you most frequently monitor in this tab

Adding Applications to Tabs

To add an application to a tab:

Step 1 From the Monitoring & Report Viewer > choose **Monitoring and Reports > Dashboard**.

The Dashboard page appears.

Step 2 Select the tab to which you want to add an application.

Note If you want to add applications to a new tab, you must add the new tab to the Dashboard before you can add applications to it.

Step 3 Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.

Step 4 Click **Add Application**.

An Add Application window appears.

Step 5 Click **View Dashboard** to see the list of applications that you can add to the Dashboard. Alternatively, you can enter the name of the application in the Search Content text box.

A list of applications appears.

Step 6 Click the Add link next to the application that you want to add.

The application of your choice is added to the tab. You can edit the parameters in this tab.

Renaming Tabs in the Dashboard

To rename existing tabs in the Dashboard:

Step 1 From the Monitoring & Report Viewer > choose **Monitoring and Reports > Dashboard.**

The Dashboard page appears.

Step 2 Select the tab that you want to rename.

Step 3 Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.

Step 4 Click **Rename Page**.

Step 5 Enter the new name in the Rename Page text box.

Step 6 Click **Update**.

The tab appears with the new name.

Changing the Dashboard Layout

You can change the look and feel of the Dashboard. ACS provides you with nine different in-built layouts. To choose a different layout:

Step 1 From the Monitoring & Report Viewer, choose **Monitoring and Reports > Dashboard**.

The Dashboard page appears.

Step 2 Select the tab whose layout you wish to change.

Step 3 Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.

A list of layout options appears.

Step 4 Click the radio button next to the layout style that you want for this tab.

Step 5 Click **Save** to change the layout.

Deleting Tabs from the Dashboard

To delete tabs from the Dashboard:

Step 1 From the Monitoring & Report Viewer, choose **Monitoring and Reports > Dashboard.**

The Dashboard page appears.

Step 2 Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.

Step 3 Click **Manage Pages**.

Step 4 Select the tab that you want to delete in the **Page Display Order** list box.

Step 5 Click to delete the tab that you have selected.

Timesaver Alternatively, when you hover the mouse over the name of the tab that you want to delete, the following icon appears: . Click this icon to delete the tab.

CHAPTER 12

Managing Alarms

The Monitoring feature in ACS generates alarms to notify you of critical system conditions. The monitoring component retrieves data from ACS. You can configure thresholds and rules on this data to manage alarms. Alarm notifications are displayed in the web interface and you can get a notification of events through e-mail and Syslog messages. ACS filters duplicate alarms by default.

This chapter contains the following sections:

- Understanding Alarms, page 12-1
- Viewing and Editing Alarms in Your Inbox, page 12-3
- Understanding Alarm Schedules, page 12-7
- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Deleting Alarm Thresholds, page 12-31
- Configuring System Alarm Settings, page 12-31
- Understanding Alarm Syslog Targets, page 12-32

Understanding Alarms

There are two types of alarms in ACS:

- Threshold Alarms, page 12-1
- System Alarms, page 12-2

Threshold Alarms

Threshold alarms are defined on log data collected from ACS servers that notify you of certain events. For example, you can configure threshold alarms to notify you of ACS system health, ACS process status, authentication activity or inactivity, and so on.

You define threshold conditions on these data sets. When a threshold condition is met, an alarm is triggered. While defining the threshold, you also define when the threshold should be applied (the time period), the severity of the alarm, and how the notifications should be sent. Fifteen categories of available alarm thresholds allow you to monitor many different facets of ACS system behavior. See Creating, Editing, and Duplicating Alarm Thresholds, page 12-9 for more information on threshold alarms.

System Alarms

System alarms notify you of critical conditions encountered during the execution of the ACS Monitoring and Reporting viewer. System alarms also provide informational status of system activities, such as data purge events or failure of the log collector to populate the View database. You cannot configure system alarms, which are predefined. However, you do have the option to disable system alarms or decide how you want to be notified if you have enabled them.

This section contains the following topics:

- Evaluating Alarm Thresholds, page 12-2
- Notifying Users of Events, page 12-3

Evaluating Alarm Thresholds

ACS evaluates the threshold conditions based on a schedule. You define these schedules and, while creating a threshold, you assign a schedule to it. A schedule consists of one or more continuous or noncontinuous periods of time during the week.

For example, you can create a schedule that is active from 8:00 a.m. to 5:00 p.m., Monday through Friday. See Understanding Alarm Schedules, page 12-7 for more information. When you assign this schedule to a threshold, ACS evaluates the threshold and generates alarms only during the active period.

ACS evaluates the thresholds periodically depending on the number of thresholds that are currently enabled.

Table 12-1 provides the length of the evaluation cycle for a given number of thresholds.

Table 12-1 Evaluation Cycle of Alarm Thresholds

Number of Enabled Thresholds	Evaluation Cycle[1]
1 to 20	Every 2 minutes
21 to 50	Every 3 minutes
51 to 100	Every 5 minutes

1. If the time taken to evaluate the thresholds increase, then the evaluation cycle increases from 2 to 3 minutes, 3 to 5 minutes, and from 5 to 15 minutes. The evaluation cycle time is reset to 2, 3, and 5 minutes every 12 hours.

When an evaluation cycle begins, ACS evaluates each enabled threshold one after another. If the schedule associated with the threshold allows the threshold to be executed, ACS evaluates the threshold conditions. An alarm is triggered if the condition is met. See Creating, Editing, and Duplicating Alarm Thresholds, page 12-9 for more information.

Note System alarms do not have an associated schedule and are sent immediately after they occur. You can only enable or disable system alarms as a whole.

Notifying Users of Events

When a threshold is reached or a system alarm is generated, the alarm appears in the Alarms Inbox of the web interface. From this page, you can view the alarm details, add a comment about the alarm, and change its status to indicate that it is Acknowledged or Closed. The alarm details in this page, wherever applicable, include one or more links to the relevant reports to help you investigate the event that triggered the alarm.

The Dashboard also displays the five most recent alarms. Alarms that you acknowledge or close are removed from this list in the Dashboard.

ACS provides you the option to receive notifications in the following formats:

- E-mail—Contains all the information that is present in the alarm details page. You can configure a list of recipients to whom this e-mail must be sent. ACS 5.1 provides you the option to receive notification of events through e-mail in HTML format.
- Syslog message—Sent to the Linux or Windows machines that you have configured as alarm syslog targets. You can configure up to two alarm syslog targets.

Viewing and Editing Alarms in Your Inbox

You can view alarms that ACS generates based on a threshold configuration or a rule on a set of data collected from ACS servers. Alarms that have met the configured thresholds are sent to your inbox. After you view an alarm, you can edit the status of the alarm, assign the alarm to an administrator, and add notes to track the event.

To view an alarm in your inbox, select **Monitoring and Reports > Alarms > Inbox**.

The Inbox page appears with a list of alarms that ACS triggered. Table 12-2 describes the fields on the Alarms page. Table 12-3 lists the system alarms in ACS 5.1 and its severity.

Table 12-2 Alarms Page

Option	Description
Severity	*Display only.* Indicates the severity of the associated alarm. Options are: • Critical • Warning • Info
Name	Indicates the name of the alarm. Click to display the Alarms: Properties page and edit the alarm.

Table 12-2 Alarms Page (continued)

Option	Description
Time	*Display only.* Indicates the time of the associated alarm generation in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit representation of the year.
Cause	*Display only.* Indicates the cause of the alarm.
Assigned To	*Display only.* Indicates who is assigned to investigate the alarm.
Status	*Display only.* Indicates the status of the alarm. Options are: • New—The alarm is new. • Acknowledged—The alarm is known. • Closed—The alarm is closed.
Edit	Check the check box next to the alarm that you want to edit, and click **Edit** to edit the status of the alarm and view the corresponding report.
Close	Check the check box next to the alarm that you want to close, and click **Close** to close the alarm. You can enter closing notes before you close an alarm. **Note** Closing an alarm only removes the alarm from the dashboard. It does not delete the alarm.
Delete	Check the check box next to the alarm that you want to delete, and click **Delete** to delete the alarm.

Table 12-3 System Alarms in ACS 5.1

Alarm	Severity
Incremental Backup	
On-demand Full Backup failed: Exception Details.	Critical
Full Database Backup failed. Exception Details.	Critical
Full Database Purge Backup failed. Exception Details.	Critical
Incremental Backup Failed. Exception Details.	Critical
Incremental Restore Successful.	Info
Incremental Restore failed. Reason: Exception Details	Critical
On-demand Full Backup failed: Exception Details	Critical
Full Database Backup failed: Exception Details.	Critical
Full Database Purge Backup failed: Exception Details	Critical

Table 12-3 System Alarms in ACS 5.1 (continued)

Alarm	Severity
Incremental Backup Failed: Exception Details	Critical
Threshold Executor	
Could not complete executing all thresholds in the allocated thresholdEvaluationInterval minute interval. Thresholds will be evaluated again in the next interval. This error could have happened because: The system is under heavy load (example: During Purging) There might be too many thresholds active at this time.	Info
Session Monitor	
Active sessions are over limit. Session is over 250000.	Warning
Syslog Collector Failure	
Please see Collector log for details.	Critical
Scheduled ACS Backup	
Scheduled backup of ACS configuration db failed to start due to invalid character in backup name.	Critical
Scheduled backup of ACS configuration db failed to start due to invalid repository. Please verify that repository exists.	Critical
Unable to get hostname. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical
Failed to load backup library. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical
Symbol lookup error. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical
Failed to perform ACS backup due to internal error. Please check ADE.log for more details.	Critical
Disk Size Check	
Backup of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit backup process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Patch of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit patch installation process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Support bundle of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit support bundle collection process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Backup of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit restore process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Disk Quota	

Table 12-3 System Alarms in ACS 5.1 (continued)

Alarm	Severity
ACS DB size has exceeded allowed quota.	Critical
ACS View DB size has exceeded allowed quota.	Critical
View Data Upgrade	
Database conversion has successfully completed. The View newVersion database has been upgraded to installedVersion and is ready for activation.	Warning
Database conversion did not complete successfully. The View newVersion upgrade process encountered errors and was not able to complete. The upgrade log contains detailed information.	Critical
Others	
Aggregator is busy. Dropping syslog.	Critical
Collector is busy. Dropping syslog.	Critical
Unregistered ACS Server servername.	Warning
Unknown Message code received.	Critical

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To edit an alarm:

Step 1 Select **Monitoring and Reports > Alarms > Inbox**.

The Inbox page appears with a list of alarms that ACS triggered.

Step 2 Check the check box next to the alarm that you want to edit and click **Edit**.

The Inbox - Edit page appears with the following tabs:

- Alarm—This tab provides more information on the event that triggered the alarm. Table 12-4 describes the fields in the Alarm tab. You cannot edit any of the fields in the Alarm tab.

Table 12-4 Inbox - Alarm Tab

Option	Description
Occurred At	Date and time when the alarm was triggered.
Cause	The event that triggered the alarm.
Detail	Additional details about the event that triggered the alarm. ACS usually lists the counts of items that exceeded the specified threshold.
Report Links	Wherever applicable, one or more hyperlinks are provided to the relevant reports that allow you to further investigate the event.
Threshold	Information on the threshold configuration.

- Status—This tab allows you to edit the status of the alarm and add a description to track the event.

Step 3 Modify the fields in the Status tab as required. Table 12-5 describes the fields.

Table 12-5 Inbox - Status Tab

Option	Description
Status	Status of the alarm. When an alarm is generated, its status is New. After you view the alarm, change the status of the alarm to Acknowledged or Closed to indicate the current status of the alarm.
Assigned To	(Optional) Specify the name of the user to whom this alarm is assigned.
Notes	(Optional) Enter any additional information about the alarm that you want to record.

Step 4 Click **Submit** to save the changes.

The Alarms page appears with the changes you made.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Deleting Alarm Thresholds, page 12-31

Understanding Alarm Schedules

You can create alarm schedules to specify when a particular alarm threshold is run. You can create, edit, and delete alarm schedules. You can create alarm schedules to be run at different times of the day during the course of a seven-day week.

By default, ACS comes with the nonstop alarm schedule. This schedule monitors events 24 hours a day, seven days a week.

To view a list of alarm schedules, choose **Monitoring and Reports > Alarms > Schedules**. The Alarm Schedules page appears. Table 12-6 lists the fields in the Alarm Schedules page.

Table 12-6 Alarm Schedules Page

Option	Description
Filter	Enter a search criterion to filter the alarm schedules based on your search criterion.
Go	Click **Go** to begin the search.
Clear Filter	Click **Clear Filter** to clear the search results and list all the alarm schedules.
Name	The name of the alarm schedule.
Description	(Optional) A brief description of the alarm schedule.

This section contains the following topics:

- Creating and Editing Alarm Schedules, page 12-8
- Assigning Alarm Schedules to Thresholds, page 12-8
- Deleting Alarm Schedules, page 12-9

Creating and Editing Alarm Schedules

To create or edit an alarm schedule:

Step 1 Choose **Monitoring and Reports > Alarms > Schedules**.

The Alarm Schedules page appears.

Step 2 Do either of the following:

- Click **Create**.
- Check the check box next to the alarm schedule that you want to edit, then click **Edit**.

The Alarm Schedules - Create or Edit page appears. Table 12-7 lists the fields in the Alarms Schedules - Create or Edit page.

Table 12-7 Alarm Schedules - Create or Edit Page

Option	Description
Identification	
Name	Name of the alarm schedule. The name can be up to 64 characters in length.
Description	A brief description of the alarm schedule; can be up to 255 characters in length.
Schedule	
Click a square to select or deselect that hour. Use the Shift key to select or deselect a block starting from the previous selection. For more information on schedule boxes, see Schedule Boxes, page 5-15.	
Select All	Click **Select All** to create a schedule that monitors for events all through the week, 24 hours a day, 7 days a week.
Clear All	Click **Clear All** to deselect all the selection.
Undo All	When you edit a schedule, click **Undo All** to revert back to the previous schedule.

Step 3 Click **Submit** to save the alarm schedule.

The schedule that you create is added to the Schedule list box in the Threshold pages.

Assigning Alarm Schedules to Thresholds

When you create an alarm threshold, you must assign an alarm schedule for the threshold. To assign an alarm schedule:

Step 1 Choose **Monitoring and Reports > Alarms > Thresholds**.

The Thresholds page appears.

Note This procedure only describes how to assign a schedule to a threshold. For detailed information on how to create, edit, or duplicate a threshold, see Creating, Editing, and Duplicating Alarm Thresholds, page 12-9.

Step 2 Do one of the following.

- Click **Create**.
- Check the check box next to the threshold that you want to edit and click **Edit**.
- Check the check box next to the threshold that you want to duplicate and click **Duplicate**.

Step 3 In the General tab, choose the schedule that you want from the Schedule drop-down list box.

Step 4 Click **Submit** to assign the schedule to the threshold.

Deleting Alarm Schedules

Note Before you delete an alarm schedule, ensure that it is not referenced by any thresholds that are defined in ACS. You cannot delete the default schedule (nonstop) or schedules that are referenced by any thresholds.

To delete an alarm schedule:

Step 1 Choose Monitoring and **Reports > Alarms > Schedules**.

The Alarm Schedules page appears.

Step 2 Check the check box next to the alarm schedule that you want to delete, then click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item(s)?
```

Step 3 Click **Yes** to delete the alarm schedule.

The alarm schedule page appears without the schedule that you deleted.

Creating, Editing, and Duplicating Alarm Thresholds

Use this page to configure thresholds for each alarm category. You can configure up to 100 thresholds.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To configure a threshold for an alarm category:

Step 1 Select **Monitoring and Reports > Alarms > Thresholds**.

The Alarms Thresholds page appears as described in Table 12-8:

Table 12-8 Alarm Thresholds Page

Option	Description
Name	The name of the alarm threshold.
Description	The description of the alarm threshold.
Category	The alarm threshold category. Options can be: • Passed Authentications • Failed Authentications • Authentication Inactivity • TACACS Command Accounting • TACACS Command Authorization • ACS Configuration Changes • ACS System Diagnostics • ACS Process Status • ACS System Health • ACS AAA Health • RADIUS Sessions • Unknown NAD • External DB Unavailable • RBACL Drops • NAD-reported AAA Down
Last Modified Time	The time at which the alarm threshold was last modified by a user.
Last Alarm	The time at which the last alarm was generated by the associated alarm threshold.
Alarm Count	The number of times that an associated alarm was generated.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the alarm that you want to duplicate, then click **Duplicate**.
- Click the alarm name that you want to modify, or check the check box next to the alarm that you want to modify, then click **Edit**.
- Check the check box next to the alarm that you want to enable, then click **Enable**.
- Check the check box next to the alarm that you want to disable, then click **Disable**.

Step 3 Modify fields in the Thresholds page as required. See the following pages for information about valid field options:

- Configuring General Threshold Information, page 12-11
- Configuring Threshold Criteria, page 12-11
- Configuring Threshold Notifications, page 12-29

Step 4 Click **Submit** to save your configuration.

The alarm threshold configuration is saved. The Threshold page appears with the new configuration.

Related Topics

- Configuring General Threshold Information, page 12-11
- Configuring Threshold Criteria, page 12-11
- Configuring Threshold Notifications, page 12-29

Configuring General Threshold Information

To configure general threshold information, fill out the fields in the General Tab of the Thresholds page. Table 12-9 describes the fields.

Table 12-9 General Tab

Option	Description
Name	Name of the threshold.
Description	(Optional) The description of the threshold.
Enabled	Check this check box to allow this threshold to be executed.
Schedule	Use the drop-down list box to select a schedule during which the threshold should be run. A list of available schedules appears in the list.

Related Topics

- Configuring Threshold Criteria, page 12-11
- Configuring Threshold Notifications, page 12-29

Configuring Threshold Criteria

ACS 5.1 provides the following threshold categories to define different threshold criteria:

- Passed Authentications, page 12-12
- Failed Authentications, page 12-14
- Authentication Inactivity, page 12-16
- TACACS Command Accounting, page 12-17
- TACACS Command Authorization, page 12-18
- ACS Configuration Changes, page 12-19
- ACS System Diagnostics, page 12-20
- ACS Process Status, page 12-21
- ACS System Health, page 12-21
- ACS AAA Health, page 12-22
- RADIUS Sessions, page 12-24
- Unknown NAD, page 12-24

- External DB Unavailable, page 12-25
- RBACL Drops, page 12-26
- NAD-Reported AAA Downtime, page 12-28

Passed Authentications

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ passed authentications that occurred during the time interval that you have specified up to the previous 24 hours. These authentication records are grouped by a common attribute, such as ACS Instance, User, Identity Group, and so on. The number of records within each of these groups is computed. If the count computed for any of these groups exceeds the specified threshold, an alarm is triggered.

For example, if you configure a threshold with the following criteria: Passed authentications greater than 1000 in the past 20 minutes for an ACS instance. When ACS evaluates this threshold and three ACS instances have processed passed authentications as follows:

ACS Instance	Passed Authentication Count
New York ACS	1543
Chicago ACS	879
Los Angeles	2096

An alarm is triggered because at least one ACS instance has greater than 1000 passed authentications in the past 20 minutes.

Note You can specify one or more filters to limit the passed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the authentication records and only those records whose filter value matches the value that you specify are counted. If you specify multiple filters, only the records that match all the filter conditions are counted.

Modify the fields in the Criteria tab as described in Table 12-10 to create a threshold with the passed authentication criteria.

Table 12-10 Passed Authentications

Option	Description
Passed Authentications	Enter data according to the following: greater than <*count*> <**occurrences** | **%**> in the past <*time*> <***Minutes*** | ***Hours***> for a <*object*>, where: • <*count*> values can be the absolute number of occurrences or percent. Valid values are: – *count* must be in the range 0 to 99 for greater than. – *count* must be in the range 1 to 100 for lesser than. • <**occurrences** | **%**> value can be occurrences or %. • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – ACS Instance – User – Identity Group – Device IP – Identity Store – Access Service – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel **Note** In a distributed deployment, if there are two ACS instances, the count is calculated as an absolute number or as a percentage for each of the instances. ACS triggers an alarm only when the individual count of any of the ACS instance exceeds the specified threshold.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
User	Click **Select** to choose or enter a valid username on which to configure your threshold.
Identity Group	Click **Select** to choose a valid identity group name on which to configure your threshold.
Device Name	Click **Select** to choose a valid device name on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.
Identity Store	Click **Select** to choose a valid identity store name on which to configure your threshold.
Access Service	Click **Select** to choose a valid access service name on which to configure your threshold.
MAC Address	Click **Select** to choose or enter a valid MAC address on which to configure your threshold. This filter is available only for RADIUS authentications.
NAD Port	Click **Select** to choose a port for the network device on which to configure your threshold. This filter is available only for RADIUS authentications.

Table 12-10 Passed Authentications (continued)

Option	Description
AuthZ Profile	Click **Select** to choose an authorization profile on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthN Method	Click **Select** to choose an authentication method on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP AuthN	Click **Select** to choose an EAP authentication value on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP Tunnel	Click **Select** to choose an EAP tunnel value on which to configure your threshold. This filter is available only for RADIUS authentications.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

Failed Authentications

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that occurred during the time interval that you have specified up to the previous 24 hours. These authentication records are grouped by a common attribute, such as ACS Instance, User, Identity Group, and so on. The number of records within each of these groups is computed. If the count computed for any of these groups exceeds the specified threshold, an alarm is triggered.

For example, if you configure a threshold with the following criteria: Failed authentications greater than 10 in the past 2 hours for Device IP. When ACS evaluates this threshold, if failed authentications have occurred for four IP addresses in the past two hours as follows:

Device IP	Failed Authentication Count
a.b.c.d	13
e.f.g.h	8
i.j.k.l	1
m.n.o.p	1

An alarm is triggered because at least one Device IP has greater than 10 failed authentications in the past 2 hours.

Note You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the authentication records and only those records whose filter value matches the value that you specify are counted. If you specify multiple filters, only the records that match all the filter conditions are counted.

Modify the fields in the Criteria tab as described in Table 12-11 to create a threshold with the failed authentication criteria.

Table 12-11 Failed Authentications

Option	Description
Failed Authentications	Enter data according to the following: greater than <*count*> <**occurrences | %**> in the past <*time*> <*Minutes|Hours*> for a <*object*>, where: • <*count*> values can be the absolute number of occurrences or percent. Valid values must be in the range 0 to 99. • <**occurrences | %**> value can be occurrences or %. • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – ACS Instance – User – Identity Group – Device IP – Identity Store – Access Service – NAD Port – AuthZ Profile – AuthN Method – EAP AuthN – EAP Tunnel **Note** In a distributed deployment, if there are two ACS instances, the count is calculated as an absolute number or as a percentage for each of the instances. ACS triggers an alarm only when the individual count of any of the ACS instance exceeds the specified threshold.
Filter	
Failure Reason	Click **Select** to enter a valid failure reason name on which to configure your threshold.
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
User	Click **Select** to choose or enter a valid username on which to configure your threshold.
Identity Group	Click **Select** to choose a valid identity group name on which to configure your threshold.
Device Name	Click **Select** to choose a valid device name on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.

Table 12-11 Failed Authentications (continued)

Option	Description
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.
Identity Store	Click **Select** to choose a valid identity store name on which to configure your threshold.
Access Service	Click **Select** to choose a valid access service name on which to configure your threshold.
MAC Address	Click **Select** to choose or enter a valid MAC address on which to configure your threshold. This filter is available only for RADIUS authentications.
NAD Port	Click **Select** to choose a port for the network device on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthZ Profile	Click **Select** to choose an authorization profile on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthN Method	Click **Select** to choose an authentication method on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP AuthN	Click **Select** to choose an EAP authentication value on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP Tunnel	Click **Select** to choose an EAP tunnel value on which to configure your threshold. This filter is available only for RADIUS authentications.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

Authentication Inactivity

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ authentications that occurred during the time interval that you have specified up to the previous 31 days. If no authentications have occurred during the specified time interval, an alarm is triggered. You can specify filters to generate an alarm if no authentications are seen for a particular ACS instance or device IP address during the specified time interval.

If the time interval that you have specified in the authentication inactivity threshold is lesser than that of the time taken to complete an aggregation job, which is concurrently running, then this alarm is suppressed. The aggregation job begins at 00:05 hours every day. From 23:50 hours, up until the time the aggregation job completes, the authentication inactivity alarms are suppressed. For example, if your aggregation job completes at 01:00 hours today, then the authentication inactivity alarms will be suppressed from 23:50 hours until 01:00 hours.

Note If you install ACS between 00:05 hours and 05:00 hours, or if you have shut down your appliance for maintenance at 00:05 hours, then the authentication inactivity alarms are suppressed until 05:00 hours.

Choose this category to define threshold criteria based on authentications that are inactive. Modify the fields in the **Criteria** tab as described in Table 12-12.

Table 12-12 Authentication Inactivity

Option	Description
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
Device	Click **Select** to choose a valid device on which to configure your threshold.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+
Inactive for	Use the drop-down list box to select one of these valid options: • Hours—Specify the number of hours in the range from 1 to 744. • Days—Specify the number of days from 1 to 31.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

TACACS Command Accounting

When ACS evaluates this threshold, it examines the TACACS+ accounting records that it received during the interval between the previous and current alarm evaluation cycle. If one or more TACACS+ accounting records match, it calculates the time that has elapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the TACACS+ accounting records received during the interval between the previous and current alarm evaluation cycle. If one or more TACACS+ accounting records match a specified command and privilege level, an alarm is triggered.

You can specify one or more filters to limit the accounting records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on TACACS commands. Modify the fields in the **Criteria** tab as described in Table 12-13.

Table 12-13 TACACS Command Accounting

Option	Description
Command	Enter a TACACS command on which you want to configure your threshold.
Privilege	Use the drop-down list box to select the privilege level on which you want to configure your threshold. Valid options are: • Any • A number from 0 to 15.

Table 12-13 TACACS Command Accounting

Option	Description
Filter	
User	Click **Select** to choose or enter a valid username on which to configure your threshold.
Device Name	Click **Select** to choose a valid device name on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

TACACS Command Authorization

When ACS evaluates this threshold, it examines the TACACS+ accounting records that it received during the interval between the previous and current alarm evaluation cycle. If one or more TACACS+ accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the TACACS+ authorization records received during the interval between the previous and current alarm evaluation cycle. If one or more TACACS+ authorization records match a specified command, privilege level, and passed or failed result, an alarm is triggered.

You can specify one or more filters to limit the authorization records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on TACACS command authorization profile. Modify the fields in the **Criteria** tab as described in Table 12-14.

Table 12-14 TACACS Command Authorization

Option	Description
Command	Enter a TACACS command on which you want to configure your threshold.
Privilege	Use the drop-down list box to select the privilege level on which you want to configure your threshold. Valid options are: • Any • A number from 0 to 15.
Authorization Result	Use the drop-down list box to select the authorization result on which you want to configure your threshold. Valid options are: • Passed • Failed
Filter	
User	Click **Select** to choose or enter a valid username on which to configure your threshold.

Table 12-14 TACACS Command Authorization

Option	Description
Identity Group	Click **Select** to choose a valid identity group name on which to configure your threshold.
Device Name	Click **Select** to choose a valid device name on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

ACS Configuration Changes

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle. If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the ACS configuration changes made during the interval between the previous and current alarm evaluation cycle. If one or more changes were made, an alarm is triggered.

You can specify one or more filters to limit which configuration changes are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on configuration changes made in the ACS instance. Modify the fields in the **Criteria** tab as described in Table 12-15.

Table 12-15 ACS Configuration Changes

Option	Description
Administrator	Click **Select** to choose a valid administrator username on which you want to configure your threshold.
Object Name	Enter the name of the object on which you want to configure your threshold.
Object Type	Click **Select** to choose a valid object type on which you want to configure your threshold.
Change	Use the drop-down list box to select the administrative change on which you want to configure your threshold. Valid options are: • Any • Create—Includes “duplicate” and “edit” administrative actions. • Update • Delete
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

ACS System Diagnostics

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle. If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines system diagnostic records generated by the monitored ACS during the interval. If one or more diagnostics were generated at or above the specified security level, an alarm is triggered. You can specify one or more filters to limit which system diagnostic records are considered for threshold evaluation. Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on system diagnostics in the ACS instance. Modify the fields in the **Criteria** tab as described in Table 12-16.

Table 12-16 ACS System Diagnostics

Option	Description
Severity at and above	Use the drop-down list box to choose the severity level on which you want to configure your threshold. This setting captures the indicated severity level and those that are higher within the threshold. Valid options are: • Fatal • Error • Warning • Info • Debug
Message Text	Enter the message text on which you want to configure your threshold. Maximum character limit is 1024.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

ACS Process Status

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle. If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS determines whether any ACS process has failed during that time. If ACS detects one or more failures, an alarm is triggered. You can limit the check to particular processes or a particular ACS instance or both.

Choose this category to define threshold criteria based on ACS process status. Modify the fields in the **Criteria** tab as described in Table 12-17.

Table 12-17 ACS Process Status

Option	Description
Monitor Processes	
ACS Database	Check the check box to add the ACS database to your threshold configuration.
ACS Management	Check the check box to add the ACS management to your threshold configuration.
ACS Runtime	Check the check box to add the ACS runtime to your threshold configuration.
Monitoring and Reporting Database	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Collector	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Alarm Manager	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Job Manager	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Log Processor	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

ACS System Health

When ACS evaluates this threshold, it examines whether any system health parameters have exceeded the specified threshold in the specified time interval up to the previous 60 minutes. These health parameters include percentage of CPU utilization, percentage of memory consumption, and so on. If any of the parameters exceed the specified threshold, an alarm is triggered. By default, the threshold applies to all ACS instances in your deployment. If you want, you can limit the check to just a single ACS instance.

Choose this category to define threshold criteria based on the system health of ACS. Modify the fields in the **Criteria** tab as described in Table 12-18.

Table 12-18 ACS System Health

Option	Description
Average over the past	Use the drop-down list box to select the amount of time you want to configure for your configuration, where <min> is minutes and can be: • 15 • 30 • 45 • 60
CPU	Enter the percentage of CPU usage you want to set for your threshold configuration. The valid range is from 1 to 100.
Memory	Enter the percentage of memory usage (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk I/O	Enter the percentage of disk usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/opt	Enter the percentage of /opt disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/local disk	Enter the percentage of local disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/	Enter the percentage of the / disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/tmp	Enter the percentage of temporary disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

ACS AAA Health

When ACS evaluates this threshold, it examines whether any ACS health parameters have exceeded the specified threshold in the specified time interval up to the previous 60 minutes. ACS monitors the following parameters:

- RADIUS Throughput
- TACACS Throughput
- RADIUS Latency
- TACACS Latency

If any of the parameters exceed the specified threshold, an alarm is triggered. By default, the threshold applies to all monitored ACS instances in your deployment. If you want, you can limit the check to just a single ACS instance.

Modify the fields in the **Criteria** tab as described in Table 12-19.

Table 12-19 ACS AAA Health

Option	Description
Average over the past	Use the drop-down list box to select the amount of time you want to configure for your configuration, where <min> is minutes and can be: • 15 • 30 • 45 • 60
RADIUS Throughput	Enter the number of RADIUS transactions per second you want to set (lesser than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
TACACS Throughput	Enter the number of TACACS+ transactions per second you want to set (lesser than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
RADIUS Latency	Enter the number in milliseconds you want to set for RADIUS latency (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
TACACS Latency	Enter the number in milliseconds you want to set for TACACS+ latency (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

RADIUS Sessions

When ACS evaluates this threshold, it determines whether any authenticated RADIUS sessions have occurred in the past 15 minutes where an accounting start event has not been received for the session. These events are grouped by device IP address, and if the count of occurrences for any device IP exceeds the specified threshold, an alarm is triggered. You can set a filter to limit the evaluation to a single device IP.

Choose this category to define threshold criteria based on RADIUS sessions. Modify the fields in the **Criteria** tab as described in Table 12-20.

Table 12-20 RADIUS Sessions

Option	Description
More than <*num*> authenticated sessions in the past 15 minutes, where accounting start event has not been received for a Device IP	<*num*>—A count of authenticated sessions in the past 15 minutes.
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.

Unknown NAD

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that have occurred during the specified time interval up to the previous 24 hours. From these failed authentications, ACS identifies those with the failure reason Unknown NAD. The unknown network access device (NAD) authentication records are grouped by a common attribute, such as ACS instance, user, and so on, and a count of the records within each of those groups is computed. If the count of records for any group exceeds the specified threshold, an alarm is triggered. This can happen if, for example, you configure a threshold as follows:

Unknown NAD count greater than 5 in the past 1 hour for a Device IP

If in the past hour, failed authentications with an unknown NAD failure reason have occurred for two different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 5.

Device IP	Count of Unknown NAD Authentication Records
a.b.c.d	6
e.f.g.h	1

You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on authentications that have failed because of an unknown NAD. Modify the fields in the **Criteria** tab as described in Table 12-21.

Table 12-21 Unknown NAD

Option	Description
Unknown NAD count	greater than <*num*> in the past <*time*> <*Minutes|Hours*> for a <*object*>, where: • <*num*> values can be any five-digit number greater than or equal to zero (0). • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – ACS Instance – Device IP
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

External DB Unavailable

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that have occurred during the specified interval up to the previous 24 hours. From these failed authentications, ACS identifies those with the failure reason, External DB unavailable. Authentication records with this failure reason are grouped by a common attribute, such as ACS instance, user, and so on, and a count of the records within each of those groups is computed. If the count of records for any group exceeds the specified threshold, an alarm is triggered. This can happen if, for example, you configure a threshold as follows:

External DB Unavailable count greater than 5 in the past 1 hour for a Device IP

If in the past hour, failed authentications with an External DB Unavailable failure reason have occurred for two different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 5.

Device IP	Count of External DB Unavailable Authentication Records
a.b.c.d	6
e.f.g.h	1

You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on an external database that ACS is unable to connect to. Modify the fields in the **Criteria** tab as described in Table 12-22.

Table 12-22 External DB Unavailable

Option	Description
External DB Unavailable	<*percent*|*count*> greater than <*num*> in the past <*time*> <*Minutes*|*Hours*> for a <*object*>, where: • <Percent|Count> value can be Percent or Count. • <*num*> values can be any one of the following: – 0 to 99 for percent – 0 to 99999 for count • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – ACS Instance – Identity Store
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
Identity Group	Click **Select** to choose a valid identity group name on which to configure your threshold.
Identity Store	Click **Select** to choose a valid identity store name on which to configure your threshold.
Access Service	Click **Select** to choose a valid access service name on which to configure your threshold.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: • RADIUS • TACACS+

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

RBACL Drops

When ACS evaluates this threshold, it examines Cisco TrustSec RBACL drops that occurred during the specified interval up to the previous 24 hours. The RBACL drop records are grouped by a particular common attribute, such as NAD, SGT, and so on. A count of such records within each of those groups is computed. If the count for any group exceeds the specified threshold, an alarm is triggered. For example, consider the following threshold configuration:

RBACL Drops greater than 10 in the past 4 hours by a SGT

If, in the past four hours, RBACL drops have occurred for two different source group tags as shown in the following table, an alarm is triggered, because at least one SGT has a count greater than 10.

SGT	Count of RBACL Drops
1	17
3	14

You can specify one or more filters to limit the RBACL drop records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the RBACL drop records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Modify the fields in the **Criteria** tab as described in Table 12-23.

Table 12-23 RBACL Drops

Option	Description
RBACL drops	greater than <*num*> in the past <*time*> <*Minutes|Hours*> by a <*object*>, where: • <*num*> values can be any five-digit number greater than or equal to zero (0). • <*time*> values can be 1 to 1440 minutes, or 1 to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – NAD – SGT – DGT – DST_IP
Filter	
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
SGT	Click **Select** to choose or enter a valid source group tag on which to configure your threshold.
DGT	Click **Select** to choose or enter a valid destination group tag on which to configure your threshold.
Destination IP	Click **Select** to choose or enter a valid destination IP address on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

NAD-Reported AAA Downtime

When ACS evaluates this threshold, it examines the NAD-reported AAA down events that occurred during the specified interval up to the previous 24 hours. The AAA down records are grouped by a particular common attribute, such as device IP address or device group, and a count of records within each of those groups is computed. If the count for any group exceeds the specified threshold, an alarm is triggered. For example, consider the following threshold configuration:

AAA Down count greater than 10 in the past 4 hours by a Device IP

If, in the past four hours, NAD-reported AAA down events have occurred for three different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 10.

Device IP	Count of NAD-Reported AAA Down Events
a.b.c.d	15
e.f.g.h	3
i.j.k.l	9

You can specify one or more filters to limit the AAA down records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the AAA down records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on the AAA downtime that a network access device reports. Modify the fields in the **Criteria** tab as described in Table 12-24.

Table 12-24 NAD-Reported AAA Downtime

Option	Description
AAA down	greater than <*num*> in the past <*time*> <*Minutes|Hours*> by a <*object*>, where: • <*num*> values can be any five-digit number greater than or equal to zero (0). • <*time*> values can be 1 to 1440 minutes, or 1to 24 hours. • <Minutes|Hours> value can be Minutes or Hours. • <*object*> values can be: – Device IP – Device Group
Filter	
ACS Instance	Click **Select** to choose a valid ACS instance on which to configure your threshold.
Device IP	Click **Select** to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click **Select** to choose a valid device group name on which to configure your threshold.

Related Topics

- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Configuring General Threshold Information, page 12-11
- Configuring Threshold Notifications, page 12-29

Configuring Threshold Notifications

Use this page to configure alarm threshold notifications.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **Monitoring and Reports > Alarms > Thresholds**, then do one of the following:

- Click **Create** to create a new alarm threshold.
- Click the name of an alarm threshold, or check the check box next to an existing alarm threshold and click **Edit** to edit a selected alarm threshold.
- Click the name of an alarm threshold, or check the check box next to an existing alarm threshold and click **Duplicate** to duplicate a selected alarm threshold.

Step 2 Click the **Notifications** tab.

The Thresholds: Notifications page appears as described in Table 12-25:

Table 12-25 Thresholds: Notifications Page

Option	Description
Severity	Use the drop-down list box to select the severity level for your alarm threshold. Valid options are: • Critical • Warning • Info
Send Duplicate Notifications	Check the check box to be notified of duplicate alarms. An alarm is considered a duplicate if a previously generated alarm for the same threshold occurred within the time window specified for the current alarm.
Email Notification	
Email Notification User List	Enter a comma-separated list of e-mail addresses or ACS administrator names or both. Do one of the following: • Enter the e-mail addresses. • Click **Select** to enter valid ACS administrator names. The associated administrator is notified by e-mail only if there is an e-mail identification specified in the administrator configuration. See Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-6 for more information. When a threshold alarm occurs, an e-mail is sent to all the recipients in the Email Notification User List. Click **Clear** to clear this field.
Email in HTML Format	Check this check box to send e-mail notifications in HTML format. Uncheck this check box to send e-mail notifications as plain text.
Custom Text	Enter custom text messages that you want associated with your alarm threshold.
Syslog Notification	
Send Syslog Message	Check this check box to send a syslog message for each system alarm that ACS generates. **Note** For ACS to send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. Understanding Alarm Syslog Targets, page 12-32 for more information.

Related Topics

- Viewing and Editing Alarms in Your Inbox, page 12-3
- Creating, Editing, and Duplicating Alarm Thresholds, page 12-9
- Deleting Alarm Thresholds, page 12-31

Deleting Alarm Thresholds

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To delete an alarm threshold:

Step 1 Select **Monitoring and Reports > Alarms > Thresholds**.

The Alarms Thresholds page appears.

Step 2 Check one or more check boxes next to the thresholds you want to delete, and click **Delete**.

Step 3 Click **OK** to confirm that you want to delete the selected alarm(s).

The Alarms Thresholds page appears without the deleted threshold.

Configuring System Alarm Settings

System alarms are used to notify users of:

- Errors that are encountered by the Monitoring and Reporting services
- Information on data purging

Use this page to enable system alarms and to specify where alarm notifications are sent. When you enable system alarms, they are sent to the Alarms Inbox. In addition, you can choose to send alarm notifications through e-mail to select recipients and as syslog messages to the destinations specified as alarm syslog targets.

From the Monitoring & Report Viewer, choose **Monitoring Configuration > System Configuration > System Alarm Settings**.

Table 12-26 System Alarm Settings Page

Option	Description
System Alarm Settings	
Notify System Alarms	Check this check box to enable system alarm notification.
System Alarms Suppress Duplicates	Use the drop-down list box to designate the number of hours that you want to suppress duplicate system alarms from being sent to the Email Notification User List. Valid options are 1, 2, 4, 6, 8, 12, and 24.
Email Notification	

Table 12-26 System Alarm Settings Page (continued)

Option	Description
Email Notification User List	Enter a comma-separated list of e-mail addresses or ACS administrator names or both. Do one of the following: • Enter the e-mail addresses. • Click **Select** to enter valid ACS administrator names. The associated administrator is notified by e-mail only if there is an e-mail identification specified in the administrator configuration. See Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-6 for more information. When a system alarm occurs, an e-mail is sent to all the recipients in the Email Notification User List. Click **Clear** to clear this field.
Email in HTML Format	Check this check box to send e-mail notifications in HTML format. Uncheck this check box to send e-mail notifications as plain text.
Syslog Notification	
Send Syslog Message	Check this check box to send a syslog message for each system alarm that ACS generates. **Note** For ACS to send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. Understanding Alarm Syslog Targets, page 12-32 for more information.

This section contains the following topics:

- Creating and Editing Alarm Syslog Targets, page 12-32
- Deleting Alarm Syslog Targets, page 12-33

Understanding Alarm Syslog Targets

Alarm syslog targets are the destinations where alarm syslog messages are sent. The Monitoring & Report Viewer sends alarm notification in the form of syslog messages. You must configure a machine that runs a syslog server to receive these syslog messages. To view a list of configured alarm syslog targets, choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

Note You can configure a maximum of two syslog targets in the Monitoring & Report Viewer.

This section contains the following topics:

- Creating and Editing Alarm Syslog Targets, page 12-32
- Deleting Alarm Syslog Targets, page 12-33

Creating and Editing Alarm Syslog Targets

To create or edit an alarm syslog target:

Step 1 Choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

The Alarm Syslog Targets page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the alarm syslog target that you want to edit, then click **Edit**.

The Alarm Syslog Targets Create or Edit page appears.

Step 3 Modify the fields described in Table 12-27.

Table 12-27 Alarm Syslog Targets Create or Edit Page

Option	Description
Identification	
Name	Name of the alarm syslog target. The name can be 255 characters in length.
Description	(Optional) A brief description of the alarm that you want to create. The description can be up to 255 characters in length.
Configuration	
IP Address	IP address of the machine that receives the syslog message. This machine must have the syslog server running on it. We recommend that you use a Windows or a Linux machine to receive syslog messages.
Use Advanced Syslog Options	
Port	Port in which the remote syslog server listens. By default, it is set to 514. Valid options are from 1 to 65535.
Facility Code	Syslog facility code to be used for logging. Valid options are Local0 through Local7.

Step 4 Click **Submit**.

Related Topics

- Understanding Alarm Syslog Targets, page 12-32
- Deleting Alarm Syslog Targets, page 12-33

Deleting Alarm Syslog Targets

Note You cannot delete the default *nonstop* schedule.

To delete an alarm syslog target:

Step 1 Choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

The Alarm Syslog Targets page appears.

Step 2 Check the check box next to the alarm syslog target that you want to delete, then click **Delete**.

The following message appears:

```
Do you want to delete the selected item(s)?
```

Step 3 Click **Yes**.

The Alarm Syslog Targets page appears without the deleted alarm syslog targets.

CHAPTER 13

Managing Reports

The Monitoring & Report Viewer component of ACS collects log and configuration data from various ACS servers in your deployment, aggregates it, and provides interactive reports that help you analyze the data. The Monitoring & Report Viewer provides you integrated monitoring, reporting, and troubleshooting capabilities to efficiently manage your network and troubleshoot network-related problems.

The Monitoring & Report Viewer offers you a powerful dashboard that you can use to monitor the health of all ACS servers in your deployment. The dashboard also provides information on network access patterns and trends in traffic that you can use to administer your network efficiently. The Monitoring & Report Viewer provides you real-time data and vital statistics that help you proactively manage your network and prevent any attacks.

ACS comes with a set of predefined reports that you can run to obtain meaningful information from the log and configuration data obtained from ACS servers. Table 13-2 lists the reports that are available in ACS under various categories. These reports provide information related to authentication, session traffic, device administration, ACS server configuration and administration, and troubleshooting. You can view these reports as tables, graphs, or charts and drill down further for more granular data.

Further, ACS allows you to:

- Filter the data in your report based on your requirements
- Export the report in a CSV format and print it
- Add the report to your list of favorites, from which you can access them frequently
- Share the report with other users
- Customize reports using the Interactive Viewer

The Monitoring and Reports drawer appears in the primary web interface window and contains the Launch Monitoring & Report Viewer option.

Click **Launch Monitoring & Report Viewer** to open the Monitoring and Reports Viewer in a secondary web interface window, which contains the following drawers:

- Monitoring and Reports
- Monitoring Configuration. (See Managing System Operations and Configuration in the Monitoring & Report Viewer, page 15-1.)

You can run reports from any of the following pages:

- Favorites—**Monitoring & Reports > Reports > Favorites**
- Shared—**Monitoring & Reports > Reports > Shared**
- Catalog—**Monitoring & Reports > Reports > Catalog >** <*report_type*>

For easy access, you can add reports to your Favorites page, from which you can customize and delete reports. You can customize the reports that must be shared within your group and add them to the Shared page. The Catalog pages provide a rich set of reports on log, diagnostic, and troubleshooting data retrieved from the ACS servers in your deployment.

The reports that reside in these pages can be:

- System reports—Preconfigured with the ACS software; you can view the list of system reports in the **Reports > Catalog** pages.
- Customized reports—System reports that you have configured and saved (see Customizing Reports, page 13-19).

Note Performance of reports in Internet Explorer (IE) 7.0 is slow because of a phishing filter, which is a new feature in IE 7.0. To resolve this issue, you must get the latest security updates from Microsoft. For more information on this, go to http://support.microsoft.com/kb/928089/.

In addition, ACS 5.1 introduces the Dynamic Change of Authorization (CoA) feature through a new report, the RADIUS Active Sessions report, which allows you to dynamically control active RADIUS sessions. With this feature, you can send a reauthenticate or disconnect request to a NAD to:

- Troubleshoot issues related to authentication—You can use the Disconnect:None option to follow up with an attempt to reauthenticate again.

Note You must not use the disconnect option to restrict access. To restrict access, use the shutdown option.

- Block a problematic host—You can use the Disconnect:Port Disable option to block an infected host that sends a lot of traffic over the network.

Note The RADIUS protocol currently does not support a method for re-enabling a port that is shut down.

- Force endpoints to reacquire IP addresses—You can use the Disconnect:Port Bounce option for endpoints that do not have a supplicant or client to generate a DHCP request after VLAN change.
- Push an updated authorization policy to an endpoint—You can use the Re-Auth option to enforce an updated policy configuration, such as a change in the authorization policy on existing sessions based on the administrator's discretion. For example, if posture validation is enabled, when an endpoint gains access initially, it is usually quarantined. After the endpoint's identity and posture are known, it is possible to send the CoA Re-Auth command to the endpoint for the endpoint to acquire the actual authorization policy based on its posture.

Note Legacy NAS devices do not support the CoA feature. Cisco plans to support CoA in all its devices as part of the NPF program.

Note For the CoA commands to be understood correctly by the device, it is important that you configure the options appropriately.

For the CoA feature to work properly, you must configure in ACS the shared secret of each and every device for which you want to dynamically change the authorization. ACS uses the shared secret configuration, both for requesting access from the device and for issuing CoA commands to it.

See Changing Authorization and Disconnecting Active RADIUS Sessions, page 13-17 for more information.

This chapter describes in detail the following:

- Working with Favorite Reports, page 13-3
- Sharing Reports, page 13-7
- Working with Catalog Reports, page 13-7
- Viewing Reports, page 13-20
- Formatting Reports in Interactive Viewer, page 13-26
- Organizing Report Data, page 13-39
- Hiding and Filtering Report Data, page 13-63
- Understanding Charts, page 13-71

Working with Favorite Reports

You can add reports that you most frequently use to your Favorites page so that you do not have to navigate each time to get to your favorite report. The Monitoring & Report Viewer allows you to:

- View the parameters that are set for each of your favorite reports
- Edit the parameters before you run the reports

For example, after you add a report to your list of favorites, the next time you want to view the same report with a different set of parameters, you need not create another report. Instead, you can simply edit the parameters in your favorite report to generate the report with different parameters.

This section contains the following topics:

- Adding Reports to Your Favorites Page, page 13-3
- Viewing Favorite-Report Parameters, page 13-4
- Editing Favorite Reports, page 13-5
- Running Favorite Reports, page 13-6
- Deleting Reports from Favorites, page 13-7

Adding Reports to Your Favorites Page

You can create a list of favorites for reports that you access often, similarly to the way you bookmark your favorite websites in a browser.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To add a report to your Favorites page:

Step 1 Select **Monitoring & Reports > Reports > Catalog > <*report_type*> >**, where *report_type* is the type of report.

The available reports for the report type you selected are displayed.

Step 2 Click the radio button next to the report you want to add to your favorites. See Table 13-5 for valid field options.

Step 3 Click **Add to Favorites**. The Add to Favorite page appears.

Step 4 Modify fields in the Add to Favorites page as required.

Step 5 Click **Add to Favorite**.

The report is added to your Favorites page.

Related Topics

- Working with Favorite Reports, page 13-3
- Viewing Favorite-Report Parameters, page 13-4
- Editing Favorite Reports, page 13-5
- Deleting Reports from Favorites, page 13-7
- Understanding the Report_Name Page, page 13-15

Viewing Favorite-Report Parameters

Before you run your favorite report, you can view the parameters that are set and edit them. To view your favorite-report parameters:

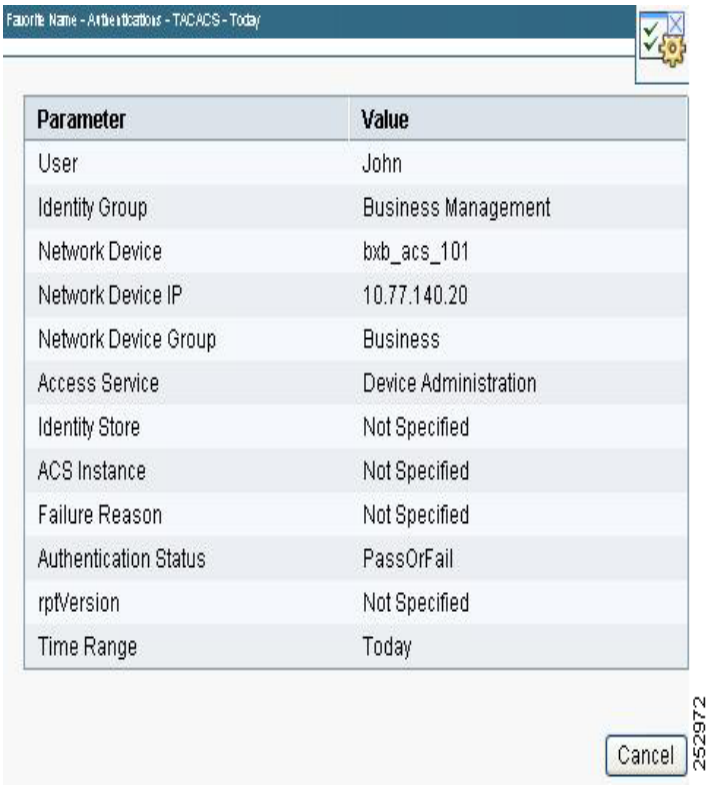
Step 1 Choose **Monitoring and Reports > Reports > Favorites**.

The Favorites page appears with a list of your favorite reports.

Step 2 Check the check box next to the favorite report whose parameters you want to see, then click **Parameters**.

A window similar to the one shown in Figure 13-1 appears, listing the parameters in your favorite report and their values.

Figure 13-1 Viewing Favorite-Report Parameters



Step 3 Click **Cancel** or the close button at the upper-right corner of the parameters window to return to the Favorites page.

Editing Favorite Reports

After you view the existing parameters in your favorite report, you can edit them. To edit the parameters in your favorite reports:

Step 1 Choose **Monitoring and Reports > Reports > Favorites**.

The Favorites page appears with a list of your favorite reports.

Step 2 Check the check box next to the favorite report that you want to edit, then click **Edit**.

The Edit Favorite Report page appears.

Step 3 Edit the values for the various parameters in the Edit Favorite Report page.

Step 4 Click:

- **Edit Favorite** to save the changes that you have made.
- **Reset** to reset the values.

- **Cancel** to cancel the changes that you have made and return to the Favorites page.

When a favorite report is edited, the Monitoring & Report Viewer displays a status message in the Favorite page, stating that the favorite report has been edited successfully.

Related Topics

- Adding Reports to Your Favorites Page, page 13-3
- Viewing Favorite-Report Parameters, page 13-4
- Running Favorite Reports, page 13-6
- Understanding the Report_Name Page, page 13-15

Running Favorite Reports

To run a report in your Favorites page:

Step 1 Select **Monitoring & Reports > Reports > Favorites**.

The Favorites page appears with the fields described in Table 13-1:

Table 13-1 Favorites Page

Option	Description
Favorite Name	The name of the favorites report. Click to open a summary of an associated report.
Report Name	The report name associated with a Catalog (Report) type.
Report Type	The general grouping name associated with the report.

Step 2 Do one of the following:

- Click the check box next to the report name that you want to run and click **Run**.
- Click the name of the report that you want to run.

The report is generated in the page.

Step 3 Click **Launch Interactive Viewer** for more options.

Related Topics

- Adding Reports to Your Favorites Page, page 13-3
- Viewing Favorite-Report Parameters, page 13-4
- Running Favorite Reports, page 13-6
- Understanding the Report_Name Page, page 13-15

Deleting Reports from Favorites

Note When you delete a system report from the Favorites page, the system report remains in the appropriate **Reports > Catalog** page.

To delete a report from the Favorites page:

Step 1 Select **Monitoring & Reports > Reports > Favorites**.

Step 2 Check one or more check boxes next to the reports you want to delete, and click **Delete**.

Step 3 Click **OK** to confirm that you want to delete the selected report(s).

The Favorites page appears without the deleted reports.

Sharing Reports

You can add reports to the Shared folder to make them available for all users. To add reports to the Shared folder:

Step 1 Choose any report that you want to share.

For example, if you want to share the ACS Health Summary report, you would choose **Monitoring and Reports > Reports > Catalog > ACS Instance**.

The ACS Instance reports page appears.

Step 2 Run the report. See Running Catalog Reports, page 13-12 for more information.

In this example, the ACS Health Summary report appears.

Step 3 Launch the report in the Interactive Viewer.

Step 4 Click the **Save** icon at the upper-left corner of the Interactive Viewer page.

The Save window appears.

Step 5 Choose the Shared folder from the Choose a Folder list box.

Step 6 Enter a filename of your choice.

Step 7 Click **Save**.

The report is saved in your Shared folder and is available for all users.

Working with Catalog Reports

Catalog reports are system reports that are preconfigured in ACS. This section contains the following:

- Available Reports in the Catalog, page 13-8
- Running Catalog Reports, page 13-12

- Deleting Catalog Reports, page 13-13
- Running Named Reports, page 13-13
- Changing Authorization and Disconnecting Active RADIUS Sessions, page 13-17
- Customizing Reports, page 13-19
- Restoring Reports, page 13-19

Available Reports in the Catalog

Table 13-2 describes the reports available when you select Monitoring and Reports, launch Monitoring & Report Viewer, then select **Monitoring and Reports > Reports > Catalog**.

Table 13-2 Available ACS Reports

Report Name	Description	Logging Category
AAA Protocol		
AAA diagnostics	Provides AAA diagnostic details based on severity for a selected time period.	Policy diagnostics, identity stores diagnostics, authentication flow diagnostics, RADIUS diagnostics, TACACS+ diagnostics
Authentication Trend	Provides RADIUS and TACACS+ authentication summary information for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
RADIUS Accounting	Provides user accounting information based on RADIUS for a selected time period.	RADIUS accounting
RADIUS Authentication	Provides RADIUS authentication details for a selected time period.	Passed authentications, failed attempts
TACACS Accounting	Provides user or command accounting information for TACACS+ authentications for a selected time period.	TACACS accounting
TACACS Authentication	Provides TACACS+ authentication details for a selected time period.	Passed authentications, failed attempts
TACACS Authorization	Provides TACACS+ authorization details for a selected time period.	Passed authentications, failed attempts
Access Service		
Access Service Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular access service for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
Top N Authentications By Access Service	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ authentications with respect to the access service for a selected time period.	Passed authentications, failed attempts
ACS Instance		

Table 13-2 Available ACS Reports (continued)

Report Name	Description	Logging Category
ACS Administrator Entitlement	Shows the role of the administrator in ACS and the: • Tasks in ACS that the administrator is entitled to access • Privileges that the administrator has for each of those operations	None
ACS Administrator Logins	Provides access-related events for administrators that includes login, logout, events, and reasons for failed login attempts.	Administrative and operational audit
ACS Configuration Audit	Provides all the configuration changes done in ACS by the administrator for a selected time period.	Administrative and operational audit
ACS Health Summary	Provides the CPU, memory utilization, RADIUS and TACACS+ latency and throughput (in tabular and graphical formats) and also process status, process downtime, and disk space utilization for a particular ACS instance in a selected time period.	System statistics
ACS Instance Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular ACS instance for a selected time period; along with a graphical representation. This report could take several minutes to run depending on the number of records in the database. **Note** When you reload this report, if rate of incoming syslog messages is around 150 messages per second or more, the total number of passed and failed authentications that appear above the graph and the passed and failed authentication count that is displayed in the table do not match.	Passed authentications, failed attempts
ACS Log Information	Provides ACS log information for a particular log category and ACS server for a selected time period.	All log categories
ACS Operations Audit	Provides all the operational changes done in ACS by the administrator for a selected time period.	Administrative and operational audit
ACS System Diagnostics	Provides system diagnostic details based on severity for a selected time period.	Internal Operations Diagnostics, distributed management, administrator authentication and authorization
Top N Authentication by ACS Instance	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ protocol with respect to a particular ACS instance for a selected time period.	Passed authentications, failed attempts

Table 13-2 Available ACS Reports (continued)

Report Name	Description	Logging Category
User Change Password Audit	Provides the username of the internal user, identity store name, name of the ACS instance, and time when the user password was changed. Helps to keep track of all changes made to internal user passwords across all ACS interfaces.	Administrative and operational audit
Endpoint		
Endpoint MAC Authentication Summary	Provides the RADIUS authentication summary information for a particular MAC or MAB for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
Top N Authentications By Endpoint MAC Address	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to MAC or MAB address for a selected time period.	Passed authentications, failed attempts
Top N Authentications By Machine	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to machine information for a selected time period.	Passed authentications, failed attempts
Failure Reason		
Authentication Failure Code Lookup	Provides the description and the appropriate resolution steps for a particular failure reason.	N/A
Failure Reason Authentication Summary	Provides the RADIUS and TACACS+ authentication summary information for a particular failure reason; along with a graphical representation for a selected time period.	Failed attempts
Top N Authentications By Failure Reason	Provides the top N failed authentication count for RADIUS and TACACS+ protocols with respect to Failure Reason for a selected time period.	Failed attempts
Network Device		
AAA Down Summary	Provides the number of AAA unreachable events that a NAD logs within a selected time period.	N/A
Network Device Authentication Summary	Provides the RADIUS and TACACS+ authentication summary information for a particular network device for a selected time period, along with the graphical representation.	Passed authentications, failed attempts
Network Device Log Messages	Provides you the log information of a particular network device, for a specified time period.	N/A
Session Status Summary	Provides the port sessions and status of a particular network device obtained by SNMP.	N/A
Top N AAA Down By Network Device	Provides the number of AAA down events encountered by each of the network devices.	N/A

Table 13-2 Available ACS Reports (continued)

Report Name	Description	Logging Category
Top N Authentications by Network Device	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ protocols with respect to network device for a selected time period.	Passed authentications, failed attempts
TrustSec		
RBACL Drop Summary	Provides a summary of RBACL drop events for a selected time period.	N/A
SGT Assignment Summary	Provides a summary of SGT assignments for a selected time period.	Passed authentications
Top N RBACL Drops By Destination	Provides the top N RBACL drop event count with respect to destination for a selected time period.	N/A
Top N RBACL Drops By User	Provides the top N RBACL drop event count with respect to the user for a selected time period.	N/A
Top N SGT Assignments	Provides the top N SGT assignment count for a selected time period.	Passed authentications
Session Directory		
RADIUS Active Sessions	Provides information on RADIUS authenticated, authorized, and started sessions. ACS 5.1 introduces the Change of Authorization (CoA) feature through the RADIUS Active Sessions report, which allows you to dynamically control active RADIUS sessions. With this feature, you can send a reauthenticate or disconnect request to a NAD to: • Reauthenticate the user • Terminate the session • Terminate the session and restart the port • Terminate the session and shut down the port	Passed authentications, RADIUS accounting
RADIUS Session History	Provides a summary of RADIUS session history, such as total authenticated, active, and terminated sessions and total and average session duration and throughput for a selected time period.	Passed authentications, RADIUS accounting
RADIUS Terminated Sessions	Provides all the RADIUS terminated session information for a selected time period.	Passed authentications, RADIUS accounting
TACACS Active Sessions	Provides information on TACACS+ active sessions.	TACACS accounting
TACACS Session History	Provides TACACS+ session history summary, such as total active and terminated sessions and total and average session duration and throughput for a selected time period.	TACACS accounting
TACACS Terminated Sessions	Provides TACACS terminated session details for a selected time period.	TACACS accounting

Table 13-2 Available ACS Reports (continued)

Report Name	Description	Logging Category
User		
Top N Authentications By User	Provides top N passed, failed, and total authentication count for RADIUS and TACACS+ protocol with respect to users for a selected time period.	Passed authentications, failed attempts
User Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular user for a selected time period; along with the graphical representation.	Passed authentications, failed attempts

Running Catalog Reports

To run a report that is in the Catalog:

Step 1 Select **Monitoring & Reports > Reports > Catalog > *<report_type>***, where *report_type* is the type of report you want to run.

The available reports for the report type you selected are displayed with the information shown in Table 13-3.

Table 13-3 <report_type> Page

Option	Description
Report Name	The available reports based on the report type you selected.
Type	The type of report.
Modified At	The time that the associated report was last modified by an administrator, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit representation of the year.

Step 2 Click the radio button next to the report name you want to run, then select one of the options under **Run**:

- **Run for Today**—The report you specified is run and the generated results are displayed.
- **Run for Yesterday**—The report you specified is run using the previous day's values and the generated results are displayed.
- **Query and Run**—The Run Report screen appears where you can enter parameters to use when generating the report.

Step 3 Click **Reset Reports** to revert to the default report parameters. A message appears asking you to confirm whether to reset the system report files in the catalog to the factory default.

Step 4 Click **Launch Interactive Viewer** for more options.

Related Topics

- Available Reports in the Catalog, page 13-8
- Deleting Catalog Reports, page 13-13
- Understanding the Report_Name Page, page 13-15

Deleting Catalog Reports

To delete a report from the **Reports > Catalog** pages:

Step 1 Select **Monitoring & Reports > Reports > Catalog > *<report_type>***, where *report_type* is the type of report that you want to delete.

Note You cannot delete system reports from the **Reports > Catalog** pages; you can delete customized reports only.

Step 2 Check one or more check boxes next to the reports you want to delete, and click **Delete**.

Step 3 Click **OK** to confirm that you want to delete the selected report(s).

The Catalog listing page appears without the deleted report.

Running Named Reports

Use this page to run reports on specific named reports.

Select **Monitoring & Reports > Reports > Catalog > *<report_type>* > *<report_name>***, where *report_type* is the type of report (see Table 13-3), and *report_name* is the name of the report that you want to access or run. Table 13-4 describes the available types and names on which you can run reports.

Table 13-4 Reports > Report Types and Names

<report_type>	<report_name>
AAA Protocol	AAA Diagnostics
	Authentication Trend
	RADIUS Accounting
	RADIUS Authentication
	TACACS Accounting
	TACACS Authentication
	TACACS Authorization

Table 13-4 Reports > Report Types and Names (continued)

<report_type>	<report_name>
Access Service	Access Service Authentication Summary
	Top N Authentications By Access Service
ACS Instance	ACS Administrator Entitlement
	ACS Administrator Logins
	ACS Configuration Audit
	ACS Health Summary
	ACS Instance Authentication Summary
	ACS Log Information
	ACS Operations Audit
	ACS System Diagnostics
	Top N Authentications By ACS Instance
	User Change Password Audit
Endpoint	Endpoint MAC Authentication Summary
	Top N Authentications By Endpoint MAC Address
	Top N Authentications By Machine
Failure Reason	Authentication Failure Code Lookup
	Failure Reason Authentication Summary
	Top N Authentications By Failure Reason
Network Device	AAA Down Summary
	Network Device Authentication Summary
	Network Device Log Messages
	Session Status Summary
	Top N AAA Down By Network Device
	Top N Authentications By Network Device
TrustSec	RBACL Drop Summary
	SGT Assignment Summary
	Top N RBACL Drops By Destination
	Top N RBACL Drops By User
	Top N SGT Assignments
Session Directory	RADIUS Active Sessions
	RADIUS Session History
	RADIUS Terminated Sessions
	TACACS Active Sessions
	TACACS Session History
	TACACS Terminated Sessions

Table 13-4 Reports > Report Types and Names (continued)

<report_type>	<report_name>
User	Top N Authentications By User
	User Authentication Summary

Related Topics

- Working with Catalog Reports, page 13-7
- Understanding the Report_Name Page, page 13-15

Understanding the Report_Name Page

Note Not all options listed in Table 13-5 are used in selecting data for all reports.

Table 13-5 <report_name> Page

Option	Description
User	Enter a username or click **Select** to enter a valid username on which to configure your threshold.
MAC Address	Enter a MAC address or click **Select** to enter a valid MAC address on which to run your report.
Identity Group	Enter an identity group name or click **Select** to enter a valid identity group name on which to run your report.
Device Name	Enter a device name or click **Select** to enter a valid device name on which to run your report.
Device IP	Enter a device IP address or click **Select** to enter a valid device IP address on which to run your report.
Device Group	Enter a device group name or click **Select** to enter a valid device group name on which to run your report.
Access Service	Enter an access service name or click **Select** to enter a valid access service name on which to run your report
Identity Store	Enter an identity store name or click **Select** to enter a valid identity store name on which to run your report.
ACS Instance	Enter an ACS instance name or click **Select** to enter a valid ACS instance name on which to run your report.
Failure Reason	Enter a failure reason name or click **Select** to enter a valid failure reason name on which to run your report.
Protocol	Use the drop down list box to select which protocol on which you want to run your report. Valid options are: • RADIUS • TACACS+
Authentication Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: • Pass Or Fail • Pass • Fail

Table 13-5 <report_name> Page (continued)

Option	Description
Radius Audit Session ID	Enter the RADIUS audit session identification name on which you want to run a report.
ACS Session ID	Enter the ACS session identification name on which you want to run a report.
Severity	Use the drop down list box to select the severity level on which you want to run a report. This setting captures the indicated severity level and those that are higher within the threshold. Valid options are: • Fatal • Error • Warning • Info • Debug
End Point IP Address	Enter the end point IP address on which you want to run a report.
Command Accounting Only	Check the check box to enable your report to run for command accounting.
Top	Use the drop down list box to select the number of top (most frequent) authentications by access service on which you want to run your report. Valid options are: • 10 • 50 • 100 • 500 • 1000 • All
By	Use the drop down list box to select the type of authentications on which you want to run your report. Valid options are: • Passed Authentications • Failed Authentications • Total Authentications
Administrator Name	Enter the administrator username, or click Select to select the administrator username, for which you want to run your report.
Object Type	Enter a valid object type on which you want to run your report.
Object Name	Enter the name, or click Select to select the object name, of the object on which you want to run your report.
Authorization Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: • Pass Or Fail • Pass • Fail

Table 13-5 <report_name> Page (continued)

Option	Description
Time Range	Use the drop down list box to select the time range on which you want to run your report. Valid options are: • Last Hour (for the ACS Health Summary report only) • Today • Yesterday • Last 7 Days • Last 30 Days • Custom—You must configure a Start Date and End Date, or a Day. **Note** Some options are not valid for some Time Range entries of the various reports.
Start Date	Enter a date, or click the date selector icon to enter the start date for which you want run your report.
End Date	Enter a date, or click the date selector icon to enter the end date for which you want run your report.
Day	Enter a date, or click the date selector icon to enter the end date for which you want run your report.
Clear	Click to delete the contents of an associate text box.
Run	Click to run the report for which you have made selections.

Related Topics

- Working with Catalog Reports, page 13-7
- Working with Favorite Reports, page 13-3
- Available Reports in the Catalog, page 13-8
- Running Catalog Reports, page 13-12

Changing Authorization and Disconnecting Active RADIUS Sessions

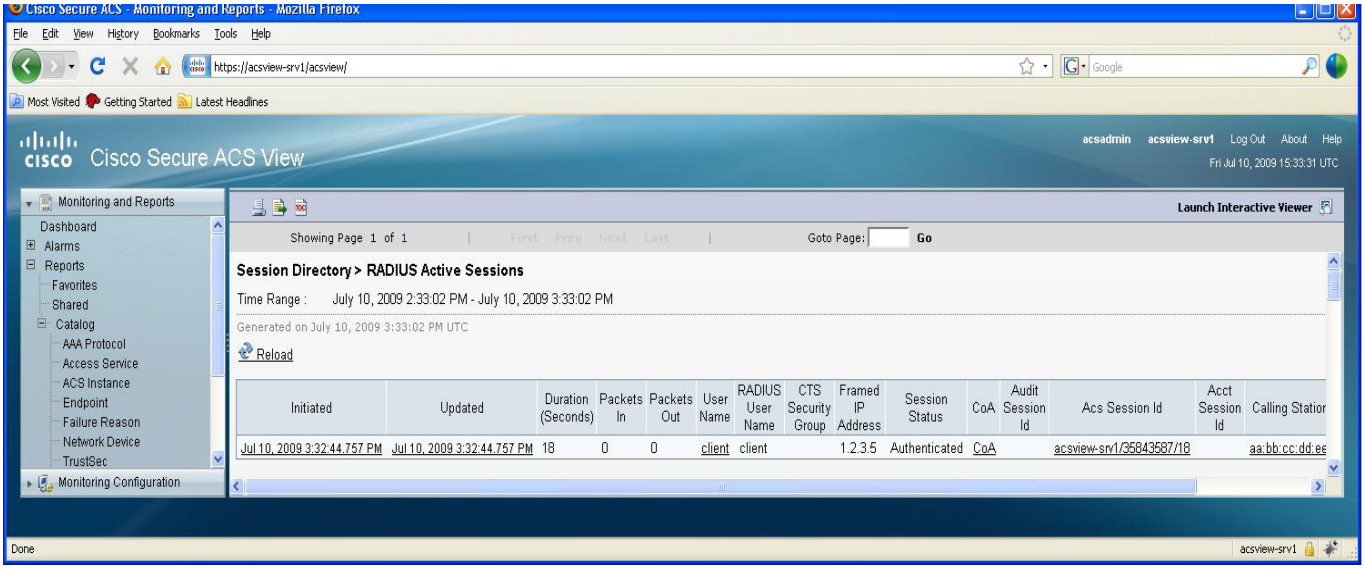
Note Some of the NADs in your deployment do not send an Accounting Stop or Accounting Off packet after a reload. As a result of this, you might find two sessions in the Session Directory reports, one of which has expired. Hence, when you want to dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session, ensure that you always choose the most recent session.

To change authorization or disconnect an active RADIUS session:

Step 1 Run the RADIUS Active Sessions report under Session Directory. See Running Catalog Reports, page 13-12 for information on how to run a RADIUS Active Sessions report.

A report similar to the one shown in Figure 13-2 appears.

Figure 13-2 RADIUS Active Session Report



Step 2 Click the CoA link from the RADIUS session that you want to reauthenticate or terminate.

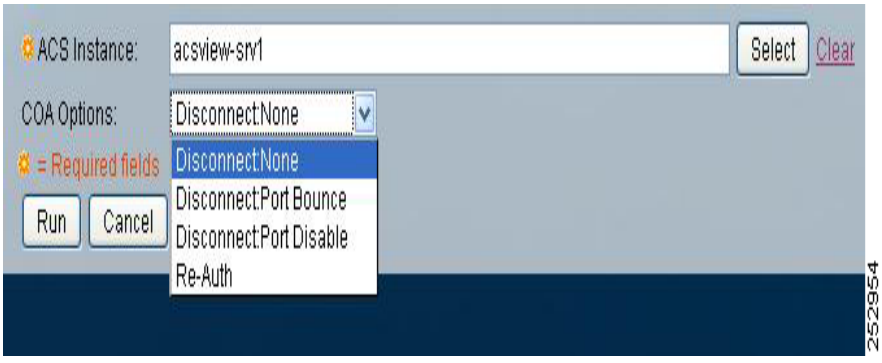
The Change of Authorization Request page appears.

Select a CoA option from the CoA option drop-down list box shown in Figure 13-3.

Valid options are:

- Disconnect:None—Do not terminate the session.
- Disconnect:Port Bounce—Terminate the session and restart the port.
- Disconnect:Port Disable—Terminate the session and shut down the port.
- Re-Auth—Reauthenticate the user.

Figure 13-3 CoA Options



Step 3 Click **Run** to reauthenticate or disconnect the RADIUS session.

If your change of authorization fails, it might be because of any of the following reasons:

- Device does not support CoA
- Changes to the identity or authorization policy

- Shared secret mismatch

Step 4 See the Troubleshooting RADIUS Authentications, page 14-6 to troubleshoot a failed change of authorization attempt. A failed dynamic CoA will be listed under failed RADIUS authentications.

Customizing Reports

To customize a system report:

Step 1 Select **Monitoring & Reports > Reports > Catalog > *<report_type>* > *<report_name>***, where *report_type* is the type of report, and *report_name* is the name of the report that you want to customize.

The Reports page appears.

Step 2 Click the radio button next to the name of the report you want to customize, or click the name of the report you want to customize.

Step 3 Click **Run**.

The Run Report page appears.

Step 4 Modify fields in the Run Reports page as required.

Step 5 Click **Run**.

The report appears.

Step 6 Click **Launch Interactive Viewer**.

Step 7 Modify the report contents as required and click **Save As** to save the customized report with the same, or a different, report name in any Catalog > Reports page.

Note If you save the customized report with the same name as the original system report (overwriting the original system report), you cannot delete it. To restore a customized report to the default, preconfigured system report settings, see Restoring Reports, page 13-19.

The customized report is saved to your specified location.

Restoring Reports

Use the procedure described in this topic, to restore a system report that you have customized back to its original preconfigured system report settings.

This procedure resets all reports that reside in a report catalog type. For example, if you want to reset a specific customized report that resides in the Monitoring & Reports > Reports > Catalog > Endpoint page, this procedure completes that task but also resets all other reports within the Endpoint page.

Step 1 Select **Monitoring & Reports > Reports > Catalog > *<report_type>***, where *report_type* is the type of report in which the customized report that you want to reset to the original system report settings resides.

Step 2 Click **Reset Reports**.

Step 3 Click **Yes** to confirm that you want to reset the System Report files to the factory default.

The page is refreshed, and the reports in **Catalog > *<report_type>*** are reset to the factory default.

Viewing Reports

This section describes how to view the reports and perform various tasks in Standard or Interactive Viewer. In Standard Viewer or Interactive Viewer, you can navigate to the report, print the data, and export the data to another format. Interactive Viewer also provides the ability to modify the content, organization, and formatting of the report.

This section contains the following topics:

- About Standard Viewer, page 13-20
- About Interactive Viewer, page 13-20
- About Interactive Viewer's Context Menus, page 13-20
- Navigating Reports, page 13-22
- Exporting Report Data, page 13-23
- Printing Reports, page 13-25
- Saving Report Designs in Interactive Viewer, page 13-25

About Standard Viewer

From Standard Viewer, you can open a table of contents, navigate the report, export data to spreadsheet format, and print the report.

You can click **Launch Interactive Viewer** to close Standard Viewer and view the report in Interactive Viewer. See About Interactive Viewer, page 13-20.

About Interactive Viewer

Interactive Viewer provides all the features of Standard Viewer and also supports modifying many aspects of the report's layout and formatting. The Interactive Viewer toolbar is much more extensive than that in Standard Viewer. See About Interactive Viewer's Context Menus, page 13-20.

About Interactive Viewer's Context Menus

Interactive Viewer provides context menus that support many of the formatting, sorting, and grouping tasks you perform on data. Figure 13-4 shows the context menu for columns. Using this menu, you can add or delete a column, sort data, add or delete a group, and work with fonts and text alignment. You also can sort and filter data, and create calculations and aggregate rows. To access this context menu, select a column, then right-click the column.

Figure 13-4 Context Menu for Column Data in Interactive Viewer

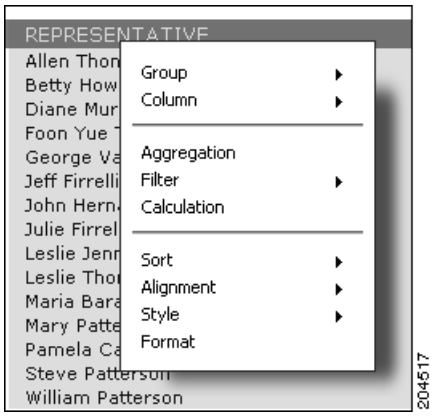
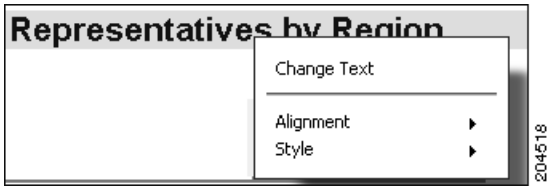


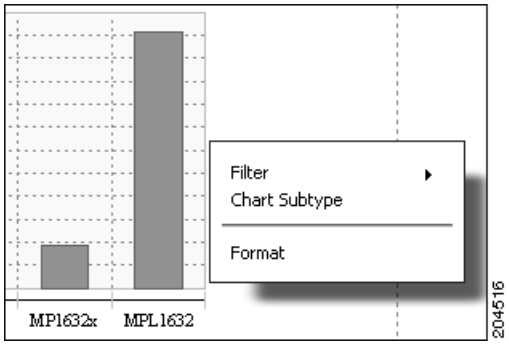
Figure 13-5 shows the context menu you use to modify labels in Interactive Viewer. To display this menu, select and right-click a label. Use this menu to edit the label text or change the text alignment or font properties of the label.

Figure 13-5 Context Menu for Labels in Interactive Viewer



If the report contains a chart, you can use the context menu for charts, shown in Figure 13-6, to modify the chart's formatting, subtype, and other properties.

Figure 13-6 Context Menu for Charts in Interactive Viewer



In each context menu, selecting an entry with a right arrow provides access to related context menu choices. For example, right-clicking a column and choosing Alignment enables you to choose Left, Center, or Right to specify the desired type of alignment.

Navigating Reports

When you open a report in the viewer, you see the first page of data. To view or work with data, you use tools that help you navigate the report.

In the viewer, you can page through a report by using the paging tool shown in Figure 13-7. Using this tool, you can click an arrow to view the first or last page in the report, or move forward or back through the report page by page.

Figure 13-7 Paging Tool

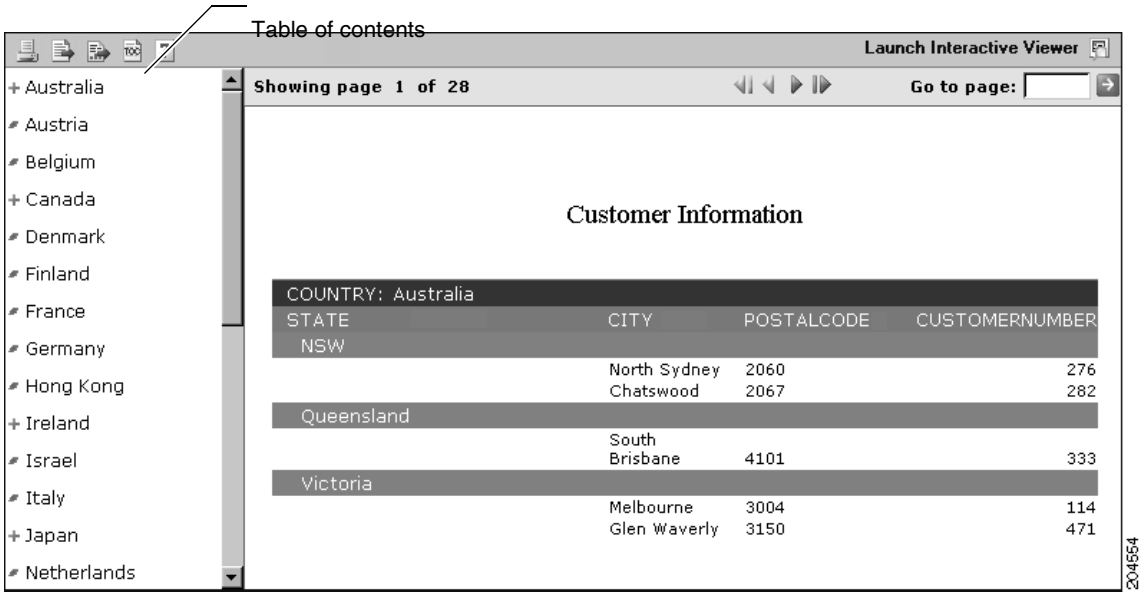
The viewer also supports going to a specific page by typing a page number in Go to page, as shown in Figure 13-8, and clicking the arrow beside the field.

Figure 13-8 Going to a Specific Page

Using the Table of Contents

In the viewer, you can open a table of contents to view the report structure and navigate the report. To open the table of contents, choose the table of contents button in the toolbar. Figure 13-9 shows a report in Standard Viewer with the table of contents open.

Figure 13-9 Using the Table of Contents to Navigate



Each entry in the table of contents is a link to a page in the report. If an entry has a plus sign (+) beside it, you can expand the entry by clicking the plus sign. Figure 13-10 shows an expanded entry.

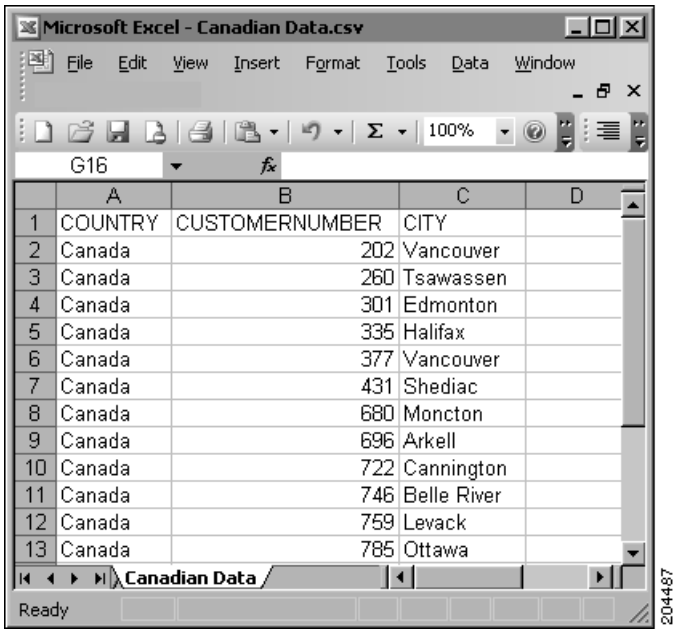
Figure 13-10 Table of Contents Expanded Entry

To navigate to a specific page, click the related link.

Exporting Report Data

The viewer supports the ability to export report data to an Excel spreadsheet as a comma-separated values (.csv) file, pipe-separated values (.psv) file, or a tab-separated values (.tsv) file. You can select an option to export the column's data type. The spreadsheet data is formatted like the data in the information object or the template. If you edited column headers or formatted numeric data in the report design, for example, the spreadsheet does not reflect your edits. Figure 13-11 shows a sample CSV output file.

Figure 13-11 Report Data Exported to Microsoft Excel

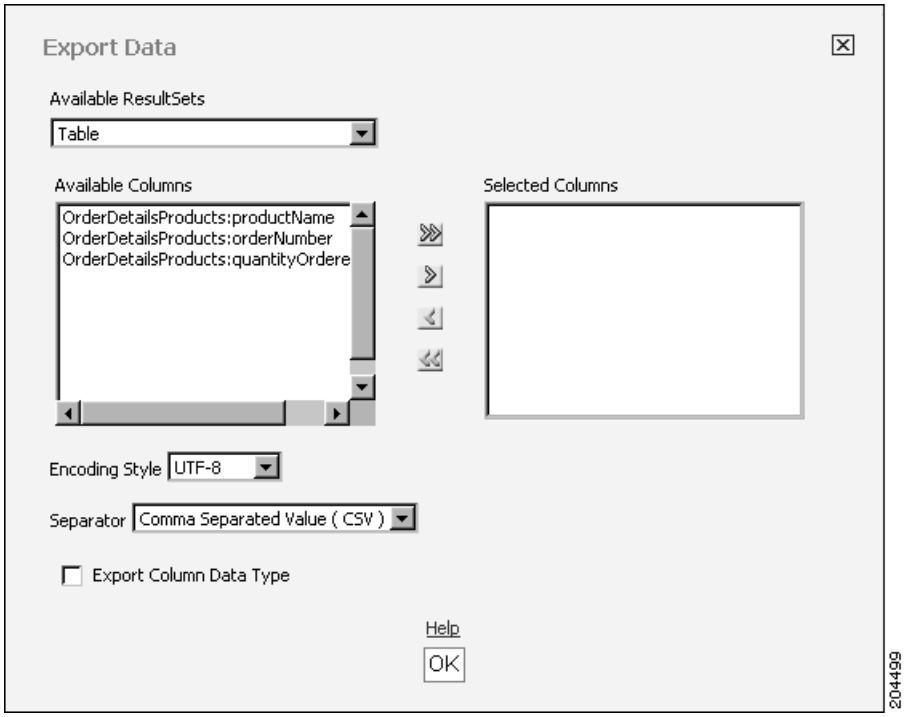


	A	B	C	D
1	COUNTRY	CUSTOMERNUMBER	CITY	
2	Canada	202	Vancouver	
3	Canada	260	Tsawassen	
4	Canada	301	Edmonton	
5	Canada	335	Halifax	
6	Canada	377	Vancouver	
7	Canada	431	Shediac	
8	Canada	680	Moncton	
9	Canada	696	Arkell	
10	Canada	722	Cannington	
11	Canada	746	Belle River	
12	Canada	759	Levack	
13	Canada	785	Ottawa	

In Excel, you can resize columns and format the data as you would do for any other spreadsheet.

Step 1 In the viewer, select Export Data. The Export Data dialog box appears, as shown in Figure 13-12.

Figure 13-12 The Export Data Dialog Box



Available Result Sets lists the tables in the report.

Available Columns lists the columns you can export from the specified table. You can export any of the data the report uses, including the data in aggregate rows and calculated columns. If the report uses more than one data source, you can export data from each data source separately.

Step 2 In Available Columns, select a column to export and choose the single right arrow. To select all the columns, choose the double right arrow and click **OK**. The File Download dialog box appears displaying the default name assigned to the file and the .csv file extension. You can change the name of the file in Step 4.

Step 3 Click **Save**.

Step 4 In the Save As dialog box:

- In Save in, navigate to the folder in which you want to save this file.
- In File name, change the name of the file.

Step 5 Click **Save**. The CSV file appears in the new location.

When you open the file, you see the data as an editable Microsoft Excel worksheet. You might need to expand columns to view all the data.

Printing Reports

You can print a report that appears in the viewer in HTML or PDF format. Because you can modify the report in Interactive Viewer, Interactive Viewer supports printing either the original report or the report as you modify it.

Step 1 In the viewer, select **Print Report**. The Print dialog box appears.

Step 2 In Format field, select HTML or PDF.

Step 3 In the Page Range field, select the pages you want to print.

Step 4 Click **OK**.

Step 5 Depending on your format selection in Step 2, you have the following options:

- If you selected HTML format, a print dialog box appears in which you can specify printer options.
- If you selected PDF format, the report appears in a PDF viewer plug-in in your web browser. You can review the report then choose Print to specify printer options.

Saving Report Designs in Interactive Viewer

You can save a report design from Interactive Viewer when you are working in the design environment or in Interactive Viewer.

Step 1 Click **Save**. The Save dialog box appears. An example is shown inFigure 13-13.

Figure 13-13 Save Dialog Box

Step 2 Navigate to the location where you want to save the file. Then, type a file name and click **Save**.

Step 3 Click **OK** on the confirmation message that appears.

Formatting Reports in Interactive Viewer

You can use the Interactive Viewer to format reports.

This section contains the following topics:

- Editing Labels, page 13-26
- Formatting Labels, page 13-27
- Applying Conditional Formats, page 13-35
- Setting and Removing Page Breaks in Detail Columns, page 13-39

Editing Labels

Labels are fields that can contain static text, such as the report title and items of the footer. In a typical report, some labels are editable and others are not editable. For example, a template might provide a label to display a confidentiality statement and a label to display the report author's name in the report footer. The confidentiality statement is not editable but the author can insert his or her name in the footer.

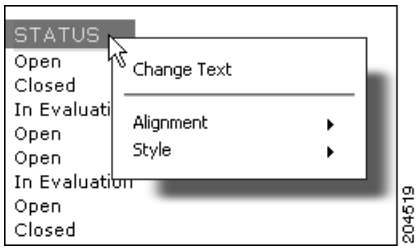
If a label such as a column header is editable, you can modify properties such as the font, the font size, the background color, and so on. You also can edit the text of the label.

The text of a **column header** comes from the data source. If the data source displays column headers in capital letters with no spaces between words, the report design displays column header names in the same way. You can change the content of the column header by using a context menu.

The formatting of the column header comes from the report template or from the theme. If the formatting comes from a report template, you cannot change the formatting. If the formatting comes from a theme, you can change the formatting by changing the theme.

Step 1 In Interactive Viewer, select and right-click a label. The context menu appears, as shown in Figure 13-14.

Figure 13-14 Interactive Viewer Context Menu



Step 2 Select **Change Text**. The Edit Text dialog box appears.

Step 3 Modify the text as desired and click **Apply**.

Formatting Labels

Step 1 To modify the formatting of a label, click on the label and then select **Style > Font**. The Font dialog box appears.

Step 2 Select the formats you desire, then click **Apply**.

Formatting Data

There are several ways to modify how the report data is formatted. You can:

- Resize a column.
- Change the alignment of data in a column.
- Hide, show, delete, or reorder columns.
- Specify that repeat values do not appear consecutively in a column.
- Filter the data values.
- Sort the data values.
- Modify the font, color, style, and other properties of the text.
- Specify that the column displays uppercase or lowercase.
- Modify the default formatting of the data value in an aggregate row.
- Format the data type. For example, if the column displays numbers, you can format the data as currency, percentages, or scientific numbers.

Resizing Columns

In the Interactive Viewer, you can change the width of the column and the alignment of the data in the column

Step 1 To change a column's width, select and right-click the column.

Step 2 Select **Column > Column Width** from the context menu.The Column Properties form appears.

Step 3 In Column Properties form, type the new column width, then click **Apply**.

Changing Column Data Alignment

To change the alignment of data in a column, right-click the column and select **Alignment** from the context menu. Then, choose one of the alignment options: Left, Center, or Right.

Formatting Data in Columns

The default formatting for column data comes from the data source. Typically, you modify the formatting of column data to enhance the appearance of the report. When you format column data, you create the same format for the entire column, except for the column header and aggregate rows. You cannot modify the data itself.

Step 1 Select and right-click a column. The context menu appears.

Step 2 Select **Style > Font**.

Step 3 In the Font form, modify any of the style properties you want to change. You can see your changes as you make them in the Preview field.

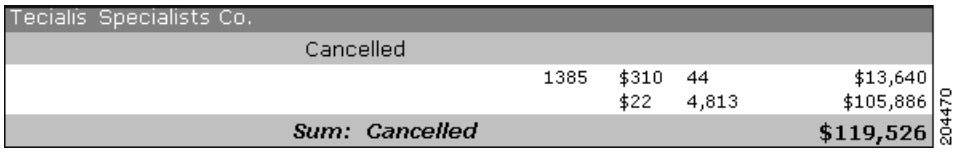
Step 4 Indicate whether to apply the new text style to all columns in the report or to the selected column. The default setting is to apply the new style to the column you selected.

Step 5 Click **Apply**.

Formatting Data in Aggregate Rows

An aggregate row displays a total, average, or other summary data for a column. You learn how to create an aggregate row in a later chapter. Figure 13-15 shows an aggregate row at the end of a report. Typically, the default formatting of the aggregate row comes from the template or the theme. You can modify the formatting of the aggregate data value and the formatting of the label that precedes the data value. You cannot modify the text of the label or the data value.

Figure 13-15 Formatting Data in an Aggregate Row



Step 1 Select an aggregate data value, then click **Font**. The Font dialog box appears.

Step 2 Modify the settings as desired, then click **Apply**.

Formatting Data Types

In an information object, as in the relational databases on which information objects are based, all the data in a column is of the same data type, excluding the column header. The column can display numeric data, date-and-time data, or string data. Each data type has a range of unique formats. Numeric data, for example, can appear as currency, percentages, or numbers with decimal values. Similarly, dates can be long dates, which include the full name of the month, or short dates, in which the month is represented by a number.

Table 13-6 shows the data type formats you can use. Most of the examples in the table reflect the U.S. English locale. If you work in a different locale, you can use the Custom format option to format data for your locale

Table 13-6 Data Types and Formats

Data type	Option	Description
Date and Time	Unformatted	The data retains the default format set by the template or theme.
	General Date	June 5, 2006 12:00:00 AM GMT +00:00
	Long Date	June 5, 2006
	Medium Date	Jun 5, 2006
	Short Date	6/5/06
	Long Time	12:00:00 AM GMT +00:00
	Medium Time	12:00:00 AM
	Short Time	12:00
	Custom	The format depends on a format code you type. For example, typing yyyy/mm results in 2006/10. You learn more about custom formatting later in this chapter.

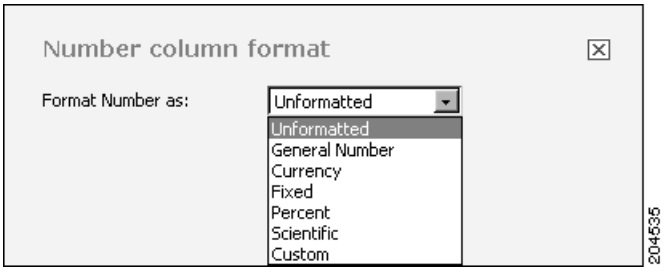
Table 13-6 Data Types and Formats (continued)

Data type	Option	Description
Number	Unformatted	The number retains the default format set by the template or theme.
	General Number	6066.88 or 6067, depending on the decimal and thousands separator settings
	Currency	$6,067.45 or ¥6067, depending on the locale and optional settings
	Fixed	6067 or 6,067 or 6067.45, depending on optional settings
	Percent	45% or 45.8%, depending on optional settings
	Scientific	2E04 or 2.67E04, where the number after the E represents the exponent of 10, depending on optional settings. For example, 2.67E04 means 2.67 multiplied by 10 raised to the fourth power.
	Custom	The format depends on a format code you type. For example, typing #,### results in a format with a comma as a thousands separator and no decimal points. You learn more about custom formats later in this chapter.
String	Unformatted	The string retains the default format set by the template or theme.
	Uppercase	The string displays in all uppercase, for example GREAT NEWS.
	Lowercase	The string displays in all lowercase, for example great news.
	Custom	The format depends on the format code you type. Use custom formatting for postal codes, telephone numbers, and other data that does not match standard formats.

Formatting Numeric Data

Numeric data can take several forms. A column of postal codes requires different formatting from a column of sales figures. Figure 13-16 shows the numeric formats you can use.

Figure 13-16 Formats for Numeric Data



The data type of a column is determined by the data source. Keep in mind that a text or string data type can contain numeric digits. A telephone number, for example, is frequently string data in the data source. The title of the formatting dialog box tells you what data type the column contains.

Step 1 Select a column that contains numeric data, then select **Format**. The Number column format dialog box appears.

Step 2 In the Format Number as field, select General Number, Currency, Fixed, Percent, or Scientific. The bottom section of Number column format displays fields that support that type of formatting.

Step 3 In Symbol field, select a currency symbol.

Step 4 In Symbol Position, select Before to place the currency or percentage symbol before the number. Select After to place the symbol after the number.

Step 5 In Decimal Places, select the number of places after the decimal marker to display

Step 6 Select **Use 1000s Separator** if you want to use a thousands separator such as a comma (,) or a period (.). Your locale settings determine the separator character.

Step 7 In Negative Numbers, select an option for displaying negative numbers, by using either a minus sign before the number or parentheses around the number.

Step 8 Click **Apply**.

Formatting Fixed or Scientific Numbers or Percentages

Step 1 Select a column that contains numeric data, then click **Format**. The Number column dialog box appears.

Step 2 In Format Number as field, select Fixed, Scientific, or Percent.

Step 3 In Decimal Places field, select the number of decimal places to display.

Step 4 Select **Use 1000s Separator** if you want to use a thousands separator such as a space, a comma (,), or a period (.).

Step 5 In Negative Numbers, select an option for displaying negative numbers: use a minus sign before the number, or use parentheses around the number.

Step 6 Click **Apply**.

Formatting Custom Numeric Data

To define a custom format, you use special symbols to construct a format pattern. A format pattern shows where to place currency symbols, thousands separators, decimal points or commas. Table 13-7 shows examples of custom format patterns and their effects on numeric data

Table 13-7 Results of Custom Number Format Patterns

Format pattern	Data in the data set	Result of formatting
0000.00	12.5 124.5 1240.553	0012.50 0124.50 1240.55
#.000	100 100.25 100.2567	100.000 100.250 100.257

Table 13-7 Results of Custom Number Format Patterns (continued)

Format pattern	Data in the data set	Result of formatting
$#,###	2000.00 20000.00	$2,000 $20,000
ID #	15	ID 15

Step 1 Select a numeric data column, then click **Format**. The Number column format appears.

Step 2 In the Format Number as field, select Custom from the drop-down list. A second field, Format Code, appears.

Step 3 In Format Code field, type a format pattern similar to those shown in Table 13-7.

Step 4 Click **Apply**.

Formatting String Data

Step 1 To define the format for a column that contains string data, select the column, then click **Format**. The String column format appears.

Step 2 Select an option from the drop-down list. See Table 13-6 for the standard string data type options.

Step 3 Click **Apply**.

Formatting Custom String Data

You can format string data to include special formatting, such as a space or a punctuation mark at a specific place in the string. For example, you can display telephone numbers in one of the following formats.

```
(415) 555-2121 ext. 2296
415.555.2121
415-555-2121
```

You can create custom formats for string data. Table 13-8 describes the symbols you can use to define custom string formats

Table 13-8 Symbols for Defining Custom String Formats

Symbol	Description
@	Character placeholder. Each @ character displays a character in the string. If the string has fewer characters than the number of @ symbols that appear in the format pattern, spaces appear. Placeholders are filled from right to left, unless you specify an exclamation point (!) at the beginning of the format pattern. See Table 13-9 for examples.
&	Same as @, except that if the string has fewer characters, spaces do not appear. See Table 13-9 for examples.

Table 13-8 Symbols for Defining Custom String Formats (continued)

Symbol	Description
!	Specifies that placeholders are to be filled from left to right. See Table 13-9 for examples.
>	Converts string characters to uppercase.
<	Converts string characters to lowercase.

Table 13-9 shows examples of custom string format patterns and their effects on text data.

Table 13-9 Results of Custom String Format Patterns

Format pattern	Data in the data source	Results of formatting
(@@@) @@@-@@@@	6175551007 5551007	(617) 555-1007 ( ) 555-1007
(&&&) &&&-&&&&	6175551007 5551007	(617) 555-1007 () 555-1007
!(@@@) @@@-@@@@	6175551007 5551007	(617) 555-1007 (555) 100-7
!(&&&) &&&-&&&&	6175551007 5551007	(617) 555-1007 (555) 100-7
!(@@@) @@@-@@@@ + ext 9	5551007	(555) 100-7 + ext 9
!(&&&) &&&-&&&& + ext 9	5551007	(555) 100-7 + ext 9
>&&&-&&&&&-&&	D1234567xy	D12-34567-XY
<&&&-&&&&&-&&	D1234567xy	d12-34567-xy

Step 1 Select a string data column, then click **Format**. The String column format window appears.

Step 2 In Format String as field, select Custom. A second field, Format Code, appears.

Step 3 In the Format Code field, enter a format pattern such as those shown in Table 13-9.

Step 4 Click **Apply**.

Formatting Date and Time

The appearance of date and time data depends on the locale in which you are working. For example, the following date and time are correct for the U.S. English locale for Pacific Standard Time zone:

```
March 5, 2007 11:00:00 AM PST
```

The following example shows the same date and time for a French (France) locale:

```
5 mars 2007 11:00:00 HNP (ÈUA)
```

In a date-and-time column, a data source can provide both a date and a time, or only the date, or only the time. If the data source provides both date and time data, you can format the column to display only a date, only a time, or both a date and a time. You also can select the exact format for the date or time. For example, if the data column displays the following value:

```
April 3, 2006 11:35 a.m.
```

selecting the Short Date format for the column displays only the date portion of the data, in the following format:

```
4/3/06
```

Table 13-6 shows the standard date-and-time data type formats.

Step 1 Select a column that contains date or time data, then click **Format**. The Date and Time Format window appears.

Step 2 In Format Date or Time As field, select the desired option.

Step 3 Click **Apply**.

Formatting Custom Date and Time

You can set custom date formats. Use custom date formatting, however, only if your report will be viewed in a single locale. Custom formats always display dates in the format you set and that format might not be clear in multiple locales. For example, if you use the format MM-dd-yy, the date January 10, 2006 always appears as 01-10-06, regardless of the locale in which the report is viewed. For locales in which dates are displayed in date-month-year format, a 01-10-06 date is interpreted as October 1, 2006.

Table 13-10 shows examples of custom formats and their effects on a date that is stored as 4/15/2006 in the data source.

Table 13-10 Results of Custom Date Formats

Format	Result of formatting
MM-dd-yy	04-15-06
E, M/d/yyyy	Fri, 4/15/2006
MMM d	Apr 15
MMMM	April
yyyy	2006
W	3 (the week in the month)
w	14 (the week in the year)
D	105 (the day in the year)

Step 1 To create a custom date or time format, select a date-and-time column, then click **Format**. The Date or Time column format window appears.

Step 2 In Format Date or Time As field, select Custom. A second field, Format Code, appears.

Step 3 In the Format Code field, type a format pattern such as those shown in Table 13-10.

Step 4 Click **Apply**.

Formatting Boolean Data

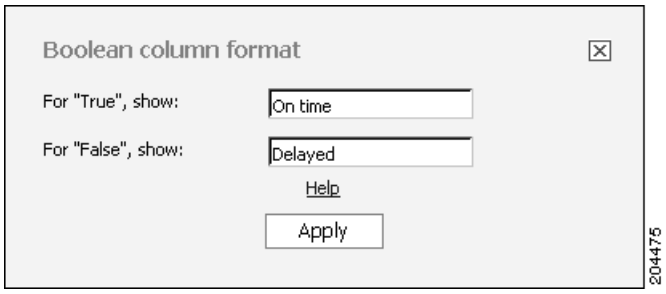
A Boolean expression evaluates to True or False. For example, you create a calculated column with the following expression:

```
ActualShipDate <= TargetShipDate
```

If the actual ship date is before or on the target ship date, the expression evaluates to True. If the actual ship date is after the target ship date, the expression evaluates to False.

If you do not format a column of Boolean data type, the column displays the values True and False. To specify different labels, select the column and choose Format Data. Then type the labels in Boolean Column Format, as shown in Figure 13-17.

Figure 13-17 Specifying Display Values for True and False



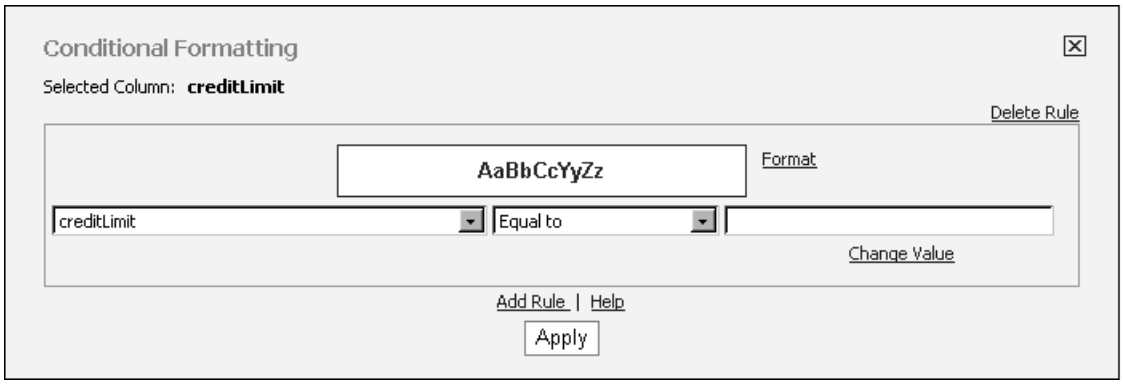
Applying Conditional Formats

Conditional formatting changes the formatting of data when a certain condition is true. For example, in a report that shows customers' past-due invoices, you can highlight in red any customer name that has an invoice 90 days or more past due. Then, you can highlight in blue any customer name that has an invoice 60 days or more past due.

To set conditional formats, open the Conditional Formatting dialog box by right-clicking a column and selecting **Style > Conditional Formatting**. You can set up to three conditional formatting rules for a single column. You also can remove or modify conditional formatting.

On Conditional Formatting, you create a rule, or condition, for displaying the data in the column you selected. The rule includes both the condition that must be true and the formatting to apply. Figure 13-18 shows Conditional Formatting.

Figure 13-18 Conditional Formatting in Interactive Viewer



You can affect the formatting of one column based on the value in another column. For example, if you select the CustomerName column, you can base the condition on the creditRank column so that conditional formatting applies to the customer name if the customer's creditRank is a particular value.

You set various types of comparisons, such as whether the data in the comparison column is null or false. You can also compare the column value to one or two other values. For example, you can specify that data that is less than or equal to a value triggers the conditional formatting. You also can check whether a value is between or not between two values. For example, you can specify conditional formatting to apply if the order total is between $10,000 and $100,000. With this setting, the names of all customers whose orders total between $10,000 and $100,000 take the conditional formatting.

After you create the condition, you set the format in which to display data that meets the condition. The format applies to the column in Select Column, not to the column you use to set the condition.

Setting Conditional Formatting for Columns

You can set conditional formatting or modify conditional formatting for a column.

Step 1 Right-click on the column that you want to display the conditional formatting. The context menu appears.

Step 2 Select **Style > Conditional Formatting**. The Conditional Formatting dialog box appears. The Selected Column field displays the name of the column that will display the conditional format.

Step 3 Set the conditional formatting rule:

a. In the first drop-down list, select the column that contains the values that determine whether the conditional format takes effect. For example, if the condition is that customer names should appear in blue if customer numbers are between 1000 and 1999, select CustomerNumber.

The column you select in this field can be the same as or different from the column in Selected Column.

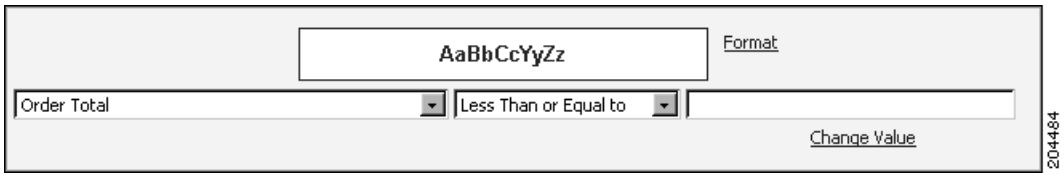
b. In the next field, use the drop-down list to select the operator to apply to the column you selected. You can select Equal to, Less than, Less than or Equal to, and so on.

Depending on your selection, zero, one, or two fields appear to the right. If you selected Is Null, Is Not Null, Is True, or Is False, zero fields appear to the right. If you selected an operator that requires a comparison between two values, one or more additional fields appear.

c. Enter a comparison value in each field that appears to the right, if any.

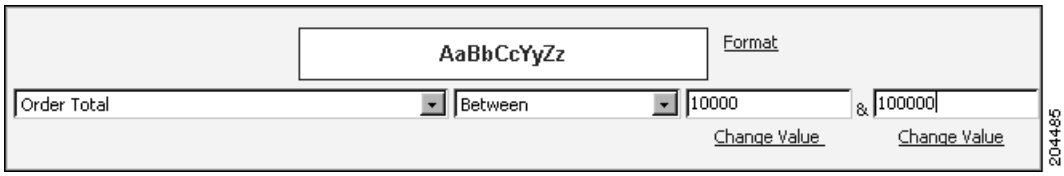
For example, if you selected Less than or Equal to, a third field appears, as shown in Figure 13-19. In this field, you type the comparison value. All data that is less than or equal to your value triggers the conditional formatting.

Figure 13-19 Comparison Value Field



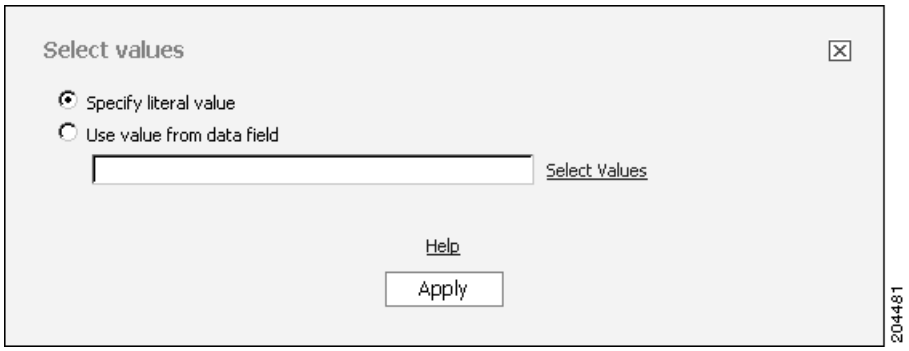
If you selected Between or Not Between, two fields appear to the right. In these fields, type the lower and upper values, respectively. For example, in the third field, type an order total of 10,000 and in the fourth field, type an order total of 100,000, as shown in Figure 13-20. The names of all customers whose orders total between $10,000 and $100,000 take the conditional formatting.

Figure 13-20 Two Comparison Value Fields Appear for the Between Operator



The values for the comparison can be typed in directly or derived from the specified report column. Select Change Value to display the Value dialog, as shown in Figure 13-21.

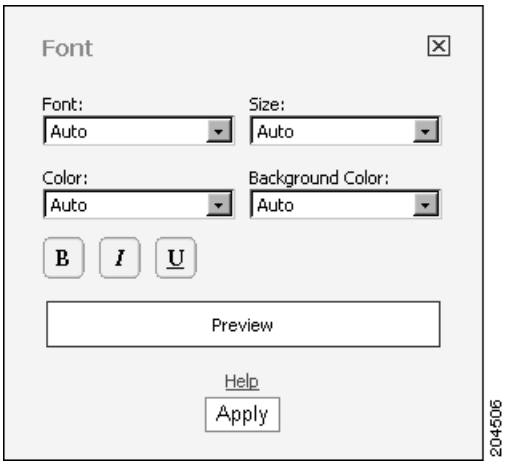
Figure 13-21 Specifying Literal or Column Values



A literal value can be directly typed or chosen from a list of values in the specified column. They also can be derived from the values in another specified column in the report.

Step 4 On Conditional Formatting, choose Format, and set the formatting for the conditional text. You can set the font, font size, font color, and background color. You also can specifying displaying the data in bold, italic, or underlined font style. You set the formatting by using the same Font dialog box used for formatting labels, as shown in Figure 13-22.

Figure 13-22 The Font Dialog Box



After you set the format, the Preview section of the window shows the formatting you selected.

Step 5 To add additional conditional formatting rules, select **Add Rule** and repeat steps 3 and 4 for each new rule.

Step 6 Click **Apply**. The report design appears with the specified conditional formatting applied.

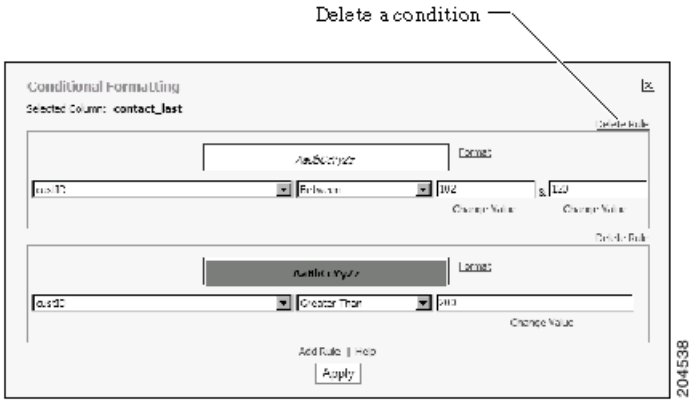
Deleting Conditional Formatting

Step 1 To remove conditional formatting for a column, select and right-click the column.

Step 2 Select **Style > Conditional Formatting**.

Step 3 In the Conditional Formatting dialog box, click **Delete Rule** for each conditional formatting rule you want to delete, as shown in Figure 13-23. To remove all conditional formatting for a column, delete all the conditional formatting rules.

Figure 13-23 Removing a Conditional Format in Interactive Viewer



Step 4 Click **Apply**.

Setting and Removing Page Breaks in Detail Columns

In Interactive Viewer, you can force page breaks after a preset number of rows.

Step 1 Select and right-click a detail column.

Step 2 From the context menu, select **Group > Page Break**. The Page Break window appears.

Step 3 In the Interval field, enter a numerical value for the row after which you want to force a page break.

Step 4 Click **Apply**.

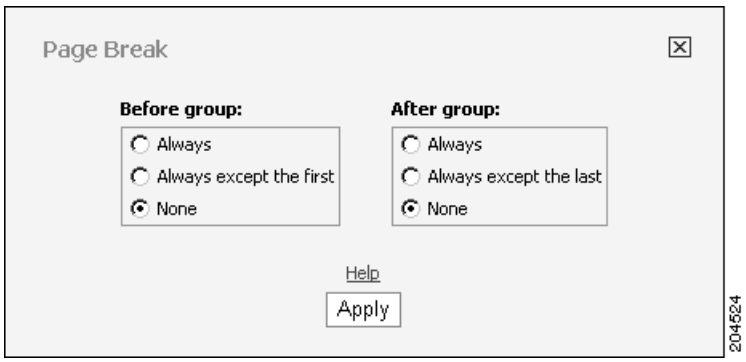
Setting and Removing Page Breaks in a Group Column

In Interactive Viewer, if your report design has grouped data, you can set page breaks before or after the grouped data.

Step 1 Select and right-click a grouped column.

Step 2 From the context menu, choose **Group > Page Break**. The Page Break window appears, as shown in Figure 13-24.

Figure 13-24 Setting a Page Break



Step 3 Specify whether to set a page break before every group, or for every group except the first or last groups. To delete an existing page break, select None in Before group or After group.

Step 4 Click **Apply**.

Organizing Report Data

You can use Interactive Viewer to organize report data.

This section contains the following topics:

- Displaying and Organizing Report Data, page 13-40
- Merging Columns, page 13-43
- Sorting Data, page 13-45
- Grouping Data, page 13-46
- Creating Report Calculations, page 13-49
- Working with Aggregate Data, page 13-60

Displaying and Organizing Report Data

After you access a data source and select the data set to use, you determine the best way to display the data in a report. There are several ways to organize data sets:

- Sort a data column in ascending or descending order.
- Organize data into groups. A group displays all the information about a type of item in one place. For example, you can display all the information about one customer, then all the information about the next customer, and so on.
- Create aggregate data. At the end of a customer group, for example, you can display the total amount of the customer's purchases or the average amount of each order. You can also create calculations, such as sums, standard deviations, rankings, and differences.

Reordering Columns in Interactive Viewer

Step 1 Select and right-click a column.

Step 2 From the context menu, select **Column > Reorder Columns**. The Arrange Columns window appears

Step 3 Select the column you want to move.

Note You can select only detail rows, not groups or sections.

Step 4 Click the up or down arrows at the right until the column is in the correct position.

Step 5 Click **Apply**.

Moving Data Values from Columns to Group Headers

You can move data values from the details rows of a column to column headers.

Step 1 Select and right-click on a column. For example, Figure 13-25 shows the customer Name column as the selected column.

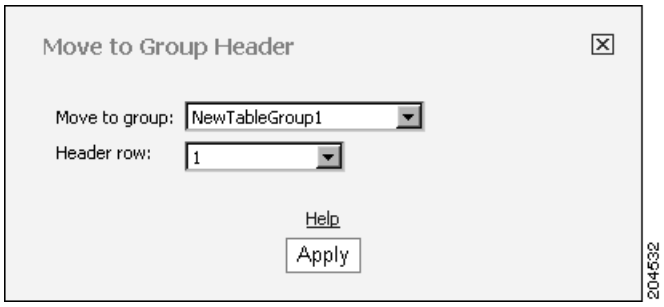
Figure 13-25 Report Displaying Customers Grouped by Country

	Customer Number	Name	City	State	Sales Volume	Credit Limit
⊟ Australia						
	114	Alustrian Collectors, Co.	Melbourne	Victoria	1611	117300
	276	Anna's Decorations, Ltd	North Sydney	NSW	1611	107800
	282	Souveniers And Things Co.	Chatswood	NSW	1611	93300
	333	Alustrian Gift Network, Co	South Brisbane	Queensland	1611	51600
	471	Alustrian Collectables, Ltd	Glen Waverly	Victoria	1611	60300
⊟ Austria						
	382	Salzburg Collectables	Salzburg		1401	71700
	452	Mini Auto Werke	Graz		1401	45300

204533

Step 2 Select **Column > Move to Group Header**. The Move to Group Header window appears, as shown in Figure 13-26.

Figure 13-26 Move to Group Header Dialog Box



Step 3 From the Move to Group field, select a value.

Step 4 In the Header row field, select the row number in which to move the value you selected in Step 3.

Step 5 Click **Apply**. The data value from the first detail row in each group appears in each group header, as shown in Figure 13-27. The Name column displays one customer name beside each country group header.

Figure 13-27 Report Displaying Customer Name in Each Group Header

	Name	Customer Number	City	State	Sales Volume	Credit Limit
⊟ Australia	Alustrian Collectors, Co.					
		114	Melbourne	Victoria	1611	117300
		276	North Sydney	NSW	1611	107800
		282	Chatswood	NSW	1611	93300
		333	South Brisbane	Queensland	1611	51600
		471	Glen Waverly	Victoria	1611	60300
⊟ Austria	Salzburg Collectables					
		382	Salzburg		1401	71700
		452	Graz		1401	45300

204534

Removing Columns

To remove a column, select the column and click **Delete**. When you remove a column from the report, you are not deleting the column from the information object or other data source.

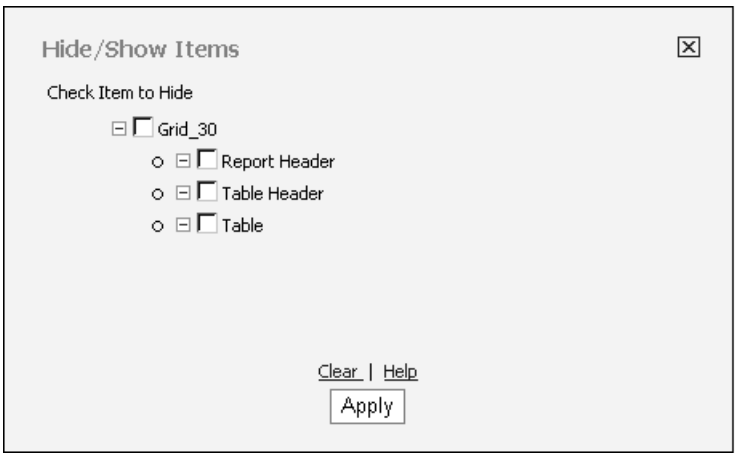
To remove multiple columns, press Ctrl and select the columns to remove. Then, click **Delete**.

Hiding or Displaying Report Items

Step 1 Select and right-click a column.

Step 2 Select **Hide or Show Items.** The Hide or Show Items dialog box appears, similar to Figure 13-28.

Figure 13-28 Hiding or Displaying Report Items



Step 3 Select any items you want to hide. Deselect any hidden items you want to display. To display all hidden items, click **Clear**.

Step 4 Click **Apply**.

Hiding Columns

Step 1 Select and right-click a column.

Step 2 Select **Column > Hide Column**. Interactive Viewer displays the report without the hidden column.

Displaying Hidden Columns

Step 1 Select and right-click a column.

Step 2 Select **Column > Show Columns**. The Show Columns dialog box appears.

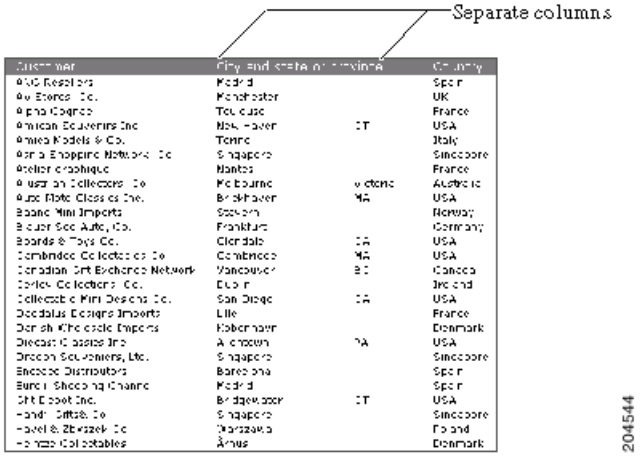
Step 3 Select any items you want to display. Use Ctrl to select several columns.

Step 4 Click **Apply**.

Merging Columns

You can merge the data from two or more columns into one column. For example, in Figure 13-29 the columns under the City and state or province column header are separate.

Figure 13-29 Separate Columns



In Figure 13-30, the data from these two columns is merged into one column.

Figure 13-30 Merged Column

Customer	City and state or province	Country
ANG Resellers	Madrid	Spain
AV Stores, Co.	Manchester	UK
Alpha Cognac	Toulouse	France
American Souvenirs Inc	New Haven CT	USA
Amica Models & Co.	Torino	Italy
Asnia Shopping Network, Co	Singapore	Singapore
Atelier graphique	Nantes	France
Alustrian Collectors, Co.	Melbourne Victoria	Australia
Auto-Moto Classics Inc.	Brickhaven MA	USA
Baane Mini Imports	Stavern	Norway
Blauer See Auto, Co.	Frankfurt	Germany
Boards & Toys Co.	Glendale CA	USA
Cambridge Collectables Co.	Cambridge MA	USA

204530

Step 1 To merge data in multiple columns, select and right-click the columns

Step 2 Select **Column > Merge Columns**.

Selecting a Column from a Merged Column

You can aggregate, filter, and group data in a column that contains data that is merged from multiple columns. You must first select one of the columns on which to aggregate, filter, or group data.

Step 1 To select one column from a merged column, select and right-click the merged column, then select a command to apply from the context menu, such as **Aggregation**, **Filter > Filter**, or **Group > Add Grou**p.

The Select data item dialog box appears.

Step 2 From the Select data drop-down list, select the column name to which you want to apply the command, then click **Apply**.

If you must provide more information to apply a command, Interactive Viewer displays a dialog box. For example, if you choose Aggregation, the Aggregation dialog box appears.

Sorting Data

When you place data in a report design, the data source determines the default sort order for the data rows. If the data source sorts a column in ascending order, the column is sorted in ascending order in the design. Typically, however, data appears randomly in the data source. A column is likely to display customer names, for example, in the order in which the customers were added to the database, rather than in alphabetical order. Sorting data, therefore, is an important task in creating a useful report.

There are three ways to sort data:

- Sorting a Single Column, page 13-45
- Sorting Multiple Columns, page 13-45

Sorting a Single Column

To perform a simple sort on a single column, select a column and select either **Sort Ascending** or **Sort Descending**. All the data rows in the report adjust to reflect the new sort order.

To return the data to its original order after performing a simple sort, choose Undo.

Sorting Multiple Columns

You can sort multiple columns in a report.

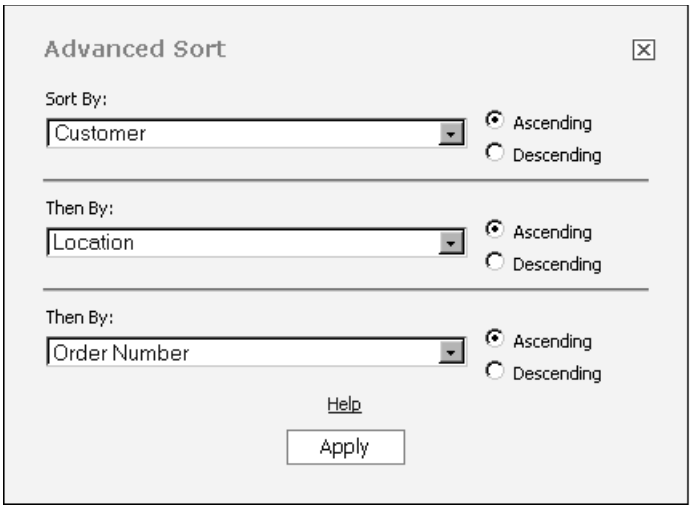
Step 1 Select and right-click a column.

Step 2 From the Context menu, select **Sort > Advanced Sort**.

Step 3 Select a column from the first drop-down list and choose either Ascending or Descending order. Select the next column and choose a sort order, and so on.

When you sort multiple columns, it is important to understand the order of precedence for the sort. In Advanced Sort, the first column you select is the primary sorting column. Report data is sorted first by this column. If the primary column is Customer and the order is Ascending, for example, the report displays customers in alphabetical order. If you select Location as the next column and the order is Ascending, then within each Customer entry, the locations are sorted in ascending order. If the third column you select is Order Number and the order is Ascending, then within each location, the order numbers are sorted in ascending order. Figure 13-31 shows the result of this multiple-column sort.

Figure 13-31 Sorting Multiple Columns



Customer	Location	Order Number	Order Status	Unit Price	Quantity	Order Totals
Barginton Financial	Boston	1555	Open	$4	212	$848
		1625		$6	158	$948
				$8	161	$1,288
				$11	160	$1,760
				$11	161	$1,771
				$12	159	$1,908
	New Haven	1570		$9	215	$1,935
				$15	157	$2,355
				$15	157	$2,355
Chardlen Corporation	Dallas	1345		$12	210	$2,520
				$18	158	$2,844
	Sacramento	1621		$15	210	$3,150
				$20	158	$3,160
				$21	159	$3,339

204547

If the report uses grouped data, the drop-down lists in Advanced Sort show only the detail columns in the report, not the columns you used to group the data.

Grouping Data

A report can contain a great deal of data. Consider the task of listing every item a corporation owns, along with information such as the purchase price, purchase date, inventory tag number, and the supplier for each item. If a report simply presents all these items in an unorganized list, there is no way to determine how much the corporation spends for heavy equipment because heavy equipment items are scattered throughout the report. The report cannot help you see which supplier sells office furniture at the lowest prices. Nor is it easy to tell which inventory items are located at a field office and which items are in the warehouse. Figure 13-32 shows the first page of an ungrouped report.

Figure 13-32 Ungrouped Data

Item	Category	Inventory Code	Description	Building Location	Office Location	Purchase Price	Purchase Date	Supplier
Executive desk with return	Office Furniture	1007-431	Mahogany, 71" x 28", 4 drawers	Bldg 1	Office 601	789.99	2/1/2004	Grant Furniture
Forklift	Equipment	219-62389	3000 lb capacity, model 3398	Warehouse A		1594.78	3/6/2004	Grant Furniture
Wing chair	Office Furniture	1509-4459	Dark brown leather with stud trim	Bldg 1	Lobby A	259.98	1/17/2005	Grant Furniture
Light tower	Heavy Equipment	4408-3221	2002 Genie TML4000N	Warehouse C		4200.00	1/6/2003	Sal's Dining Rooms
Credenza	Office Furniture	336-9887	Mahogany, 64" x 36" x 48", 6 drawers	Bldg 1	Office 601	449.75	2/1/2004	Grant Furniture
Air compressor	Heavy Equipment	3398-9907	Diesel, 185 CFM	Warehouse C		9500.00	3/6/2004	Grant Furniture
Dining table	Cafeteria Furniture	1248-4339	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Secretary's chair	Office Furniture	1005-4498	Black ergonomic chair	Bldg 2	Office 422	149.99	3/2/2002	Sal's Dining Rooms
Conference table	Office Furniture	1098-7543	Oval mahogany table, 8 ft x 5 ft x 30"	Bldg 1	Board room	1459.98	4/17/2002	Grant Furniture
Credenza	Office Furniture	336-9887	Mahogany, 64" x 36" x 48, 6 drawers	Bldg 1	Office 403	449.75	2/1/2004	Grant Furniture
Forklift	Equipment	219-66737	5,000 lb capacity, model 2890	Warehouse A		2200.78	3/6/2004	Sal's Dining Rooms
Dining table	Cafeteria Furniture	1248-4401	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Dining table	Cafeteria Furniture	1248-4335	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Wing chair	Office Furniture	1508-3389	Dark brown leather with stud trim	Bldg 1	Lobby A	259.98	1/17/2005	Sal's Dining Rooms
Executive desk with return	Office Furniture	1004-322	Steel, 71" x 36", 3 drawers	Bldg 2	Office 423	629.29	3/3/2005	Grant Furniture
Credenza	Office Furniture	336-9887	Mahogany, 64" x 36" x 48, 6 drawers	Bldg 1	Office 423	449.75	2/1/2004	Sal's Dining Rooms
Executive desk with return	Office Furniture	1005-2112	Mahogany, 71" x 28", 4 drawers	Bldg 1	Office 604	789.99	2/1/2004	Sal's Dining Rooms
Secretary's chair	Office Furniture	1005-4498	Black ergonomic chair	Bldg 2	Office 422	149.99	3/2/2002	Sal's Dining Rooms
Crawler loader	Heavy equipment	2020-3731	Model 450D	Warehouse A		9200.00	6/04/2003	Grant Furniture

204513

To organize all this information into a useful inventory report, you create data groups and data sections. Data groups contain related data rows. For example, you can create a report that lists all heavy equipment in one group, all office furniture in another group, all telephony equipment in a third group, and so on. For each group, you can show aggregate data, such as the total purchase price or a count of the items in a group. Grouping data gives your report a more polished, organized look and makes it easier to create useful comparisons and calculations.

Figure 13-33 shows the same inventory, grouped according to the category, with one category on each page.

Figure 13-33 Grouped Data

Category: Cafeteria Furniture							
Item	**Inventory Code**	**Description**	**Building Location**	**Office Location**	**Purchase Price**	**Purchase Date**	**Supplier**
Dining table	1248-4339	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Dining table	1248-4401	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Dining table	1248-4335	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Dining table	1248-4492	Gray laminate table, round, seats 4	Bldg 1	Cafeteria	128.98	10/12/2002	Sal's Dining Rooms
Total purchase price					515.92		

204512

You can group data in the report design editor or in Interactive Viewer. The changes you make in the viewer do not affect the report design. If you work in Enterprise mode, you can save report output that reflects your changes.

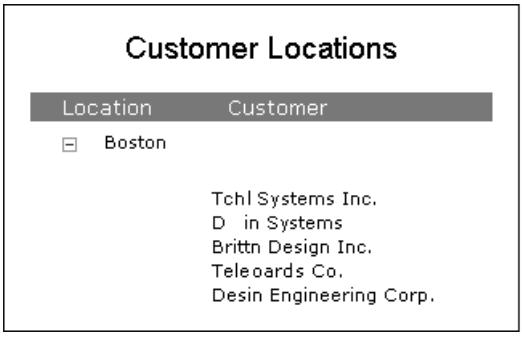
You can add or remove data groups in Interactive Viewer if the report design does not contain the grouping desired during that use of Interactive Viewer.

Adding Groups

Step 1 Select and right-click the column you want to use to create a group.

Step 2 From the Context menu, select **Group > Add Group**. The new group appears in the viewer. As shown in Figure 13-34, the group expands to show all the detail rows. To collapse the group, click the minus sign (-) beside the group name.

Figure 13-34 Adding a Group



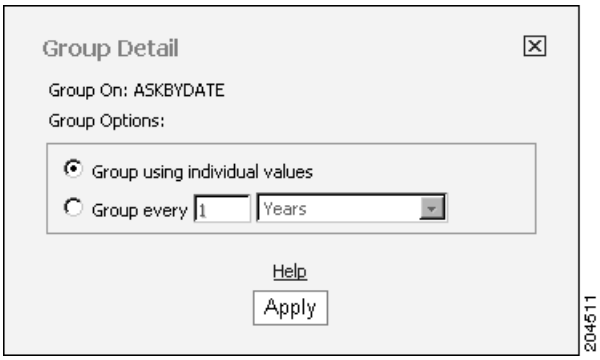
Grouping Data Based on Date or Time

When you create a group based on a column that contains date or time data, you have the option of setting a grouping interval. For example, if the column contains time data, you can group on hours, minutes, or seconds.

Step 1 Select and right-click the column you want to use to create a group.

Step 2 From the context menu, select **Group > Add Group**. The Group Detail dialog box appears, as shown in Figure 13-35.

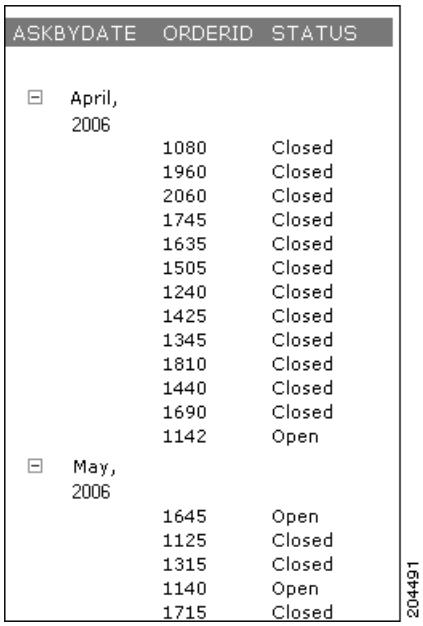
Figure 13-35 Grouping Date or Time Data



Step 3 To show every date or time value, leave the default setting **Group using individual values**.

Step 4 To set a grouping interval, select **Group every** and enter a value and select the grouping interval. For example, to create a new group for every month, type 1 and select Month from the drop-down list. The report displays monthly data groups, as shown in Figure 13-36.

Figure 13-36 Data Grouped by Month



Removing an Inner Group

Step 1 Select and right-click the column for the group you want to remove.

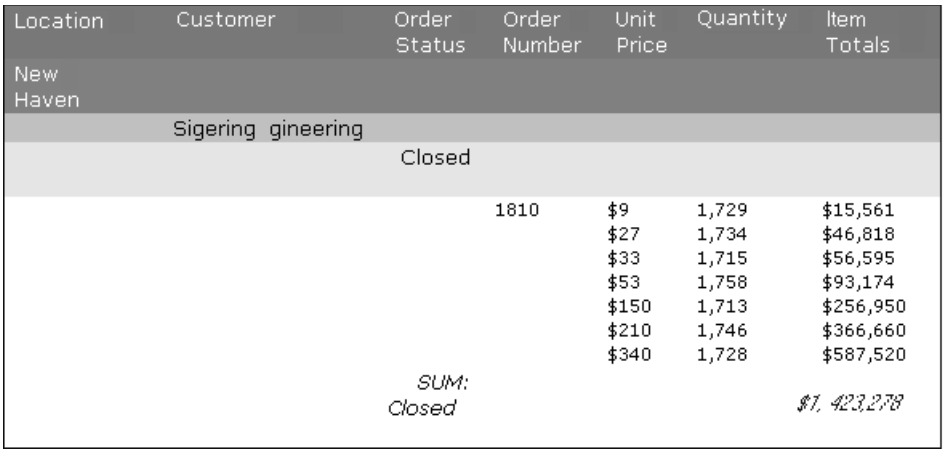
Step 2 From the context menu, select **Group > Delete Inner Group**.

Creating Report Calculations

Most reports require some sort of calculations to track sales, finances, inventory, and other critical business activities. You might want to keep a simple count of items in a warehouse or you might need to provide more complex financial data such as tracking stock portfolio performance over time. You can use typical mathematical functions such as counting, addition, subtraction, multiplication, and division. In addition, you can write expressions that extend these basic functions.

To display calculated data in a report, you create a calculated column, such as the one shown in Figure 13-37. In this illustration, the Item Totals column displays the product of the unit price times the quantity.

Figure 13-37 Calculated Column



Location	Customer	Order Status	Order Number	Unit Price	Quantity	Item Totals
New Haven						
	Sigering gineering					
		Closed				
			1810	$9	1,729	$15,561
				$27	1,734	$46,818
				$33	1,715	$56,595
				$53	1,758	$93,174
				$150	1,713	$256,950
				$210	1,746	$366,660
				$340	1,728	$587,520
		SUM: Closed				$1,423,278

204477

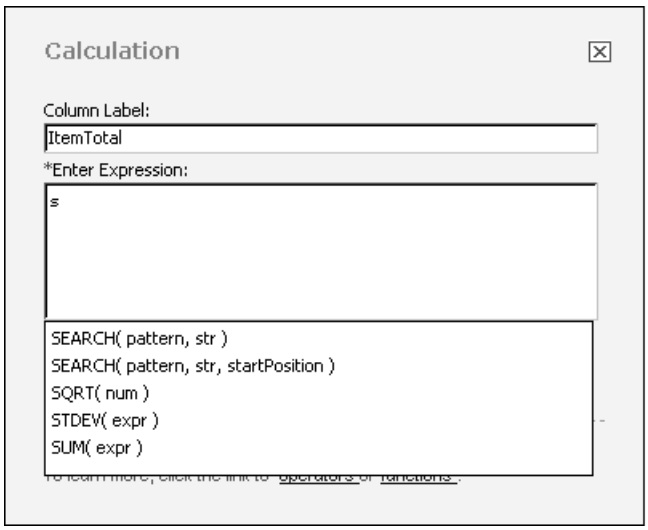
To create a calculation, you

- Provide a title for the calculated column.
- Write an expression that indicates which data to use and how to display the calculated data in the report.

  The expression contains a function and one or more arguments. Arguments indicate the data you want to use to create the calculation.

  As shown in Figure 13-38, when you type the first letter of a function name in Enter Expression, Calculation presents a list of functions that begin with that letter. You select a function and provide the arguments.

Figure 13-38 Selecting a Function



Understanding Supported Calculation Functions

Table 13-11 provides examples of the functions you can use to create calculations.

Note The Calculation dialog box does not support the use of uppercase TRUE and FALSE functions in expressions.Calculation also does not support the use of initial capital letters for True and False. These functions must be expressed in lowercase only.

Table 13-11 Examples of Functions

Function	Description	Example of use
ABS(num)	Displays an absolute value for the data in a column.	`ABS([TemperatureCelsius])`
ADD_DAY(date, daysToAdd)	Adds a specified number of days to a date value and displays the result as a date value.	`ADD_DAY([ClosingDate], 30)`
ADD_HOUR(date, hoursToAdd)	Adds a specified number of hours to a time value and displays the result as a time value.	`ADD_HOUR([OpenHour], 8)`
ADD_MINUTE(date, minutesToAdd)	Adds a specified number of minutes to a time value and displays the result as a time value.	`ADD_MINUTE([StartTime], 60)`
ADD_MONTH(date, monthsToAdd)	Adds a specified number of months to a date value and displays the result as a date value.	`ADD_MONTH([InitialRelease], 2)`
ADD_QUARTER(date, quartersToAdd)	Adds a specified number of quarters to a date value.	`ADD_QUARTER([ForecastClosing], 2)`
ADD_SECOND(date, secondsToAdd)	Adds a specified number of seconds to a time value.	`ADD_SECOND([StartTime], 30)`
ADD_WEEK(date, weeksToAdd)	Adds a specified number of weeks to a date value and displays the result as a date value.	`ADD_WEEK([askByDate], 4)`
ADD_YEAR(date, yearsToAdd)	Adds a specified number of years to a date value.	`ADD_YEAR([HireDate], 5)`
AND	Combines two conditions and returns records that match both conditions. For example, you can request records from customers who spend more than $50,000 a year and also have a credit rank of A.	This function is used to connect clauses in an expression and does not take arguments.
AVERAGE(expr)	Displays an average value for the column.	`AVERAGE([CostPerUnit])`
AVERAGE(expr, groupLevel)	Displays the average value at the specified group level.	`AVERAGE([TotalCost], 2)`
BETWEEN(value, upperBound, lowerBound)	For a specified column, displays true if a value is between two specified values and false otherwise. String values and date or time values must be enclose in quotation marks. For dates and times, use the short date and short time formats.	`BETWEEN([PostalCode], 11209, 12701)` `BETWEEN([ReceiptDate], "10/01/06", "12/31/06")`
CEILING(num, significance)	Rounds a number up, away from 0, to the nearest specified multiple of significance. For data that has been converted from a double or float to an integer, displays the smallest integer that is greater than or equal to the float or double.	`CEILING([PortfolioAverage], 1)`
COUNT( )	Counts the rows in a table.	`COUNT( )`
COUNT(groupLevel)	Counts the rows at the specified group level.	`COUNT(2)`

Table 13-11 Examples of Functions (continued)

Function	Description	Example of use
COUNTDISTINCT(expr)	Counts the rows that contain distinct values in a table.	`COUNTDISTINCT([CustomerID])` `COUNTDISTINCT([Volume]*2)`
COUNTDISTINCT (expr, groupLevel)	Counts the rows that contain distinct values at the specified group level.	`COUNTDISTINCT([CustomerID], 3)`
DAY(date)	Displays the number of a day in the month, from 1 to 31, for a date-and-time value.	`DAY([forecastShipping])`
DIFF_DAY(date1, date2)	Displays the difference between two date values, in the number of days.	`DIFF_DAY([checkoutDate], [returnDate])`
DIFF_HOUR(date1, date2)	Displays the difference between two time values, in the number of hours.	`DIFF_HOUR([StartTime],[Finish Time])`
DIFF_MINUTE(date1, date2)	Displays the difference between two time values, in the number of minutes.	`DIFF_MINUTE([StartTime], [FinishTime])`
DIFF_MONTH(date1, date2)	Displays the difference between two date values, in the number of months.	`DIFF_MONTH([askByDate], [shipByDate])`
DIFF_QUARTER(date1, date2)	Displays the difference between two date values, in the number of quarters.	`DIFF_QUARTER([PlanClosing], [ActualClosing])`
DIFF_SECOND(date1, date2)	Displays the difference between two time values, in the number of seconds.	`DIFF_SECOND([StartTime], [FinishTime])`
DIFF_WEEK(date1, date2)	Displays the difference between two weeks as a number.	`DIFF_WEEK([askByDate], [shipByDate])`
DIFF_YEAR(date1, date2)	Displays the difference between two years as a number.	`DIFF_YEAR([HireDate], [TerminationDate])`
false	The Boolean false. This function is used in expressions to indicate that an argument is false.	In the following example, false indicates that the second argument, ascending, is false and therefore the values should be returned in descending order. `RANK([Score], false)`
FIND(strToFind, str)	Displays the index of the first occurrence of specified text. The index is zero-based. The search is case sensitive and the search string cannot include wildcards. The value in the strToFind argument must be enclosed in quotation marks.	`FIND("HQ", [OfficeName])`
FIND(strToFind, str, startPosition)	Similar to FIND(strToFind, str) but supports providing a start position for the search. The index is zero-based.	`FIND("HQ", [OfficeName], 3)`
FIRST(expr)	Places the first value that appears in a specified column into the calculated column. This function supports viewing a row-by-row comparison against a specific value.	`FIRST([customerID])`
FIRST(expr, groupLevel)	Displays the first value that appears in the specified column at the specified group level.	`FIRST([customerID], 3)`

Table 13-11 Examples of Functions (continued)

Function	Description	Example of use
IF(condition, doIfTrue, doIfFalse)	Displays the result of an If...Then...Else statement.	`IF([purchaseVolume] >5 , 7 , 0)` where • [purchaseVolume] is the column name and >5 is the test condition. • 7 is the value to place in the new column if the condition is true. • 0 is the value to place in the new column if the condition is false.

IN(value, check)	Displays true if a data row contains a value specified by the check argument and false otherwise. String values and date or time values must be enclosed in quotation marks. For dates and times, use the short date and short time formats for your locale.	`IN([custID], 101)`
		`IN([city], "New Haven")`
		`IN([FinishTime], "16:09")`

IN(value, check1, ..., checkN)	Displays true if a data row contains any value specified by the check argument list and false otherwise. String values and date or time values must be enclosed in quotation marks. For dates and times, use the short date and short time formats for your locale.	`IN([city], "New Haven", "Baltimore", "Cooperstown")` `IN([ShipDate], "05/01/06", "05/10/06", "05/15/06")`
ISBOTTOMN(expr, n)	Displays true if the value is within the lowest *n* values for the expression, and false otherwise.	`ISBOTTOMN([OrderTotals], 50)`
ISBOTTOMN(expr, n, groupLevel)	Displays true if the value is within the lowest *n* values for the expression at the specified group level, and false otherwise.	`ISBOTTOMN([OrderTotals], 50, 2)`
ISBOTTOMNPERCENT (expr, percent)	Displays the lowest *n* percentage.	`ISBOTTOMNPERCENT([Sales Total], 5)`
ISBOTTOMNPERCENT (expr, percent, groupLevel)	Displays the lowest *n* percentage for the expression at the specified group level.	`ISBOTTOMNPERCENT([Sales Total], 5, 3)`
ISNULL(value)	Displays true if a row does not display a value. Displays false if a row displays a value.	`ISNULL([DepartmentName])`
ISTOPN(expr, n)	Displays true if the value is within the highest *n* values for the expression, and false otherwise.	`ISTOPN([OrderTotals], 10)`
ISTOPN(expr, n, groupLevel)	Displays true if the value is within the highest *n* values for the expression at the specified group level, and false otherwise.	`ISTOPN([OrderTotals], 10, 3)`
ISTOPNPERCENT(expr, percent)	Displays true if the value is within the highest *n* percentage, and false otherwise.	`ISTOPNPERCENT([SalesTotals], 5)`
ISTOPNPERCENT(expr, percent, groupLevel)	Displays true if the value is within the highest *n* percentage values for the expression at the specified group level, and false otherwise.	`ISTOPNPERCENT([SalesTotals], 5, 3)`
LAST(expr)	Displays the last value in a specified column.	`LAST([FinishTime])`

Table 13-11 Examples of Functions (continued)

Function	Description	Example of use
LAST(expr, groupLevel)	Displays the last value for the expression at the specified group level.	`LAST([FinishTime], 3)`
LEFT(str)	Displays the character at the left of the specified string.	`LEFT([city])`
LEFT(str, n)	Displays the specified number of characters in a column's string, counting from the left.	`LEFT([city], 3)`
LEN(str)	Displays the length of a string, including spaces and punctuation marks.	`LEN([Description])`
LIKE(str)	Displays true if the values match, and false otherwise. Use SQL syntax to specify the string pattern. The following rules apply: • Literal pattern characters must match exactly. LIKE is case-sensitive. • A percent character (%) matches zero or more characters. • An underscore character (_) matches any single character. • Escape a literal percent, underscore, or backslash character (\) with a backslash character.	`LIKE([customerName], "D%")` `LIKE([quantityOrdered], "2_")`
LOWER(str)	Displays the string in a specified column in lowercase.	`LOWER([cityName])`
MAX(expr)	Displays the highest value in the specified column.	`MAX([OrderTotal])`
MAX(expr, groupLevel)	Displays the highest value for the expression at the specified group level.	`MAX([OrderTotal], 2)`
MEDIAN(expr)	Displays the median value in a specified column.	`MEDIAN([HomePrices])`
MEDIAN(expr, groupLevel)	Displays the median value for the expression at the specified group level.	`MEDIAN([HomePrices], 2)`
MIN(expr)	Displays the lowest value in the specified column.	`MIN([OrderTotal])`
MIN(expr, groupLevel)	Displays the lowest value for the expression at the specified group level.	`MIN([OrderTotal], 1)`
MOD(num, div)	Displays the remainder after a number is divided by a divisor. The result has the same sign as the divisor.	`MOD([Salary], 12)`
MONTH(date)	Displays the name of the month for a specified date-and-time value.	`MONTH([ForecastShipDate])`

Table 13-11 Examples of Functions (continued)

Function	Description	Example of use
MONTH(date, option)	Displays the month of a specified date-and-time value, in one of three optional formats: • 1 - Displays the month number of 1 through 12. • 2 - Displays the complete month name in the user's locale. • 3 - Displays the abbreviated month name in the user's locale.	`MONTH([Semester], 2)`
MOVINGAVERAGE (expr, window)	Displays an average value over a specified window, such as an average price or volume over a number of days.	`MOVINGAVERAGE([Price], [Days])`
NOTNULL(value)	For a specified column, displays true if a data value is not empty. Displays false if a data value is empty.	`NOTNULL([DepartmentID])`
NOW( )	Displays the current time stamp.	`NOW([PastDueDate])`
OR	The logical OR operator.	This function is used to connect clauses in an expression and does not take arguments.
PERCENTILE(expr, pct)	Displays a percentile value, a value on a scale of 100 that indicates the percent of a distribution that is equal to or below the specified value. Valid pct argument ranges are 0 to 1. 0 returns the minimum value of the series. 1 returns the maximum value of the series.	`PERCENTILE([Rank], 1)`
PERCENTILE(expr, pct, groupLevel)	Displays a percentile value for the expression at the specified group level. Valid pct argument ranges are 0 to 1. 0 returns the minimum value of the series. 1 returns the maximum value of the series.	`PERCENTILE([Income], 60, 1)`
PERCENTRANK(expr)	Displays the percentage rank of a value.	`PERCENTRANK([TestScores])`
PERCENTRANK(expr, groupLevel)	Displays the percentage rank of a value at the specified group level.	`PERCENTRANK([TestScores], 2)`
PERCENTSUM(expr)	Displays a value as a percentage of a total.	`PERCENTSUM([OrderTotals])`
PERCENTSUM(expr, groupLevel)	Displays a value as a percentage of a total at the specified group level.	`PERCENTSUM([OrderTotals], 3)`
QUARTER(date)	Displays the quarter number, from 1 through 4, of a specified date-and-time value.	`QUARTER([ForecastCloseDate])`
QUARTILE(expr, quart)	Displays the quartile value, where the quart argument is an integer between 0 and 4.	`QUARTILE([OrderTotal], 3)`
QUARTILE(expr, quart, groupLevel)	Displays the quartile value for the expression at the specified group level, where the quart argument is an integer between 0 and 4.	`QUARTER([OrderTotal], 2, 3)`
RANK(expr)	Displays the rank of a number, string, or date-and-time value, starting at 1. Duplicate values receive identical rank but the duplication does not affect the ranking of subsequent values.	`RANK([AverageStartTime])`

Table 13-11 Examples of Functions (continued)

Function	Description	Example of use
RANK(expr, ascending, groupLevel)	Displays the rank of a number, string, or date-and-time value in either ascending or descending order, at the specified group level. To display values in ascending order, use true as the second argument. To display values in descending order, use false as the second argument.	`RANK([Score], false, 3)` `RANK([Score], true, 2)`
RIGHT(str)	Displays the character at the right of a string.	`RIGHT([name])`
RIGHT(str, n)	Displays the specified number of characters in a string, counting from the right.	`RIGHT([name], 3)`
ROUND(num)	Rounds a number.	`ROUND([SalesTarget])`
ROUND(num, dec)	Rounds a number to the specified number of digits. The default value for dec is 0.	`ROUND([StockValue], 2)`
ROUNDDOWN(num)	Rounds a number down.	`ROUNDDOWN([StockPrice])`
ROUNDDOWN(num, dec)	Rounds a number down, away from 0, to the specified number of digits. The default value for dec is 0.	`ROUNDDOWN([StockPrice], 2)`
ROUNDUP(num)	Rounds a number up.	`ROUNDUP([TotalValue])`
ROUNDUP(num, dec)	Rounds a number up, away from 0, to the specified number of digits. The default value for dec is 0.	`ROUNDUP([TotalValue], 2)`
RUNNINGSUM(expr)	Displays a running total, adding the values in successive data rows.	`RUNNINGSUM([StockValue])`
SEARCH(pattern, str)	Case-insensitive search function that can use wildcard characters. An asterisk (*) matches any sequence of characters, including spaces. A question mark (?) matches any single character.	The following search yields New York, New Haven, and so on from the City column: `SEARCH([CustomerData:city], "new*")`
SEARCH(pattern, str, startPosition)	Searches for a specified pattern in a string, starting at a specified position in the string. A case-insensitive search function that can use wildcard characters.	`SEARCH([Location], "new", 1)`
SQRT(num)	Displays the square root of a value.	`SQRT([PrincipalValue])`
STDEV(expr)	Displays the standard deviation.	`STDEV([PurchaseFrequency])`
SUM(expr)	Displays the sum of two specified values.	`SUM([Price]+[Tax])`
TODAY( )	Displays a time stamp value equal to midnight of the current date.	`TODAY([DueDate])`
TRIM(str)	Displays a string with all leading and trailing blank characters removed. Also removes all consecutive blank characters. Leading and trailing blanks can be spaces, tabs, and so on.	`TRIM([customerName])`
TRIMLEFT(str)	Displays a string with all leading blanks removed. Does not remove consecutive blank characters.	`TRIMLEFT([PortfolioName])`

Table 13-11 Examples of Functions (continued)

Function	Description	Example of use
TRIMRIGHT(str)	Displays a string with all trailing blanks removed. Does not remove consecutive blank characters.	`TRIMRIGHT([Comments])`
true	The Boolean true. This function is used in expressions to indicate that an argument is true.	In the following example, true indicates that the second argument, ascending, is true and therefore the values should be returned in ascending order. `RANK([Score], true)`
UPPER(str)	Displays a string in a specified column in all uppercase.	`UPPER([cityName])` `UPPER("new haven")`
VAR(expr)	Displays a variance for the specified expression.	`VAR([EstimatedCost])`
WEEK(date)	Displays the number of the week, from 1 through 52, for a date-and-time value.	`WEEK([LeadQualifyingDate])`
WEEKDAY(date, option)	Displays the day of the week in one of the following format options: • 1 - Returns the day number, from 1 (Sunday) through 7 (Saturday). 1 is the default option. • 2 - Returns the day number, from 1 (Monday) through 7 (Sunday). • 3 - Returns the day number, from 0 (Monday) through 6 (Sunday). • 4 - Returns the weekday name according to the user's locale. • 5 - Returns the abbreviated weekday name according to the user's locale.	`WEEKDAY([DateSold], 4)`
WEIGHTEDAVERAGE (value, weight)	Displays a weighted average of a specified value.	`WEIGHTEDAVERAGE([Score], weight)`
YEAR(date)	Displays the four-digit year value for a date-and-time value.	`YEAR([ClosingDate])`

Understanding Supported Operators

Table 13-12 describes the mathematical and logical operators you can use in writing expressions that create calculated columns.

Table 13-12 Supported Operators to Use in Writing Expressions

Operator	Description
x + y	Addition of numeric values
x - y	Subtraction of numeric values
x * y	Multiplication of numeric values
x / y	Division of numeric values

Table 13-12 Supported Operators to Use in Writing Expressions (continued)

Operator	Description
x%	Percentage of a numeric value
x & y	Concatenation of string values
x = y	Test for equality of two values
x > y	Tests whether x is greater than y
x < y	Tests whether x is less than y
x >= y	Tests whether x is greater than or equal to y
x <= y	Tests whether x is less than or equal to y
x <> y	Tests whether x is not equal to y
x AND y	Tests for values that meet both condition x and condition y
x OR y	Tests for values that meet either condition x or condition y
NOT x	Tests for values that are not x

Using Numbers and Dates in an Expression

When you create an expression that contains a number, you must type the number according to the conventions of the US English locale. In other words, use a period (.), not a comma (,), as the decimal separator. For example:

```
Correct:       1234.56
Incorrect:     1234,56
```

When you create an expression that contains a date, type the date according to the conventions of the locale you chose when you logged in. For example, in the French (France) locale type 03/12/2007 to represent December 3, 2007, not 12/03/2007. You can enter a date or a date and time. Dates and times must be enclosed in double quotes ("), for example:

```
"03/12/2007"
"03/12/2007 11:00 AM"
```

ns.

Using Multiply Values in Calculated Columns

Step 1 Select a column. In the report, the new calculated column appears to the *right* of the column you select.

Step 2 Select **Add Calculation**. The Calculation dialog box appears.

Step 3 In the Column Label field, type a header for the calculated column. The header must start with a letter and can contain only letters, numbers, underscores, and spaces.

Step 4 In the Enter Expression field, type a left square bracket ([ ). A list of the columns in the report appears. This list includes any calculated columns the report contains.

Select the column that contains the multiplier. For example, to multiply a unit price times the quantity ordered, select the column that contains unit prices.

Step 5 Enter an asterisk (*) as the multiplication operator. You do not need to include a space after the column name.

Step 6 Enter another left square bracket ([ ) and select the multiplicand. For example, if the multiplier is the unit price, select the column that contains the quantity ordered as the multiplicand.

Step 7 To verify the expression, click **Validate**. If the expression syntax is correct, the dialog box displays a validation message. If the expression syntax is incorrect, the dialog box displays a message explaining the error.

Step 8 After validating the expression, click **Apply**. The calculated column appears in the report, by using the column header you typed.

Adding Days to an Existing Date Value

You can create a column that displays date values that are greater than the date values in another column.

Step 1 Select a column. The calculated column appears to the *right* of the column you select.

Step 2 Select **Add Calculation**. The Calculation dialog box appears.

Step 3 In Column Label, type a name for the calculated column. For example, type Forecast Shipping Date.

Step 4 In Enter Expression, type the letter A. A drop-down list appears, displaying functions that begin with A.

Step 5 Select ADD_DAY(date, daysToAdd).

Step 6 For the first argument, type a left opening bracket ([ ) and select the date column from the drop-down list. For example, select Order Date.

Step 7 For the second argument, type the number of days to add. In this case, type 7.

Step 8 Validate the expression, then click **Apply**.

The new calculated column appears in the report. For every value in the Order Date column, the calculated column displays a date seven days later than the order date.

Subtracting Date Values in a Calculated Column

You can display the difference between two date values.

Step 1 Select a column. In the report, the calculated column will appear to the right of the column you select. Select Add Calculation. The Calculation dialog box appears.

Step 2 In Column Label, type a name for the calculated column. For example, to subtract the actual shipping date from the date requested, type Shipping Delay.

Step 3 In Enter Expression, type the letter d. A drop-down list appears, displaying functions that begin with d.

Step 4 Select DIFF_DAY(date1, date2).

Step 5 For the first argument, type a left opening bracket ([ ) and select the first date column from the drop-down list. For example, select Date Requested.

Step 6 For the second argument, type a left opening bracket ([ ) and select the second date column from the drop-down list. For example, select Actual Shipping Date.

Step 7 Validate the expression, then click **Apply**. The new calculated column appears in the report, displaying the difference between the two dates.

Working with Aggregate Data

Aggregating data involves performing a calculation over a set of data rows. For example, in a report that has a column to calculate price*quantity, you can take the sum of all those calculations to obtain the total price of all items. You can create up to three aggregations for a calculated column.

When you aggregate data, you choose whether the aggregation appears in the table header or footer. If the column is a detail column in a data group, you can display the aggregate value in the group header or footer. Figure 13-39 shows aggregate data in a group footer.

Figure 13-39 Aggregate Row for a Group

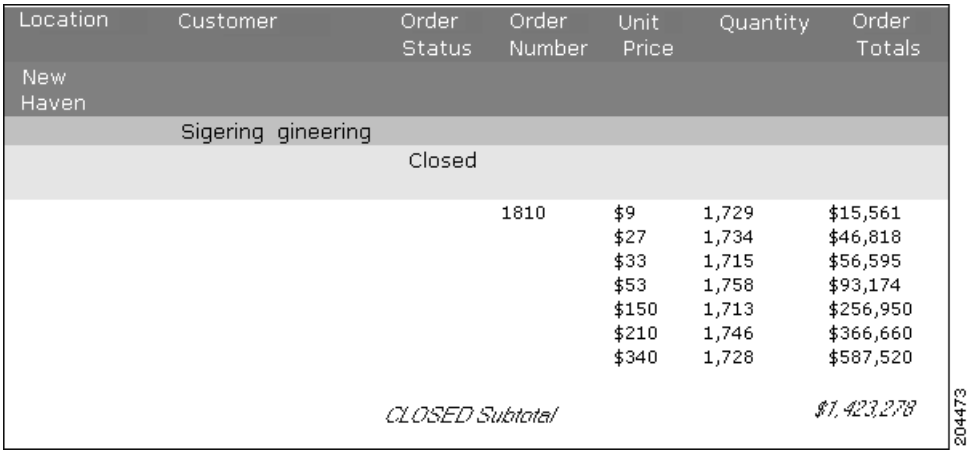


Table 13-13 shows the aggregate functions that you can use.

Table 13-13 Aggregate Functions

Aggregate functions	Description
Average	Calculates the average value of a set of data values.
Count	Counts the data rows in the column.
Count Value	Counts distinct values in the column.
First	Returns the first value in the column.
Last	Returns the last value in the column.
Max	Returns the highest value in the column.
Median	Returns the median value in the column.
Min	Returns the lowest value in the column.
Mode	Returns the most frequently-occurring value in the column.
Quartile	Returns one of four equal-sized sets of data, based on the rank you select. For example, you can request the first quartile to get the top quarter of the data set or the fourth quartile to get the fourth quarter of the data set.
Standard Deviation	Returns the standard deviation, the square root of the variance.
Sum	Adds the values in the column.

Table 13-13 Aggregate Functions (continued)

Aggregate functions	Description
Variance	Returns a value that indicates the spread around a mean or expected value.
Weighted average	Returns the weighted average of a numeric field over a set of data rows. In a weighted average, some numbers carry more importance, or weight, than others.

Creating an Aggregate Data Row

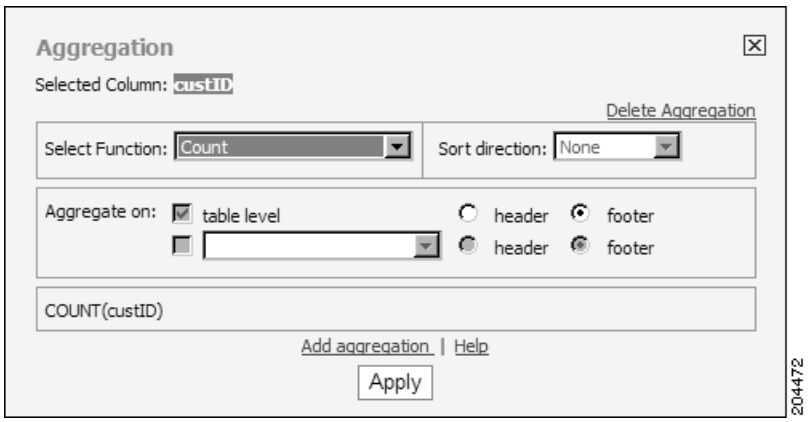
Step 1 Select a column, then select **Aggregation**. The Aggregation dialog box appears. The name of the column you selected is listed in the Selected Column field.

Step 2 From the Select Function menu, select the function you want to use. The available functions depend on the type of data the column contains:

- If the column contains text data, you can count all the values in the column or count the distinct values in the column, for example.
- If the column contains numeric data, you can count values, get an average value or a weighted average, total the values in the column, and so on.

The syntax of the selected function appears in the lower portion of the Aggregation dialog box, as shown in Figure 13-40.

Figure 13-40 The Aggregation Dialog Box in Interactive Viewer



Step 3 In the Aggregate on field:

- Select whether to display the aggregate value in the table header or the table footer. The default setting is to display the aggregate value in the table footer.
- Select whether to display the aggregate value in the group header or group footer, if the selected column is a *grouped* column.

Step 4 Click **Apply**. The aggregate data appears where you placed it in the report design.

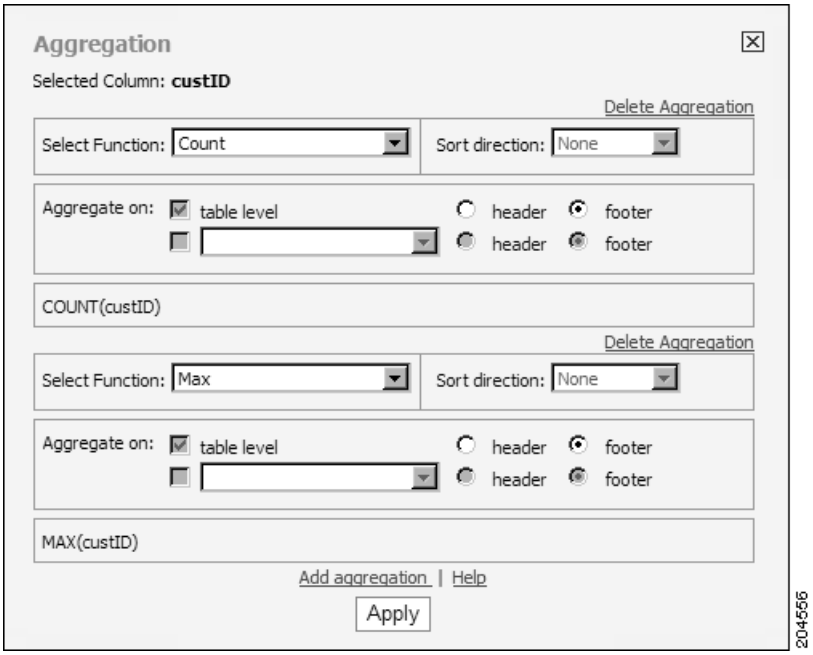
Adding Additional Aggregate Rows

After you create a single aggregate row for a column, you can add up to two more aggregate rows for the same column. For an item total column, for example, you can create a sum of all the values, count all the values, and get the average order total.

Step 1 To add an aggregate row, select a calculated column that contains an aggregate row, then select **Aggregation**. The Aggregation window appears.

Step 2 Click Add aggregation. An additional section appears in the Aggregation dialog box, as shown in Figure 13-41.

Figure 13-41 Adding an Aggregate Row for a Column in Interactive Viewer



Step 3 Create the second aggregate row, then click **Apply**.

Deleting Aggregate Rows

Step 1 Select the calculated column that contains the aggregation you want to remove, then select **Aggregation**.

Step 2 The Aggregation dialog box appears, displaying all the aggregations for the column.

Step 3 For the aggregation you want to remove, choose **Delete Aggregation**, then click **Apply**.

Hiding and Filtering Report Data

You can decide whether to hide or display data in your report in several ways:

- You can specify whether to hide or display detail rows.
- You can specify that you want to display only one copy of duplicate rows.
- When the data set provides more information than your report needs, you can filter out unwanted data. You also can enable your users to specify the filter values by using run-time parameters.

Hiding or Displaying Column Data

Frequently, you do not want to display all the data in a report. For example, a column of detail can display duplicate values in consecutive data rows. When the duplication is unnecessary or makes the report difficult to read, you can suppress consecutive duplicate values. In addition, as you design a report, you can collapse groups or sections to display only the column headings and summary data, such as aggregate data rows.

Suppressing Repeated Values

Before you begin formatting and adjusting the data in your report, data rows appear in the report exactly as they appear in the data source. In the report shown in Figure 13-42, for example, the Location column shows the city name each time the name occurs.

Figure 13-42 Duplicate Values in Columns

Customer	Location	State	Representative
Tchl Systems Inc.	Boston	MA	1401
D in Systems	Boston	MA	1401
Brittn Design Inc.	Boston	MA	1401
Teleoards Co.	Boston	MA	1401
Desin Engineering Corp.	Boston	MA	1401
Tek ards Corp.	Philadelphia	PA	1216
D in Solutions	Philadelphia	PA	1216
Signl MicroSystems	Philadelphia	PA	1216
Sign ialists Corp.	NYC	NY	1286
Tchl MicroSystems Inc.	NYC	NY	1286
Infohgineering	NYC	NY	1286
Advc Design Inc.	NYC	NY	1286
Tchl Design Inc.	NYC	NY	1286
Desi Sol Corp.	NYC	NY	1286

204497

As Figure 13-43 shows, the report is easier to read when duplicate values are not repeated.

Figure 13-43 Suppressed Values

Customer	Location	State	Representative
Tchl Systems Inc.	Boston	MA	1401
D in Systems			
Brittn Design Inc.			
Teleoards Co.			
Desin Engineering Corp.			
Tek ards Corp.	Philadelphia	PA	1216
D in Solutions			
Signl MicroSystems			
Sign ialists Corp.	NYC	NY	1286
Tchl MicroSystems Inc.			
Infohgineering			
Advc Design Inc.			
Tchl Design Inc.			

204549

You can suppress duplicate values to make your report easier to read. You can suppress only consecutive occurrences of duplicate values. In the Location column in Figure 13-43, the Boston value is suppressed in the second, third, fourth, and fifth rows. If Boston occurs again after the listing for NYC, that occurrence of Boston is visible and subsequent consecutive occurrences are suppressed. The values must be exact duplicates to be suppressed.

If a column splits across multiple pages, the first row on each page displays a value, even if duplicate values are suppressed for that column.

Step 1 Select and right-click the column that contains duplicate values.

Step 2 From the context menu, select **Column > Do Not Repeat Values**.

Displaying Repeated Values

Select and right-click the column that does not repeat duplicate values.

From the context menu, select **Column > Repeat Values**.

Hiding or Displaying Detail Rows in Groups or Sections

If a report contains groups, you can collapse and expand a group by using the context menu.

For example, Figure 13-44 shows a report where the data is grouped by *creditrank* and the detail rows for each creditrank value are shown.

Figure 13-44 Group Detail Rows Displayed

creditrank	custID	contact_last	contact_first
⊟ A			
	102	Murphy	Leslie
	106	Young	Jeff
	109	Frick	Michael
	111	Hernandez	Maria
	113	Yu	Kwai
	115	Thompson	Bill
	116	Brown	William
	117	Lewis	Bill
	120	Thompson	Steve
	122	Firrelli	Dan

204493

Figure 13-45 shows the results of hiding the detail rows for the creditrank grouping.

Figure 13-45 Group Detail Rows Hidden

creditrank	custID	contact_last	contact_first
A			
B			
C			

204492

Step 1 To collapse a group or section, select and right-click a member of the group or section that you want to collapse. The context menu appears.

Step 2 To display the group members without their detail rows, select **Group > Hide Detail**.

Step 3 To display the group members with their detail rows, select **Group > Show Detail**.

Working with Filters

Filters limit the data that appears in reports. For example, by using a database of customer data, you can use filters to run a report that lists only the customers in a specific state or province, or only the customers whose purchases total more than $1.5 million. To limit the data even more, you can, for example, list customers in a specific state who have credit limits of less than $50,000 and who have not made a purchase in the past 90 days.

A filter is based on one or more fields in a report.

To create a filter based on a single field, you select a condition and a value. For example, you can create a filter that returns values that are equal to a specified value, less than a specified value, between two values, and so on. Table 13-14 describes the conditions you can select.

Table 13-14 Conditions to Use with Filters

Condition	Description
Any Of	Returns any of the values you specify.
Between	Returns values that are between two specified values. When you select Between, a second Value field appears for the second default value.
Bottom N	Returns the lowest *n* values in the column.
Bottom Percent	Returns the lowest *n* percent of values in the column.
Equal to	Returns values that are equal to a specified value.
Greater Than	Returns values that are greater than a specified value.
Greater Than or Equal to	Returns values that are greater than or equal to a specified value.
Is False	In a column that evaluates to true or false, returns data rows that contain false values.
Is Not Null	Returns data rows that contain values.
Is Null	Returns data rows that do not contain values.
Is True	In a column that evaluates to true or false, returns data rows that contain true values.
Less Than	Returns values that are less than another value.
Less Than or Equal to	Returns values that are less than or equal to another value.
Like	Returns strings that match all or part of the specified string. % matches zero or more characters. _ matches one character.
Not Between	Returns values that are not between two specified values. When you select Not Between, a second Value field appears for the second default value.
Not Equal to	Returns values that are not equal to another value.
Not Like	Returns strings that do not match all or part of the specified string. % matches zero or more characters. _ matches one character.
Top N	Returns the top *n* values in the column.
Top Percent	Returns the top *n* percent of values in the column.

Types of Filter Conditions

Table 13-15 describes the types of filter conditions and provides examples of how filter conditions are translated into instructions to the data source.

Table 13-15 Examples of Filter Conditions

Type of filter condition	Description	Examples of instructions to data source

Comparison	Compares the value of one expression to the value of another expression using:
	• Equal to
	• Not Equal to
	• Less Than
	• Less Than or Equal to
	• Greater Than
	• Greater Than or Equal to
		`quantity = 10`
		`custName = 'Acme Inc.'`
		`custName > 'P'`
		`custState <> 'CA'`
		`orderDate > {d '2005-06-30'}`

Range	Tests whether the value of an expression falls or does not fall within a range of values using Between or Not Between. The test includes the endpoints of the range.	`price BETWEEN 1000 AND 2000`
		`custName BETWEEN 'E' AND 'K'`
		`orderDate BETWEEN`
		`{d '2005-01-01'} AND {d '2005-06-30'}`

Membership	Tests whether the value of an expression matches one value in a set of values using Any Of.	`officeCode IN (101,103,104)`
		`itemType IN ('sofa', 'loveseat', 'endtable', 'clubchair')`
		`orderDate IN`
		`({d '2005-10-10'}, {d '2005-10-17'})`

Pattern-matching	Tests whether the value of a string field matches or does not match a specified pattern using Like or Not Like. % matches zero or more characters. _ matches one character.	`custName LIKE 'Smith%'`
		`custName LIKE 'Smiths_n'`
		`custState NOT LIKE 'CA%'`

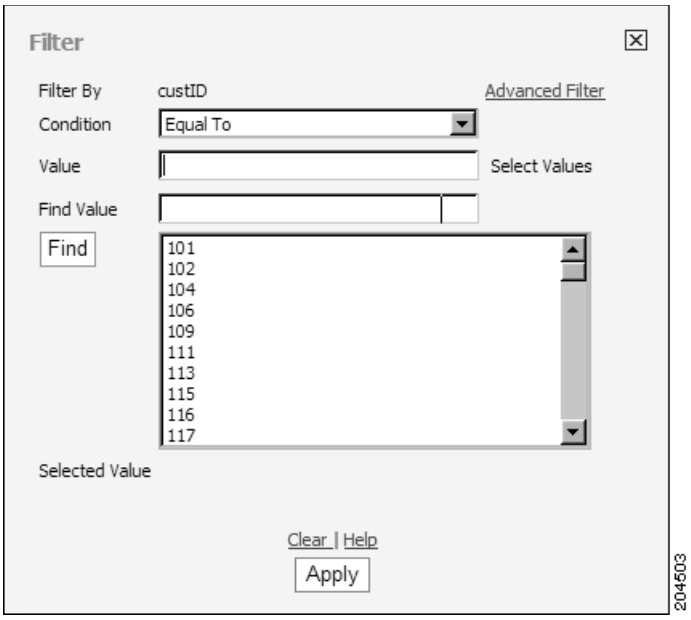
Null value	Tests whether a field has or does not have a null, or missing, value using Is Null or Is Not Null.	`manager IS NULL`
		`shipDate IS NULL`
		`shipDate IS NOT NULL`

Setting Filter Values

After you choose a condition, you set a filter value.

Step 1 To view all the values for the selected column, select **Select Values**. Additional fields appear in the Filter dialog box as shown in Figure 13-46. These fields allow you to find and select a filter value.

Figure 13-46 Selecting a Filter Value in Interactive Viewer



Step 2 To search for a value, type the value in the Find Value field, then click **Find**. All values that match your filter text are returned. For example, if you type:

```
40
```

the text box displays any values in the column that begin with 40, such as:

```
40
400
4014
40021
```

When you see the value you want in the large text box, double-click the value. The value appears in the Value field.

Creating Filters

Step 1 In Interactive Viewer, select a detail column and choose **Filter**.

If the detail column you selected is a merged column, the Select data item dialog box appears.

Step 2 From the Select date drop-down list, select the column name for which you want to apply a filter, then click **Apply**. The Filter dialog box appears. The name of the column you selected appears in the Filter By field. You cannot change the name.

Step 3 From the Condition pulldown menu, select a condition. Table 13-14 describes the conditions you can select.

If you select **Between** or **Not Between**, **Value From** and **Value To**, additional fields appear to display a range of values.

If you select **Is False**, **Is True**, **Is Null**, or **Is Not Null**, no value fields appear. For all other selections, a single value field appears.

Step 4 Enter values in each of the available fields. To view all possible values for the column, click **Select Values** and select from the drop-down list.

Step 5 Click **Apply**. The results of applying the filter are displayed.

Modifying or Clearing a Filter

Step 1 Select the column that uses the filter.

Step 2 Select **Filter**. The Filter dialog box opens, displaying the existing filter condition

Step 3 To modify the filter, change the setting in the Condition field or change the values.

Step 4 To remove the filter, click **Clear**.

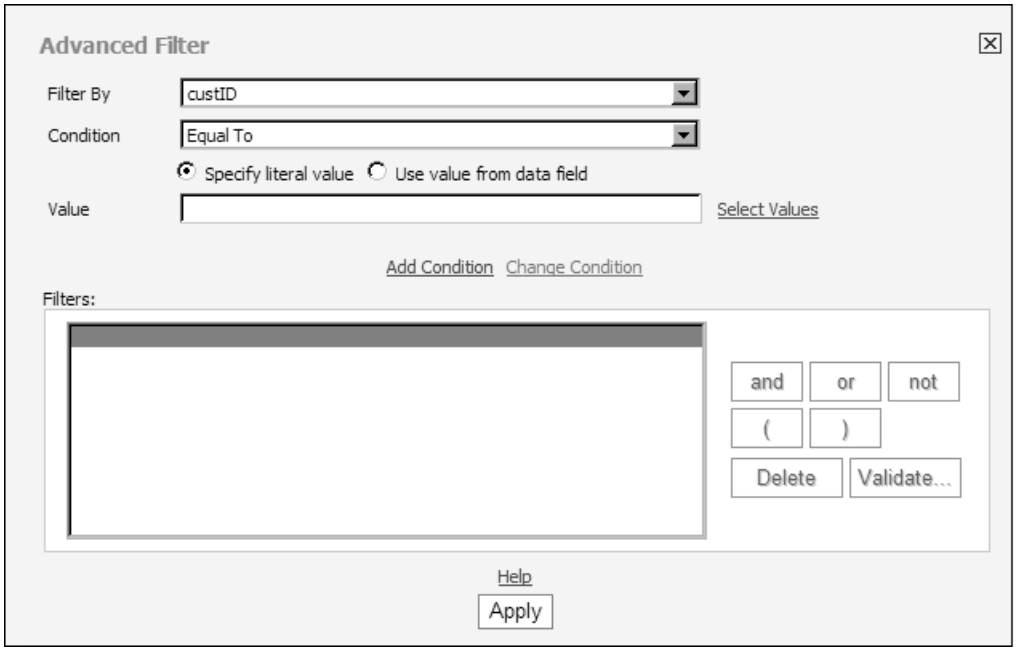
Step 5 Click **Apply**.

Creating a Filter with Multiple Conditions

You can create a filter with more than one condition. For example, you can create a filter that retrieves the names of customers who have a credit rank of either A or B, and who have open orders totaling between $250,000 and $500,000.

To create a filter with multiple conditions, you choose Advanced Filter on the Filter dialog to use the Advanced Filter dialog box. The Advanced Filter dialog box for Interactive Viewer is shown in Figure 13-47.

Figure 13-47 The Advanced Filter Dialog Box in Interactive Viewer



Advanced Filter provides a great deal of flexibility in setting the filter value. For conditions that test equality and for the Between condition, you can either set a literal value or you can base the value on another data column. For example, you can request actual shipping dates that are greater than the forecast shipping dates, or actual sales that are less than sales targets.

Step 1 Select a column, then select **Filter**. The Filter dialog box appears.

Step 2 Click **Advanced Filter**. The Advanced Filter dialog box appears. The Filter By field displays the name of the first column in the report.

Step 3 From the Filter By menu, select the column that contains the data you want to filter.

Step 4 In the Condition field, select a condition, such as Equal To, Between, or Less Than.

Step 5 In Value, select one of the following options:

- **Specify literal value**—This is the default selection. To specify a literal value, type a value in the field provided. If you click **Select Values**, a field appears displaying all data values for the specified column. For long lists, you can find a value by typing the value in the Filter Text field and clicking **Find**.
- **Use value from data field**—When you select Use value from data field, a drop-down list of columns appears. The columns in this list have the same data type as the column you selected in the Filter By field.

Step 6 Click **Add Condition**. The filter condition appears in Filters.

Step 7 Validate the filter syntax by clicking **Validate**.

You have now created a filter with one condition. The next step is to add conditions.

Step 8 Follow steps Step 3 to Step 7 to create each additional desired filter condition.

Step 9 In Filters, adjust the filter conditions to achieve the desired filtering. You can combine the conditions in the following ways:

- Using AND, OR, and NOT

  By default, the second filter condition is preceded by AND. AND means that both conditions must be true for a data row to appear in the report. You can change AND to OR by choosing OR. OR means that only one condition has to be true for a data row to appear in the report. If you choose NOT, NOT appears after the AND or OR. NOT means that the condition must be false for a data row to appear in the report.

- If you add more than one condition, you can use the parentheses buttons to group conditions.

  If you enclose two or more filter conditions in parentheses, the conditions in the parentheses are evaluated first. Then, the entire filter expression is evaluated. For example, A AND B OR C is evaluated from left to right, so A and B must be true or C must be true for a data row to appear in the report. In A AND (B OR C), B OR C is evaluated first, so A must be true and B or C must be true for a data row to appear in the report.

Deleting One Filter Condition in a Filter that Contains Multiple Conditions

Step 1 Select a detail column, then select **Filter**. The Filter dialog box appears.

Step 2 Click **Advanced Filter**. The Advanced Filter dialog box appears.

The lower portion of Advanced Filter displays all the filter conditions in the report.

Step 3 Select a filter condition to delete, then click **Delete**.

Step 4 Click **Apply**.

Filtering Highest or Lowest Values in Columns

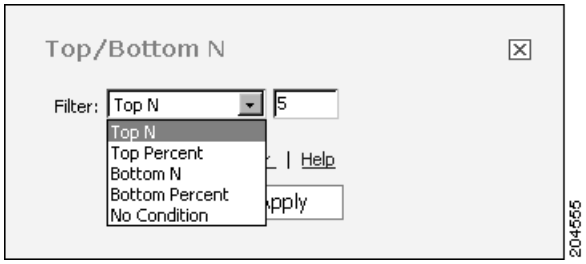
When a table contains hundreds of rows, it can be helpful to display the highest or lowest values in a column. For example, you might want to view the ten sales representatives who produce the most revenue or the top twenty-five percent of energy consumers.

Step 1 To perform this type of filter, right-click a selected column, then select **Filter > Top or Bottom N**. The Top or Bottom N dialog box appears.

Step 2 From the Filter pulldown menu, select a particular number of rows or a percentage of rows, as shown in Figure 13-48.

Step 3 Enter a value in the field next to the Filter pulldown menu to specify the number or percentage of rows to display. For example, to select the top 10 sales representatives by sales volume, after you have selected the column that contains sales volume data and chosen **Filter > Top or Bottom N**, in the Top or Bottom N dialog box, select **Top N** and enter ***10***.

Figure 13-48 Sorting Top or Bottom Values in a Column



Step 4 Click **Apply**.

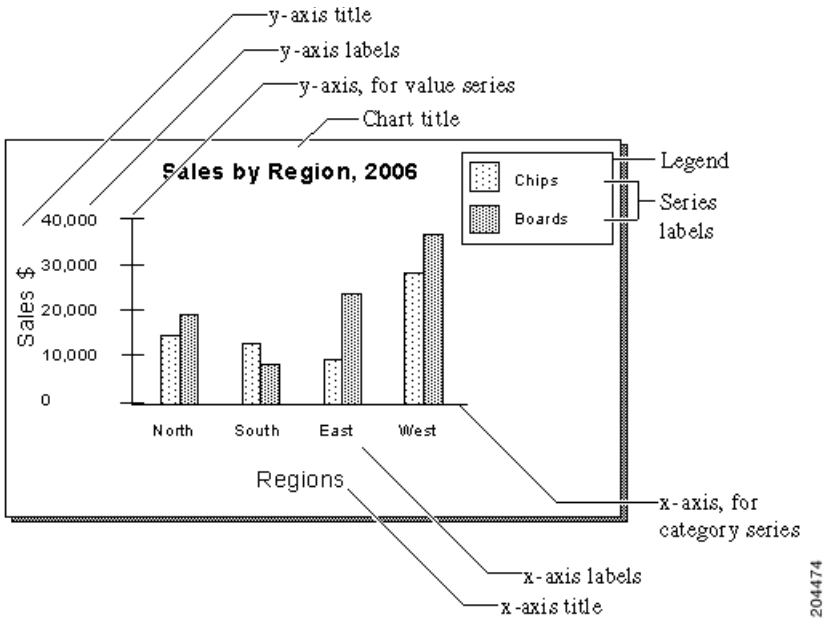
Understanding Charts

A **chart** is a graphical representation of data or the relationships among data sets. Charts display complex data in an easy-to-assimilate format. Figure 13-49 shows the parts of a basic bar chart. A chart displays data as one or more sets of points. The chart organizes data points into sets of values called series. The two types of series are:

- Category series— The category series typically determines what text, numbers, or dates you see on the x-axis.
- Value series—The value series typically determines the text, numbers, or dates on the y-axis.

In Figure 13-49, the category series contains a set of regions, and the value series contains a set of sales figure values.

Figure 13-49 Parts of a Basic Bar Chart



There are a variety of chart types. Some types of data are best depicted with a specific type of chart. Charts can be used as reports in themselves and they can be used together with tabular data report styles.

Modifying Charts

The basic characteristics of a chart are determined in the report design editor. Such things as the chart type and the data source are part of the report design and cannot be changed in the viewer. You can change the following aspects of the chart:

The Interactive Viewer presents the capability to:

- Filter the data presented in the chart
- Change the chart subtype
- Change the chart format

Select these options from a context menu by right-clicking on the chart in Interactive Viewer.

Filtering Chart Data

The data displayed in the chart can be filtered in much the same way that any data column is filtered. With a chart you can filter either the x-axis or the y-axis.

Step 1 Right-click on the chart to display the context menu.

Step 2 Select **Filter**. The Chart Filter dialog box appears.

Changing Chart Subtype

charts have subtypes, which you can change as needed:

- Bar chart—Side-by-Side, Stacked, Percent Stacked
- Line chart—Overlay, Stacked, Percent Stacked
- Area chart—Overlay, Stacked, Percent Stacked
- Meter chart—Standard, Superimposed
- Stock chart—Candlestick, Bar Stick

Many chart types offer two-dimensional subtypes, in which the chart shape appears flat against the chart background. Some charts also can be displayed with depth. A chart with depth appears to have added dimension.

Step 1 Right-clicking the chart whose subtype you want to modify.

Step 2 Select **Chart Subtype**. The Chart Subtype dialog box appears.

Step 3 Select the desired chart subtype.

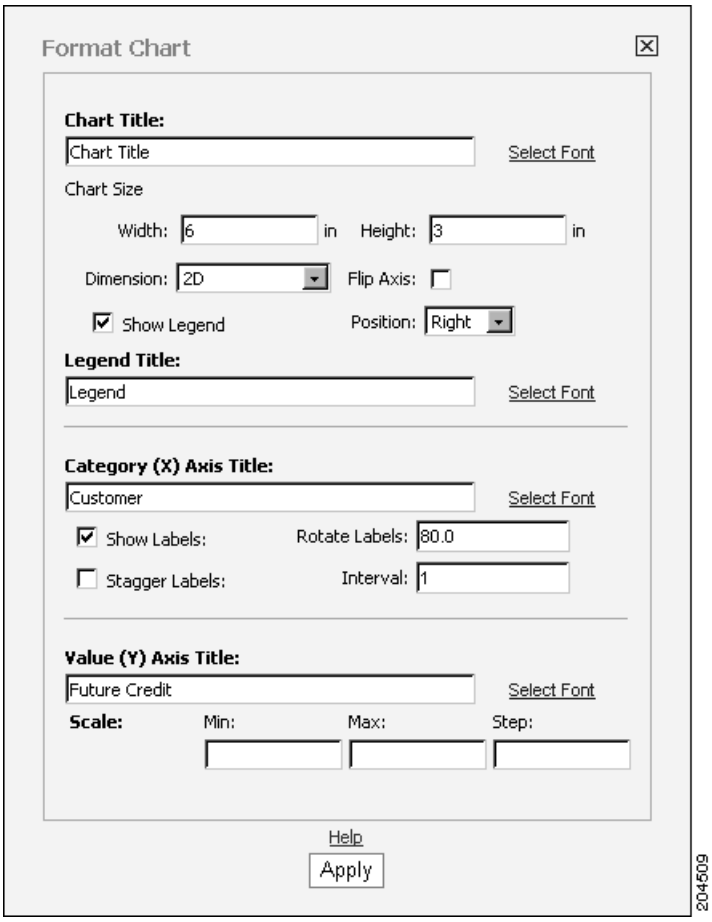
Changing Chart Formatting

Some of the formatting for a chart, such as the colors of the bars in a bar chart and the background color of the chart, comes from the report template or the theme. When viewing the report you can modify other items of the chart's format, including the fonts and font sizes of the chart title and axis labels, and the height and width of the chart. You can hide axis labels, place labels at an angle relative to the axis, and hide the legend or determine where to display the legend in relation to the chart.

You can modify other aspects of the chart's appearance by right-clicking the chart and choosing Format. In the dialog box that appears, choose the desired formatting properties.

To modify other aspects of the chart's appearance, use Format Chart, shown in Figure 13-50.

Figure 13-50 Chart Formatting Options



You use this page to:

- Edit and format the default chart title.
- Edit and format the default title for the category, or x-, axis.
- Modify settings for the labels on the x-axis. You can:
  - Indicate whether to display x-axis labels.
  - Indicate whether to rotate x-axis labels and set the degree of rotation.
  - Indicate whether to stagger x-axis labels. For example, you can show data points for every third month, every ten days, every other year, and so on.
  - Set the interval for staggered x-axis labels.
- Edit and format the default title for the y-axis, if the chart uses a y-axis.
- Set the chart's height and width.
- Select the dimension. The options are 2-dimensional and 2-dimensional with depth.
- Indicate whether to flip, or reverse, the chart's x- and y-axes.
- Indicate whether to show a legend, and if so, whether to place it above the chart, below the chart, or to the left or right of the chart.

CHAPTER 14

Troubleshooting ACS with the Monitoring & Report Viewer

This chapter describes the diagnostic and troubleshooting tools that the Monitoring & Report Viewer provides for the Cisco Secure Access Control System.

This chapter contains the following sections:

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Performing Connectivity Tests, page 14-3
- Downloading ACS Support Bundles for Diagnostic Information, page 14-4
- Working with Expert Troubleshooter, page 14-5

Available Diagnostic and Troubleshooting Tools

The Monitoring & Report Viewer provides the following:

- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Connectivity Tests

When you have authentication problems, you can perform a connectivity test to check for connectivity issues. You can enter the hostname or the IP address of the network device that you are trying to connect with and execute the following commands from the web interface: **ping**, **traceroute**, and **nslookup**. The Monitoring & Report Viewer displays the output of these commands. See Performing Connectivity Tests, page 14-3 for detailed instructions on how to perform the connectivity tests.

ACS Support Bundle

You can use the ACS support bundle to prepare diagnostic information for TAC to troubleshoot problems with ACS.

Support bundles typically contain the ACS database, log files, core files, and Monitoring & Report Viewer support files. You can exclude certain files from the support bundle, per ACS node. You can download the support bundle to your local computer. The browser (depending on its configuration) displays the progress of the download and prompts you to save the support bundle to an appropriate location.

If the ACS server is a primary instance, the support bundle includes an export of the ACS configuration. If the ACS server is a secondary instance, the ACS database is not included. If the ACS server is a log collector, the support bundle includes an export of the monitoring and report configuration and collected AAA audit and diagnostic logs. If the ACS server is not the log collector, the monitoring and reporting configuration is not included in the support bundle. See Downloading ACS Support Bundles for Diagnostic Information, page 14-4 for detailed instructions on how to download ACS support bundles.

Expert Troubleshooter

Expert Troubleshooter is an easy-to-use, web-based troubleshooting utility that helps you diagnose and troubleshoot problems in ACS deployments. It reduces the time that you take to diagnose the problem and provides you detailed instructions on how to resolve the problem.

You can use Expert Troubleshooter to diagnose and troubleshoot passed and failed authentications. For example, if a user is unable to gain access to the network, you can use the Expert Troubleshooter to diagnose the cause of this problem.

Expert Troubleshooter provides you the option to run **show** commands on any network device from the ACS web interface. The output of the **show** command is returned to you in precisely the same manner as the output appears on a console.

You can use Expert Troubleshooter to evaluate the configuration of any network device to see if there are any discrepancies that cause the problem.

In addition, Expert Troubleshooter provides you four diagnostic tools for troubleshooting TrustSec device-related problems.

The Expert Troubleshooter identifies the cause of the problem and lists an appropriate course of action that you can take to resolve the problem. See Working with Expert Troubleshooter, page 14-5 for more information on the various tools that Expert Troubleshooter offers.

Table 14-1 describes the diagnostic tools that ACS 5.1 offers:

Table 14-1 Expert Troubleshooter - Diagnostic Tools

Diagnostic Tool	Description
RADIUS Authentication Troubleshooting	Troubleshoots a RADIUS authentication. See Troubleshooting RADIUS Authentications, page 14-6 for more information.
Execute Network Device Command	Executes any **show** command on a network device. See Executing the Show Command on a Network Device, page 14-9 for more information.
Evaluate Configuration Validator	Evaluates the configuration of a network device. See Evaluating the Configuration of a Network Device, page 14-10 for more information.
Trust Sec Tools	
Egress (SGACL) Policy	Compares the Egress Policy (SGACL) between a network device and ACS. See Comparing SGACL Policy Between a Network Device and ACS, page 14-11 for more information.

Table 14-1 Expert Troubleshooter - Diagnostic Tools (continued)

Diagnostic Tool	Description
SXP-IP Mappings	Compares SXP mappings between a device and peers. See Comparing the SXP-IP Mappings Between a Device and its Peers, page 14-12 for more information.
IP User SGT	Compares IP-SGTs on a device with ACS authentication-assigned User-IP-SGT records. See Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records, page 14-14 for more information.
Device SGT	Compares device SGT with ACS-assigned SGT. See Comparing Device SGT with ACS-Assigned Device SGT, page 14-15 for more information.

Performing Connectivity Tests

You can test your connectivity to a network device with the device's hostname or IP address. For example, you can verify your connection to an identity store by performing a connectivity test.

To test connectivity between your ACS and a device's hostname or IP address:

Step 1 Select **Monitoring and Reports > Troubleshooting > Connectivity Tests**.

The Connectivity Tests page appears as described in Table 14-2:

Table 14-2 Connectivity Tests

Option	Description
Hostname or IP Address	Enter the hostname or IP address of a connection you want to test. Click **Clear** to clear the hostname or IP address that you have entered.
ping	Click to see the **ping** command output, where you can view the packets sent and received, packet loss (if any) and the time for the test to complete.
traceroute	Click to see the **traceroute** command output, where you can view the intermediary IP addresses (hops) between your ACS and the tested hostname or IP address, and the time for each hop to complete.
nslookup	Click to see the **nslookup** command output, where you can see the server and IP address of your tested domain name server hostname or IP address.

Step 2 Modify the fields in the Connectivity Tests page as required.

Step 3 Click **ping**, **traceroute**, or **nslookup**, depending upon your test.

The output of the **ping**, **traceroute**, or **nslookup** command appears.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Downloading ACS Support Bundles for Diagnostic Information

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create and download an ACS support bundle:

Step 1 Select **Monitoring and Reports > Troubleshooting > ACS Support Bundle**.

The ACS Support Bundle page appears with the fields described in Table 14-3:

Table 14-3 ACS Support Bundle Page

Option	Description
Server	Name of an ACS node instance. Click to display the Download Parameters for the Server page, to create and download an ACS support bundle for the ACS node instance.
IP Address	*Display only.* Indicates the IP address of an associated ACS node.
Node Designation	*Display only.* Indicates the primary or secondary instance of an associated ACS node.

Step 2 Choose a server and click **Get Support Bundle** to display the Download Parameters for the Server page, to create and download an ACS support bundle for the associated ACS node instance.

Step 3 Select the download options you want to incorporate in your ACS support .tar.gz file.

Note Downloading a support bundle can be slow if the size of the file is extremely large. For faster downloads, do not include core files and View support files in the support bundle.

The options are:

- Include full configuration database—Check this box to have the whole database included in the support bundle. If this option in not checked, only a subset of the database is included in the support bundle. Click **Include sensitive information** or **Exclude sensitive information** to include or exclude sensitive information in the logs.

Note Sensitive information consists of passwords in the encrypted format, ACS configuration data, and so on.

- Include debug logs—Check this check box to include debug logs, then click **All**, or click **Recent** and enter a value from 1 to 999 in the file(s) field to specify which debug logs to include.
- Include local logs—Check this check box to include local logs, then click **All**, or click **Recent** and enter a value from 1 to 999 in the file(s) field to specify which debug logs to include.
- Include core files—Check this check box to include core files, then click **All** or click **Include files from the last** and enter a value from 1 to 365 in the day(s) field.

- Include monitoring and reporting logs—Check this check box to include monitoring and reporting logs, then click **All** or click **Include files from the last** and enter a value from 1 to 365 in the day(s) field.

  Specify which monitoring and reporting logs to include:

  - AAA Audit
  - AAA Diagnostics
  - System Diagnostics
  - AAA Accounting
  - Administrative and Operational Audit
- Include system logs—Check the check box to include system logs, then click **All** or **Recent** and enter a value from 1 to 999 in the file(s) field.

Step 4 (Optional) Enter a description in the Description field.

Step 5 Click:

- **Download** to download the support bundle with the options you specified. The support bundle is created and downloaded.
- **Restore Defaults** to clear the changes you made and return to the default settings.

Note ACS does not pick up the core files while creating or downloading the support bundle for the associated ACS node instance by default. If you want to include the core files in the support bundle, you can check the **Include core files** check box. You can check the **Encrypt Support Bundle** checkbox to encrypt the support bundle in ACS. It will ensure that the core files are encrypted and included in the supported bundle.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Working with Expert Troubleshooter

The following sections describe how to use the Expert Troubleshooter diagnostic tools:

- Troubleshooting RADIUS Authentications, page 14-6
- Executing the Show Command on a Network Device, page 14-9
- Evaluating the Configuration of a Network Device, page 14-10
- Comparing SGACL Policy Between a Network Device and ACS, page 14-11
- Comparing the SXP-IP Mappings Between a Device and its Peers, page 14-12
- Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records, page 14-14
- Comparing Device SGT with ACS-Assigned Device SGT, page 14-15

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Troubleshooting RADIUS Authentications

Use the RADIUS Authentication diagnostic tool to troubleshoot issues with RADIUS authentications. To do this, you must:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

The Expert Troubleshooter page appears.

Step 2 Select RADIUS Authentication Troubleshooting from the list of troubleshooting tools.

The RADIUS Authentication Troubleshooter page appears.

Step 3 Modify the fields as shown in Table 14-4 to filter the RADIUS authentications that you want to troubleshoot.

Table 14-4 RADIUS Authentication Troubleshooter Page

Option	Description
Search and select a RADIUS authentication for troubleshooting	
Username	Enter the username of the user whose authentication you want to troubleshoot, or click **Select** to choose the username from a list. Click **Clear** to clear the username.
MAC Address	Enter the MAC address of the device that you want to troubleshoot, or click **Select** to choose the MAC address from a list. Click **Clear** to clear the MAC address.
Audit Session ID	Enter the audit session ID that you want to troubleshoot. Click **Clear** to clear the audit session ID.
NAS IP	Enter the NAS IP address or click **Select** to choose the NAS IP address from a list. Click **Clear** to clear the NAS IP address.
NAS Port	Enter the NAS port number or click **Select** to choose a NAS port number from a list. Click **Clear** to clear the NAS port number.
Authentication Status	Choose the status of your RADIUS authentication from the Authentication Status drop-down list box. The available options are: • Pass or Fail • Pass • Fail
Failure Reason	Enter the failure reason or click **Select** to choose a failure reason from a list. Click **Clear** to clear the failure reason.

Table 14-4 RADIUS Authentication Troubleshooter Page (continued)

Option	Description
Time Range	Define a time range from the Time Range drop-down list box. The Monitoring & Report Viewer fetches the RADIUS authentication records that are created during this time range. The available options are: • Last hour • Last 12 hours • Today • Yesterday • Last 7 days • Last 30 days • Custom
Start Date-Time	(Only if you choose Custom Time Range) Enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
End Date-Time	(Only if you choose Custom Time Range) Enter the end date and time, or click the calendar icon to select the end date and time. The date should be in the *mm/dd/yyyy* format and time in the *hh:mm* format.
Fetch Number of Records	Choose the number of records that you want the Monitoring & Report Viewer to fetch at a time from the Fetch Number of Records drop-down list. The available options are 10, 20, 50, 100, 200, and 500.

Step 4 Click **Search** to display the RADIUS authentications that match your search criteria.

The Search Result table is populated with the results of your search. The following fields appear in the table: Time, Status, Username, MAC Address, Audit Session ID, Network Device IP, Failure Reason, and Access Service.

Step 5 Choose the RADIUS authentication record from this table that you want to troubleshoot, and click **Troubleshoot**.

The Expert Troubleshooter begins to troubleshoot your RADIUS authentication. The Monitoring & Report Viewer prompts you for additional input, if required. For example, if the Expert Troubleshooter must connect to a network device, it prompts you for connection parameters and login credentials.

Step 6 Click the **User Input Required** button and modify the fields as described in Table 14-5.

Step 7 Click **Submit**.

The Progress Details page appears. This page provides a summary and might prompt you for additional input, if required. If the Monitoring & Report Viewer requires additional input, you must click the **Click User Input Required** button. A dialog box appears.

Modify the fields in the dialog box as described in Table 14-5 and click **Submit**.

Table 14-5 Progress Details Page - User Input Dialog Box

Option	Description
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol from the Protocol drop-down list. Valid options are: • Telnet • SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an "Expect timeout error" or you know that the device has non-standard prompt strings) **Note** The Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

Step 8 Click **Done** to return to the Expert Troubleshooter.

The Progress Details page refreshes periodically to display the tasks that are performed as troubleshooting progresses. After the troubleshooting is complete, the Show Results Summary button appears.

Step 9 Click **Show Results Summary**.

The Results Summary page appears with the information described in Table 14-6.

Table 14-6 Results Summary Page

Option	Description
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
<*Summary*>	A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. **Note** Any configuration errors are indicated by red text.

Step 10 Click **Done** to return to the Expert Troubleshooter.

The Monitoring & Report Viewer provides you the diagnosis, steps to resolve the problem, and troubleshooting summary to help you resolve the problem.

Note You can launch the RADIUS authentication troubleshooter from the RADIUS authentication report pages as well. You must drill down to the details page of a particular RADIUS authentication to launch this diagnostic tool.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Executing the Show Command on a Network Device

The Execute Network Device Command diagnostic tool allows you to run any **show** command on a network device from the ACS web interface. The result of the **show** command is precisely what you would see on a console and can be used to identify problems in the device configuration. To run a **show** command on any network device:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Select Execute Network Device Command from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and lists the fields described in Table 14-7.

Table 14-7 Execute Show Command on a Network Device

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device on which you want to run the **show** command.
Command	Enter the **show** command that you want to run.

Step 3 Click **Run** to run the **show** command on the specified network device.

Step 4 The Progress Details page appears. The Monitoring & Report Viewer prompts you for additional input. Click the **User Input Required** button and modify the fields as described in Table 14-5.

Step 5 Click **Submit** to run the show command on the network device and view the output.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Evaluating the Configuration of a Network Device

You can use this diagnostic tool to evaluate the configuration of a network device and identify any missing or incorrect configuration. The Expert Troubleshooter compares the configuration on the device with the standard configuration. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Click Evaluate Configuration Validator from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and lists the fields described in Table 14-8.

Table 14-8 Evaluate Configuration Validator

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device whose configuration you want to evaluate.
Select the configuration items below that you want to compare against the recommended template.	
AAA	This option is checked by default.
RADIUS	This option is checked by default.
Device Discovery	This option is checked by default.
Logging	This option is checked by default.

Table 14-8 Evaluate Configuration Validator

Option	Description
Web Authentication	Check this check box if you want to compare the web authentication configuration.
Profiler Configuration	Check this check box if you want to compare the Profiler configuration.
CTS	Check this check box if you want to compare TrustSec configuration.
802.1X	Check this check box if you want to compare the 802.1X configuration, and choose one of the following options: • Open Mode • Low Impact Mode (Open Mode + ACL) • High Security Mode (Closed Mode)

Step 3 Click **Run**.

The Progress Details page appears. The Monitoring & Report Viewer prompts you for additional input.

Step 4 Click the **User Input Required** button and modify the fields as described in Table 14-5.

The Troubleshooting Progress Details page appears. The Expert Troubleshooter retrieves the CLI response from the network device. A new window appears and prompts you to select the interfaces for which you want to analyze the interface configuration.

Step 5 Check the check boxes next to the interfaces that you want to analyze, and click **Submit** to evaluate the configuration of the interfaces.

The Progress Details page appears with a summary.

Step 6 Click **Show Results Summary** to view the troubleshooting summary.

The Results Summary page appears with the information described in Table 14-6. The missing configurations appear in red.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Comparing SGACL Policy Between a Network Device and ACS

For TrustSec-enabled devices, ACS assigns an SGACL for every source SGT-destination SGT pair based on the Egress policy matrix that you configure in ACS. The Egress policy diagnostic tool does the following:

1. Connects to the device whose IP address you provide and obtains the ACLs for each source SGT— destination SGT pair.
2. Checks the Egress policy that is configured in ACS and obtains the ACLs for each source SGT— destination SGT pair.

3. Compares the SGACL policy obtained from the network device with the SGACL policy obtained from ACS.
4. Displays the source SGT —destination SGT pair if there is a mismatch. Also, displays the matching entries as additional information.

To compare the SGACL policy between a network device and ACS:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Select Egress (SGACL) Policy from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and shows the Network Device IP field.

Step 3 Enter the IP address of the TrustSec device whose SGACL policy you want to compare with ACS.

Step 4 Click **Run** to compare the SGACL policy between ACS and the network device.

The Progress Details page appears. The Monitoring & Report Viewer prompts you for additional input.

Step 5 Click the **User Input Required** button and modify the fields as described in Table 14-5.

Step 6 Click **Submit**.

The Progress Details page appears with a brief summary of the results.

Step 7 Click **Show Results Summary** to view the diagnosis and resolution steps. The Results Summary page appears with the information described in Table 14-6.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Comparing the SXP-IP Mappings Between a Device and its Peers

TrustSec devices communicate with their peers and learn their SGT values. The Security Exchange Protocol-IP (SXP)-IP Mappings diagnostic tool connects to the device whose IP address you provide and lists the peer devices' IP addresses and SGT values. You must select one or more of the device's peers. This tool connects to each of the peers that you select and obtains their SGT values to verify that these values are the same as the values that it learned earlier.

Use this diagnostic tool to compare the SXP-IP mappings between a device and its peers. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Select SXP-IP Mappings from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and shows the Network Device IP field.

Step 3 Enter the IP address of the network device.

Step 4 Click SXP-IP Mappings from the list of troubleshooting tools.

The Expert Troubleshooter page refreshes and shows the following field:

Network Device IP—Enter the IP address of the network device.

Step 5 Click **Run**.

The Progress Details page appears. The Monitoring & Report Viewer prompts you for additional input.

Step 6 Click the **User Input Required** button and modify the fields as described in Table 14-5.

The Troubleshooting Progress Details page appears. The Expert Troubleshooter retrieves CTS SXP connections from the network device and again prompts you to select the peer SXP devices.

Step 7 Click the **User Input Required** button.

A new window appears with the fields as described in Table 14-9.

Table 14-9 Peer SXP Devices

Option	Description
Peer SXP Devices	
Peer IP Address	IP address of the peer SXP device.
VRF	The VRF instance of the peer device.
Peer SXP Mode	The SXP mode of the peer device; for example, whether it is a speaker or a listener.
Self SXP Mode	The SXP mode of the network device; for example, whether it is a speaker or a listener.
Connection State	The status of the connection.
Common Connection Parameters	
User Common Connection Parameters	Check this check box to enable common connection parameters for all the peer SXP devices. **Note** If the common connection parameters are not specified or if they do not work for some reason, the Expert Troubleshooter again prompts you for connection parameters for that particular peer device.
Username	Enter the username of the peer SXP device.
Password	Enter the password to gain access to the peer device.
Protocol	• Choose the protocol from the Protocol drop-down list box. Valid options are: – Telnet – SSHv2 **Note** Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	• Enter the port number. The default port number for Telnet is 23 and SSH is 22.
Enable Password	Enter the enable password if it is different from your login password.
Same as login password	Check this check box if your enable password is the same as your login password.

Step 8 Check the check box of the peer SXP devices for which you want to compare the SXP mappings and enter the Common Connection Parameters as described in Table 14-9.

Step 9 Click **Submit**.

The Progress Details page appears with a brief summary of the results.

Step 10 Click **Show Results Summary** to view the diagnosis and resolution steps. The Results Summary page appears with the information described in Table 14-6.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records

For TrustSec-enabled devices, ACS assigns each user an SGT value through RADIUS authentication. The IP User SGT diagnostic tool connects to the network device whose IP address you provide and does the following:

1. Obtains a list of all IP-SGT assignments on the network device.
2. Checks the RADIUS authentication and accounting records for each IP-SGT pair to find out the IP-SGT-User value that ACS has assigned to it most recently.
3. Displays the IP-SGT pairs in a tabular format and identifies whether the SGT values most recently assigned by ACS and those on the device are the same or different.

Use this diagnostic tool to compare the IP-SGT values on a device with ACS-assigned SGT. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Click IP User SGT from the list of troubleshooting tools.

The Expert Troubleshooter page refreshes and lists the fields described in Table 14-10.

Table 14-10 IP User SGT

Option	Description
Enter Information	
Network Device IP	Enter the IP address of the network device.
Filter Results	
Username	Enter the username of the user whose records you want to troubleshoot.
User IP Address	Enter the IP address of the user whose records you want to troubleshoot.
SGT	Enter the user SGT value.

Step 3 Click **Run**.

The Progress Details page appears. The Monitoring & Report Viewer prompts you for additional input.

Step 4 Click the **User Input Required** button and modify the fields as described in Table 14-5.

Step 5 Click **Submit**.

The Progress Details page appears with a brief summary of the results.

Step 6 Click **Show Results Summary** to view the diagnosis and resolution steps.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

Comparing Device SGT with ACS-Assigned Device SGT

For TrustSec-enabled devices, ACS assigns each network device an SGT value through RADIUS authentication. The Device SGT diagnostic tool connects to the network device whose IP address you provide and does the following:

1. Obtains the network device's SGT value.
2. Checks the RADIUS authentication records to determine the SGT value that ACS had assigned to it most recently.
3. Displays the Device-SGT pairs in a tabular format and identifies whether the SGT values are the same or different.

Use this diagnostic tool to compare the device SGT with ACS-assigned device SGT. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

The Expert Troubleshooter page appears.

Step 2 Click Device SGT from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and lists the fields described in Table 14-11.

Table 14-11 Device SGT

Option	Description
Enter Information	
Network Device IPs (comma-separated list)	Enter the network device IP addresses (whose device SGT you want to compare with an ACS-assigned device SGT) separated by commas.
Common Connection Parameters	

Table 14-11 Device SGT

Option	Description
Use Common Connection Parameters	Check this check box to use the following common connection parameters for comparison: • Username—Enter the username of the network device. • Password—Enter the password. • Protocol—Choose the protocol from the Protocol drop-down list box. Valid options are: – Telnet – SSHv2 **Note** Telnet is the default option. If you choose SSHv2, 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.

Step 3 Click **Run**.

The Progress Details page appears with a summary.

Step 4 Click **Show Results Summary** to view the results of device SGT comparison.

The Results Summary page appears with the diagnosis, resolution, and troubleshooting summary.

Related Topics

- Available Diagnostic and Troubleshooting Tools, page 14-1
- Connectivity Tests, page 14-1
- ACS Support Bundle, page 14-1
- Expert Troubleshooter, page 14-2

CHAPTER 15

Managing System Operations and Configuration in the Monitoring & Report Viewer

This chapter describes the tasks that you must perform to configure and administer the Monitoring & Report Viewer. The Monitoring Configuration drawer allows you to:

- Manage data—The Monitoring & Report Viewer handles large volumes of data from ACS servers. Over a period of time, the performance and efficiency of the Monitoring & Report Viewer depends on how well you manage the data. To do so efficiently, you must back up the data and transfer it to a remote repository on a periodic basis. You can automate this task by scheduling jobs to run periodically. See Configuring Data Purging and Incremental Backup, page 15-2 for more information on data backup.
- View log collections—The Monitoring & Report Viewer collects log and configuration data from ACS servers in your deployment, stores the data in the Monitoring & Report Viewer server, and processes it to generate reports and alarms. You can view the details of the logs collected from any of the servers in your deployment. See Viewing Log Collections, page 15-6 for more information.
- View scheduled jobs—The Monitoring & Report Viewer allows you schedule tasks that you must perform periodically. For example, you can schedule an incremental or full backup to be run at regular intervals. You can use the Scheduler to view the details of these tasks. See Viewing Scheduled Jobs, page 15-10 for more information on the Scheduler.
- View process status—You can view the status of the various processes that run in the Monitoring & Report Viewer. See Viewing Process Status, page 15-10 for more information on the various processes that run in the Monitoring & Report Viewer.
- View data upgrade status—After you upgrade from ACS 5.0 to ACS 5.1 through the CLI, you must ensure that the Monitoring & Report Viewer data upgrade is complete. You can view the Monitoring & Report Viewer data upgrade status through the web interface and switch the Monitoring & Report Viewer database if upgrade is complete. See Viewing Data Upgrade Status and Switching Database, page 15-11 for more information.
- Configure and edit failure reasons—The Monitoring & Report Viewer allows you to configure the description of the failure reason code and provide instructions to resolve the problem. See Viewing Failure Reasons, page 15-12 for more information on how to edit the failure reason description and instructions for resolution.
- Configure e-mail settings—You can configure the e-mail server and administrator e-mail address. See Specifying E-Mail Settings, page 15-13 for more information.
- Configure collection filters—The Monitoring & Report Viewer provides you the option to filter data that is not used for monitoring or troubleshooting purposes. The data that is filtered is not stored in the database and hence saves much needed disk space. See Understanding Collection Filters, page 15-14 for more information on how to configure collection filters.

- Configure system alarms—System alarms notify you of critical conditions encountered during the execution of the ACS Monitoring and Reporting viewer. You can configure if and how you would like to receive notification of system alarms. See Configuring System Alarm Settings, page 15-16 for more information.
- Configure Syslog targets—If you have configured the Monitoring & Report Viewer to send system alarm notifications as Syslog messages, then you must configure a Syslog target to receive the notification. See Configuring Alarm Syslog Targets, page 15-16 for more information.
- Export Monitoring & Report Viewer data—You can configure a remote database, which could either be an Oracle SID or Microsoft AD to which you can export the Monitoring & Report Viewer data. You can create and run custom reporting applications using the data in your remote database. See Configuring Remote Database Settings, page 15-16 for more information on how to configure a remote database with the Monitoring & Report Viewer.

ACS provides you the option to schedule jobs in the Monitoring & Report Viewer. By scheduling jobs, you can automate the monitoring tasks to be run at specified intervals. You can view the status of the scheduled jobs, control events, and intervene whenever necessary. You can schedule the following jobs:

- Data Purge
- Backup
- Event notification (system and threshold alarms)
- Export of Monitoring & Report Viewer data to a remote database

This chapter contains the following sections:

- Configuring Data Purging and Incremental Backup, page 15-2
- Restoring Data from a Backup, page 15-5
- Viewing Log Collections, page 15-6
- Viewing Scheduled Jobs, page 15-10
- Viewing Process Status, page 15-10
- Viewing Data Upgrade Status and Switching Database, page 15-11
- Viewing Failure Reasons, page 15-12
- Editing Failure Reasons, page 15-12
- Specifying E-Mail Settings, page 15-13
- Configuring SNMP Preferences, page 15-13
- Understanding Collection Filters, page 15-14
- Configuring System Alarm Settings, page 15-16
- Configuring Alarm Syslog Targets, page 15-16
- Configuring Remote Database Settings, page 15-16

Configuring Data Purging and Incremental Backup

The Monitoring & Report Viewer database handles large volumes of data. When the database size becomes too large, it slows down all the processes. You do not need all the data all the time. Therefore, to efficiently manage data and to make good use of the disk space, you must back up your data regularly and purge unwanted data that uses up necessary disk space. Purging data deletes it from the database.

Since the Monitoring & Report Viewer database size is large, the backup process takes quite a bit of time to complete. ACS 5.1 introduces the incremental backup option, which enables you to take a complete backup of your Monitoring & Report Viewer database once and then to back up data incrementally (that is, only the updates are backed up and stored separately) from the next time onward. An incremental backup performs a full database backup the first time it is executed, and subsequently only backs up the updates that are made to the database. Incremental backups are therefore much faster and make efficient use of disk space. You can also configure the frequency and time of incremental backups.

With incremental backups, multiple backup files are stored in the repository. However, when you restore data from an incremental backup, ACS restores data from all the backup files starting from the full backup and continuing until the latest incremental backup.

Note If you disable incremental backup for some reason, ensure that you run a full backup the next time before you can continue with incremental backups again.

You can also configure a full database backup and define its frequency and time.

ACS also allows you to run an immediate backup of the full Monitoring & Report Viewer database. However, you cannot concurrently run an incremental backup, full backup, and data purge. If any of these jobs are running, you must wait for a period of 90 minutes before you can begin the next job.

Timesaver We recommend that you take a full backup the first time and then incrementally back up your data instead of running full backups every time.

Note To ensure that your data is backed up before the purge, configure a data repository via the CLI or the ACS web interface (**System Administration > Operations > Software Repositories**). Refer to the *CLI Reference Guide for the Cisco Secure Access Control System 5.1* for more information on configuring a repository.

If you enable incremental backup, data is purged daily at 4:00 a.m. at the local time zone where the ACS instance that runs the View process is located.

The following database limitations apply for purging:

- If the database disk usage is greater than 114 GB (95% of the total database size of 120 GB), an alarm is sent to the dashboard.
- If the database disk usage is greater than 120 GB (100% of the total database size of 120 GB), a backup is run immediately followed by a purge until the database disk usage is below 120 GB. If the backup fails, check the database disk usage again.
  - If the database disk usage is greater than 120 GB, but less than 150 GB (125% of the total database size of 120 GB), the Monitoring & Report Viewer decides to wait.
  - If the backup fails and the database disk usage is greater than 150 GB, a purge occurs regardless of whether or not a backup has occurred until the database disk usage is below 120 GB.

  For example, if you specify to preserve 5 months of data, but the database size is over 120 GB, a purge occurs. If the database size remains over 120 GB after the purge, an additional month of data is purged, which results in 4 months of data preserved. Before the purge, the database is backed up.
- If the database size is over 150 GB, a purge occurs regardless of whether or not a database backup has occurred. If the database size remains over 120 GB, additional purges occur until the database is 120 GB or less.

Note Database purge fails if we do not configure the repository and the incremental backup is set to OFF.

Note When incremental backup is disabled, data is purged at the end of every month.

You can use the Data Purging and Incremental Backup page to:

- Configure purge window size
- Purge data from the database
- Assign a data repository backup location to manage backup (of the purge job)
- Configure incremental and full backup schedules
- Configure immediate backup.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

From the Monitoring & Report Viewer, select **Monitoring Configuration > System Operations > Data Management > Removal and Backup**.

Table 15-1 Data Purging and Incremental Backup Page

Option	Description
Data Purging	
Data Repository	Use the drop-down list box to select the data repository backup location to be used during data purging. **Note** See the *CLI Reference for ACS 5.1* to add a data repository.
Maximum Stored Data Period <*num*> months.	Use the drop-down list box to indicate the number of months, where <*num*> is the number of months of data you want to retain in the Monitoring & Report Viewer database.
View Full Database Backup Now	
Data Repository	Use the drop-down list box to select the data repository backup location to store the full database backup.
Backup Now	Click **Backup Now** to start a full Monitoring & Report Viewer database backup.
Incremental Backup	
On	Click the **On** radio button to enable incremental backup.
Off	Click the **Off** radio button to disable incremental backup.
Configure Incremental View Database Backup	
Data Repository	Use the drop-down list box to select a data repository for the backup files.
Schedule	Use the drop-down list boxes to select the time of the day when you want the incremental backup to run.

Table 15-1 Data Purging and Incremental Backup Page (continued)

Option	Description
Frequency	Use the drop-down list box to choose the frequency at which you want the incremental backup to run. Valid options are: • Daily • Weekly—Typically occurs at the end of every week. • Monthly—Typically occurs at the end of every month.
Configure Full View Database Backup	
Data Repository	Use the drop-down list box to select a data repository to store the backup files.
Schedule	Use the drop-down list boxes to select the time of the day when you want the full View database backup to run.
Frequency	Use the drop-down list box to choose the frequency at which you want the full View database backup to run. Valid options are: • Daily • Weekly—Typically occurs at the end of every week. • Monthly—Typically occurs at the end of every month.

Related Topic

Restoring Data from a Backup, page 15-5

Restoring Data from a Backup

Use this page to restore data from the View database that was backed up earlier. You can restore data from an incremental or full backup. If you choose to restore incremental backup data, ACS restores the full View data backup and then the rest of the incremental backups one at a time in the correct sequence.

To restore data from a backup:

Step 1 Choose **Monitoring Configuration > System Operations > Data Management > Restore**.

The Incremental Backup Restore page appears, displaying the Available Backups to Restore table. Table 15-2 describes the columns in the table.

Table 15-2 Incremental Backup Restore Page

Column	Description
Skip View Database backup before Restore	Check this check box to skip the Monitoring & Report Viewer database backup before restoring data from a backup. This option, when checked, hastens the restore process. **Note** We recommend that you uncheck this check box because your current data might be lost if a failure occurs during the restore process.
Name	Name of the backup file. The backup filename includes the time stamp; for example, ACSViewBackup-20090618_003400. For an incremental backup, click the **Expand** icon to view the associated full and incremental backups.
Date	Date on which the backup is run.
Repository	Name of the repository that contains the backup file.
Type	The type of backup, Incremental or Full.

Step 2 Choose a backup file that you want to restore.

Note If you choose an incremental backup file to restore, ACS restores all previously associated incremental and full backups. This restore process restores only the Monitoring & Report Viewer data.

Step 3 Click **Restore** to restore the backup file.

Related Topic

Configuring Data Purging and Incremental Backup, page 15-2

Viewing Log Collections

Use this page to view the recently collected logs from ACS servers.

From the Monitoring & Report Viewer, select **Monitoring Configuration > System Operations > Log Collection**.

Note You can use the refresh symbol to refresh the contents of the page.

Table 15-3 Log Collection Page

Option	Description
ACS Server	The name of the ACS server. Click to open the Log Collection Details page and view recently collected logs.
Last Syslog Message	Display only. Indicates the arrival time of the most recent syslog message, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • timezone = The time zone. In a distributed environment, the time zone displayed for all secondary servers corresponds to the time zone of the server in which the view is active. If your primary instance has a time zone of PDT and the secondary instance is in UTC, the secondary instance displays the time zone and timestamp of syslog messages with PDT, which corresponds to the time zone of the primary instance. • yyyy = A four-digit representation of the year.
Last Error	Display only. Indicates the name of the most recent error message.
Last Error Time	Display only. Indicates the arrival time of the most recent error message, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • timezone = The time zone. In a distributed environment, the timezone displayed for all secondary servers corresponds to the timezone of the server in which the view is active. If your primary instance has a timezone of PDT and the secondary instance is in UTC, the secondary instance displays the timezone and timestamp of syslog messages with PDT, which corresponds to the timezone of the primary instance. • yyyy = A four-digit representation of the year.
Get Details	Click to view recently collected logs for a selected ACS server.

Related Topic

Log Collection Details Page, page 15-8

Log Collection Details Page

Use this page to view the recently collected log names for an ACS server.

Step 1 From the Monitoring & Report Viewer, select **Monitoring and Reports > Monitoring Configuration > Log Collection**.

Step 2 Do one of the following:

- Click the name of an ACS server.
- Select the radio button of an ACS server name which you want to view recently collected logs, and click **Get Details**.

Note You can use the refresh symbol to refresh the contents of the page.

Table 15-4 Log Collection Details Page

Option	Description
Log Name	Name of the log file.
Last Syslog Message	Display only. Indicates the arrival time of the most recent syslog message, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • timezone = The time zone. In a distributed environment, the timezone displayed for all secondary servers corresponds to the timezone of the server in which the view is active. If your primary instance has a timezone of PDT and the secondary instance is in UTC, the secondary instance displays the timezone and timestamp of syslog messages with PDT, which corresponds to the timezone of the primary instance. • yyyy = A four-digit representation of the year.
Last Error	Display only. Indicates the name of the most recent error message.
Last Error Time	Display only. Indicates the arrival time of the most recent error message, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • timezone = The time zone. In a distributed environment, the timezone displayed for all secondary servers corresponds to the timezone of the server in which the view is active. If your primary instance has a timezone of PDT and the secondary instance is in UTC, the secondary instance displays the timezone and timestamp of syslog messages with PDT, which corresponds to the timezone of the primary instance. • yyyy = A four-digit representation of the year.
Back	Click to return to the Log Collection page.
Refresh	Click to refresh the data in this page.

Related Topic

- Viewing Log Collections, page 15-6

Viewing Scheduled Jobs

Use this page to view the scheduled jobs.

From the Monitoring & Report Viewer, select **Monitoring Configuration > System Operations > Scheduler**.

Table 15-5 Scheduler Status Page

Option	Description
Name	*Display only.* The name of the job.
Type	*Display only.* The type of associated job; for example, Incremental Backup Utility, Session Termination, DB Aggregation Event, Database Purge Utility, and so on. This list includes both system- and user-defined jobs.
Owner	*Display only.* The owner of the associated job—System.
Last Run Time	*Display only.* The time of the associated job, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit representation of the year.
Last Run Result	*Display only.* The result of the last run of the associated job.
Status	*Display only.* The status of the associated job.

Note When you change any schedule through the ACS web interface, for the new schedule to take effect, you must manually restart the Job Manager process. For more information on the CLI command to restart processes, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/command/reference/cli_app_a.html#wp1618490.

Viewing Process Status

Use this page to view the status of processes running in your ACS environment.

From the Monitoring & Report Viewer, select **Monitoring Configuration > System Operations > Process Status**.

Note You can click the refresh symbol to refresh the contents of the page.

Table 15-6 Process Status Page

Option	Description
Process Name	*Display only.* The name of the process. Options can be: • Database • Management (ACS management subsystem) • Runtime (ACS runtime subsystem) • View-alertmanager • View-collector • View-database • View-jobmanager • View-logprocessor
Status	*Display only.* Indicates the status of the associated process.
CPU Utilization	*Display only.* Indicates the CPU utilization of the associated process.
Memory Utilization	*Display only.* Indicates the memory utilization of the associated process.
Uptime	*Display only.* Indicates the time that the process was started successfully, in the format *Ddd Mmm dd hh:mm:ss timezone yyyy*, where: • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • *timezone* = The time zone. • yyyy = A four-digit representation of the year.

Viewing Data Upgrade Status and Switching Database

After you upgrade to ACS 5.1, you must restore the Monitoring & Report Viewer database, ensure that the Monitoring & Report Viewer database upgrade is complete, and switch the Monitoring & Report Viewer database. You can do this through the ACS web interface. Refer to the *Installation Guide for the Cisco Secure Access Control System 5.1* for more information on the upgrade process.

To view the status of Monitoring & Report Viewer data upgrade:

Step 1 From the Monitoring & Report Viewer, select **Monitoring Configuration > System Operations > Data Upgrade Status**.

The Data Upgrade Status page appears with the following information:

- Status—Indicates whether or not the Monitoring & Report Viewer data upgrade is complete.
- Progress—Indicates the progress of the Monitoring & Report Viewer data upgrade.

Step 2 After the data upgrade status is complete, click **Switch Database**.

The Monitoring & Report Viewer stops all Viewer processes, renames the database files to conform to ACS 5.1 naming conventions, and restarts the Monitoring & Report Viewer.

Viewing Failure Reasons

Use this page to view failure reasons.

From the Monitoring & Report Viewer, select **Monitoring Configuration > System Configuration > Failure Reasons Editor**.

Table 15-7 lists the field in the Failure Reasons page.

Table 15-7 Failure Reasons Page

Option	Description
Failure Reasons	The name of possible failure reasons. Click a failure reason name to open the Failure Reasons Editor page.

Related Topic

- Editing Failure Reasons, page 15-12

Editing Failure Reasons

Use this page to edit failure reasons and include possible resolution steps to assist administrators when they encounter failures.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 From the Monitoring & Report Viewer, select **Monitoring Configuration > System Configuration > Failure Reasons Editor**.

Step 2 Click:

- The name of the failure reason you want to edit.
- The radio button associated with the failure reason you want to edit, then click **Edit**.

The Failure Reason Editor Page appears as described in Table 15-8.

Table 15-8 Failure Reasons Editor Page

Option	Description
Failure Reason	Display only. The error code and associated failure reason name.
Description	Enter a free text description of the failure reason to assist administrators; use the text tools as needed.
Resolution Steps	Enter a free text description of possible resolution steps for the failure reason to assist administrators; use the text tools as needed.

Related Topic

Viewing Failure Reasons, page 15-12

Specifying E-Mail Settings

Use this page to specify the e-mail server and administrator e-mail address.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

From the Monitoring & Report Viewer, select **Monitoring Configuration > System Configuration > Email Settings**.

Table 15-9 Email Settings Page

Option	Description
Mail Server	Enter a valid e-mail host server.
Mail From	Enter the e-mail address name that you want to configure for users to see when they receive e-mail from the system.

Configuring SNMP Preferences

You can configure SNMP preferences to authenticate access to MIB objects. The text string that you enter for SNMP preference functions as an embedded password.

To configure SNMP preferences:

Step 1 From the Monitoring & Report Viewer, choose **Monitoring Configuration > System Configuration > Collection Filters**.

The Collection Filters page appears.

Step 2 Enter a password in the SNMP V2 Read Community String field to authenticate MIB objects.

Step 3 Click **Submit**.

Understanding Collection Filters

You can create collection filters that allow you to filter and drop syslog events that are not used for monitoring or troubleshooting purposes. When you configure collection filters, the Monitoring & Report Viewer does not record these events in the database and saves much needed disk space.

To set your SNMP preferences:

Step 1 From the Monitoring & Report Viewer, choose **Monitoring Configuration > System Configuration > Collection Filters**.

The Collection Filters page appears.

Step 2 Configure SNMP preferences to authenticate access to MIB objects. For more information, see Configuring SNMP Preferences, page 15-13.

Step 3 Click **Submit**.

Your SNMP preference is now configured.

This section contains the following topics:

- Creating and Editing Collection Filters, page 15-14
- Deleting Collection Filters, page 15-15

Creating and Editing Collection Filters

Use this page to create or edit collection filters. To do this:

Step 1 From the Monitoring & Report Viewer, choose **Monitoring Configuration > System Configuration > Collection Filters**.

The Collection Filters page appears.

Step 2 In the Filters area, do one of the following:

- Click **Create** to create a collection filter.
- Check the check box of the syslog attribute that you want to edit, then click **Edit**.
- Check the check box of the syslog attribute that you want to delete, then click **Delete**.

The Add or Edit Collection Filters page described in Table 15-10 appears.

Table 15-10 Add or Edit Collection Filters Page

Option	Description
Syslog Attribute	• In the Add Filter page, choose any one of the following syslog attributes: – NAS IP Address – Access Service – MAC Address – User • In the Edit Filter page, this field is Display only.
Value	Enter the value of the syslog attribute: • NAS IP Address—Enter the IP address of the NAS that you want to filter. • Access Service—Enter the name of the access service that you want to filter. • MAC Address—Enter the MAC address of the machine that you want to filter. • User—Enter the username of the user you want to filter.

Step 3 Click **Submit**.

Related Topics

- Creating and Editing Collection Filters, page 15-14
- Deleting Collection Filters, page 15-15

Deleting Collection Filters

To delete a collection filter:

Step 1 Choose **Monitoring Configuration > System Configuration > Collection Filters**.

The Collection Filters page appears.

Step 2 Check the check box of the collection filter or filters that you want to delete, then click **Delete**.

The following message appears:

```
Are you sure you want to delete the selected item(s)?
```

Step 3 Click **Yes**.

The Collection Filters page appears without the deleted collection filter.

Configuring System Alarm Settings

See Configuring System Alarm Settings, page 12-31 for a description of how to configure system alarm settings.

Configuring Alarm Syslog Targets

See Understanding Alarm Syslog Targets, page 12-32 for a description of how to configure the syslog targets.

Configuring Remote Database Settings

Use this page to configure a remote database to which you can export the Monitoring & Report Viewer data. ACS exports data to this remote database at specified intervals. You can schedule the export job to be run once every 1, 2, 4, 6, 8, 12, or 24 hours. You can create custom reporting applications that interact with this remote database. ACS supports the following databases:

- Oracle SQL Developer
- Microsoft SQL Server 2005

Note ACS does not support remote database with cluster setup.

To configure a remote database:

Step 1 From the Monitoring & Report Viewer, choose **Monitoring Configuration > System Configuration > Remote Database Settings**.

The Remote Database Settings Page appears as described in Table 15-11.

Table 15-11 Remote Database Settings Page

Option	Description
Publish to Remote Database	Check the check box for ACS to export data to the remote database periodically. By default, ACS exports data to the remote database every 4 hours.
Server	Enter the DNS name or the IP address of the remote database.
Port	Enter the port number of the remote database.
Username	Enter the username for remote database access.
Password	Enter the password for remote database access.

Table 15-11 Remote Database Settings Page

Option	Description
Publish data every *n* hours	Choose a time interval from the drop-down list box for ACS to export data at the specified interval. Valid options are 1, 2, 4, 6, 8, 12, and 24 hours. The default interval is 4 hours.
Database Type	The type of remote database that you want to configure: • Click Microsoft Database radio button to configure a Microsoft database, and enter the name of the remote database. • Click Oracle SID radio button to configure an Oracle database, and enter the system identifier for the Oracle database.

Step 2 Click **Submit** to configure the remote database.

Note You can view the status of your export job in the Scheduler. See Viewing Scheduled Jobs, page 15-10 for more information.

CHAPTER 16

Managing System Administrators

System administrators are responsible for deploying, configuring, maintaining, and monitoring the ACS servers in your network. They can perform various operations in ACS through the ACS administrative interface. When you define an administrator in ACS, you assign a password and a role or set of roles that determine the access privilege the administrator has for the various operations.

When you create an administrator account, you initially assign a password, which the administrator can subsequently change through the ACS web interface. Irrespective of the roles that are assigned, the administrators can change their own passwords.

ACS provides the following configurable options to manage administrator passwords:

- Password Complexity—Required length and character types for passwords.
- Password History—Prevents repeated use of same passwords.
- Password Lifetime—Forces the administrators to change passwords after a specified time period.
- Account Inactivity—Disables the administrator account if it has not been in use for a specified time period.
- Password Failures—Disables the administrator account after a specified number of consecutive failed login attempts.

In addition, ACS provides you configurable options that determine the IP addresses from which administrators can access the ACS administrative web interface and the session duration after which idle sessions are logged out from the system.

You can use the Monitoring & Report Viewer to monitor administrator access to the system. The Administrator Access report is used to monitor the administrators who are currently accessing or attempting to access the system. You can view the Administrator Entitlement report to view the access privileges that the administrators have, the configuration changes that are done by administrators, and the administrator access details. In addition, you can use the Configuration Change and Operational Audit reports to view details of specific operations that each of the administrators perform.

The System Administrator section of the ACS web interface allows you to:

- Create, edit, duplicate, or delete administrator accounts
- Change the password of other administrators
- View predefined roles
- Associate roles to administrators
- Configure authentication settings that include password complexity, account lifetime, and account inactivity

- Configure administrator session setting
- Configure administrator access setting

The first time you log in to ACS 5.1, you are prompted for the predefined administrator username (*ACSAdmin*) and required to change the predefined password name (*default*). After you change the password, you can start configuring the system. The predefined administrator has super administrator permissions—Create, Read, Update, Delete, and eXecute (CRUDX)—to all ACS resources. When you register a secondary instance to a primary instance, you can use any account created on the primary instance. The credentials that you create on the primary instance apply to the secondary instance.

Note After installation, the first time you log in to ACS, you must do so through the ACS web interface and install the licenses. You cannot log in to ACS through the CLI immediately after installation.

This section contains the following topics:

- Understanding Administrator Roles and Accounts, page 16-2
- Configuring System Administrators and Accounts, page 16-3
- Understanding Roles, page 16-3
- Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-6
- Viewing Predefined Roles, page 16-8
- Configuring Authentication Settings for Administrators, page 16-9
- Configuring Session Idle Timeout, page 16-11
- Configuring Administrator Access Settings, page 16-11
- Resetting the Administrator Password, page 16-12
- Changing the Administrator Password, page 16-13

Understanding Administrator Roles and Accounts

The first time you log in to ACS 5.1, you are prompted for the predefined administrator username (*ACSAdmin*) and required to change the predefined password name (*default*).

Note You cannot rename, disable, or delete the ACSAdmin account.

After you change the password, you can start configuring the system. The predefined administrator has super administrator permissions—Create, Read, Update, Delete, and eXecute (CRUDX)—to all ACS resources.

If you do not need granular access control, the Super Admin role is most convenient, and this is the role assigned to the predefined ACSAdmin account.

To create further granularity in your access control, follow these steps:

1. Define Administrators. See Configuring System Administrators and Accounts, page 16-3.
2. Associate roles to administrators. See Understanding Roles, page 16-3

When these steps are completed, defined administrators can log in and start working in the system.

Understanding Authentication

An authentication request is the first operation for every management session. If authentication fails, the management session is terminated. But if authentication passes, the management session continues until the administrator logs out or the session times out.

ACS 5.1 authenticates every login operation by using user credentials (username and password). Then, by using the administrator and role definitions, ACS fetches the appropriate permissions and answers subsequent authorization requests.

The ACS user interface displays the functions and options for which you have the necessary administrator privileges only.

Note Allow a few seconds before logging back in so that changes in the system have time to propagate.

Related Topics

- Understanding Administrator Roles and Accounts, page 16-2
- Configuring System Administrators and Accounts, page 16-3

Configuring System Administrators and Accounts

This section contains the following topics:

- Understanding Roles
- Administrator Accounts and Role Association
- Creating, Duplicating, Editing, and Deleting Administrator Accounts
- Viewing Role Properties

Understanding Roles

Roles consist of typical administrator tasks, each with an associated set of permissions. Each administrator can have more than one predefined role, and a role can apply to multiple administrators. As a result, you can configure multiple tasks for a single administrator and multiple administrators for a single task.

You use the Administrator Accounts page to assign roles. In general, a precise definition of roles is the recommended starting point. Refer to Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-6 for more information.

Note The ACS web interface displays only the functions for which you have privileges. For example, if your role is Network Device Admin, the System Administration drawer does not appear because you do not have permissions for the functions in that drawer.

Permissions

A permission is an access right that applies to a specific administrative task. Permissions consist of:

- **A Resource** – The list of ACS components that an administrator can access, such as network resources, or policy elements.
- **Privileges** – The privileges are Create, Read, Update, Delete, and eXecute (CRUDX). Some privileges cannot apply to a given resource. For example, the user resource cannot be executed.

A resource given to an administrator without any privileges means that the administrator has no access to resources. In addition, the permissions are discrete. If the privileges create, update, and delete apply to a resource, the read privilege is not available.

If no permission is defined for an object, the administrator cannot access this object, not even for reading.

Note You cannot make permission changes.

Predefined Roles

Table 16-1 shows the predefined roles included in ACS:

Table 16-1 Predefined Role Descriptions

Role	Privileges
ChangeAdminPassword	This role is intended for ACS administrators who manage other administrator accounts. This role entitles the administrator to change the password of other administrators.
ChangeUserPassword	This role is intended for ACS administrators who manage internal user accounts. This role entitles the administrator to change the password of internal users.
NetworkDeviceAdmin	This role is intended for ACS administrators who need to manage the ACS network device repository only, such as adding, updating, or deleting devices. This role has the following permissions: • Read and write permissions on network devices • Read and write permissions on NDGs and all object types in the Network Resources drawer
PolicyAdmin	This role is intended for the ACS policy administrator responsible for creating and managing ACS access services and access policy rules, and the policy elements referenced by the policy rules. This role has the following permissions: • Read and write permissions on all the elements used in policies, such as authorization profile, NDGs, IDGs, conditions, and so on • Read and write permissions on services policy
ReadOnlyAdmin	This role is intended for ACS administrators who need read-only access to all parts of the ACS user interface. This role has read-only access to all resources
ReportAdmin	This role is intended for administrators who need access to the ACS Monitoring & Report Viewer to generate and view reports or monitoring data only. This role has read-only access on logs.

Table 16-1 Predefined Role Descriptions (continued)

Role	Privileges
SecurityAdmin	This role is required in order to create, update, or delete ACS administrator accounts, to assign administrative roles, and to change the ACS password policy. This role has the following permissions: • Read and write permissions on internal protocol users and administrator password policies • Read and write permissions on administrator account settings • Read and write permissions on administrator access settings
SuperAdmin	The Super Admin role has complete access to every ACS administrative function. If you do not need granular access control, this role is most convenient, and this is the role assigned to the predefined *ACSAdmin* account. This role has Create, Read, Update, Delete, and eXecute (CRUDX) permissions on all resources.
SystemAdmin	This role is intended for administrators responsible for ACS system configuration and operations. This role has the following permissions: • Read and write permissions on all system administration activities except for account definition • Read and write permissions on ACS instances
UserAdmin	This role is intended for administrators who are responsible for adding, updating, or deleting entries in the internal ACS identity stores, which includes internal users and internal hosts. This role has the following permissions: • Read and write permissions on users and hosts • Read permission on IDGs

Note At first login, only the Super Admin is assigned to a specific administrator.

Related Topics

- Administrator Accounts and Role Association
- Creating, Duplicating, Editing, and Deleting Administrator Accounts

Changing Role Associations

By design, all roles in ACS are predefined and cannot be changed. ACS allows you to only change role associations. Due to the potential ramifications on the system's entire authorization status, the ACS Super Admin and SecurityAdmin roles alone have the privilege to change role associations. Changes in role associations take effect only after the affected administrators log out and log in again. At the new login, ACS reads and applies the role association changes.

Note You must be careful in assigning the ACS Super Admin and SecurityAdmin roles because of the global ramifications of role association changes.

Administrator Accounts and Role Association

Administrator account definitions consist of a name, status, description, e-mail address, password, and role assignment.

Note It is recommended that you create a unique administrator for each person. In this way, operations are clearly recorded in the audit log.

Note Administrators are authenticated against the internal database only.

You can edit and delete existing accounts. However, the web interface displays an error message if you attempt to delete or disable the last super administrator.

Only appropriate administrators can configure identities and certificates. The identities configured in the System Administration drawer are available in the Users and Identity Stores drawer, but they cannot be modified there.

Related Topics

- Understanding Roles
- Creating, Duplicating, Editing, and Deleting Administrator Accounts

Creating, Duplicating, Editing, and Deleting Administrator Accounts

To create, duplicate, edit, or delete an administrator account:

Step 1 Choose **System Administration > Administrators > Accounts**.

The Administrators page appears with a list of configured administrators as described in Table 16-2:

Table 16-2 Accounts Page

Option	Description
Status	The current status of this administrator: • Enabled—This administrator is active. • Disabled—This administrator is not active. **Note** You cannot log in to ACS with a disabled admin account.
Name	The name of the administrator.
Role(s)	The role(s) assigned to the administrator.
Description	A description of this administrator.

Step 2 Perform one of these actions:

- Click **Create**.

- Check the check box next to the account that you want to duplicate and click **Duplicate**.
- Click the account that you want to modify; or, check the check box for the Name and click **Edit**.
- Check the check box next to the account for which you want to change the password and click **Change Password**. See Resetting Another Administrator's Password, page 16-13 for more information.

Note On the Duplicate page, you must change at least the Admin Name.

- Check one or more check boxes next to the accounts that you want to delete and click **Delete**.

Step 3 Complete the Administrator Accounts Properties page fields as described in Table 16-3:

Table 16-3 Administrator Accounts Properties Page

Option	Description
General	
Admin Name	The configured name of this administrator. If you are duplicating a rule, be sure to enter a unique name.
Status	From the Status drop-down menu, select whether the account is enabled or disabled. This option is disabled if you check the Account never disabled check box.
Description	A description of this administrator.
Email Address	Administrator e-mail address. ACS View will direct alerts to this e-mail address.
Account never disabled	Check to ensure that your account is never disabled. Your account will not be disabled even when: • Your password expires • Your account becomes inactive • You exceed the specified number of login retries
Authentication Information	
Password	Authentication password.
Confirm Password	Confirmation of the authentication password.
Change password on next login	Check to prompt the user for a new password at the next login.
Role Assignment	
Available Roles	A list of all configured roles. Select the roles that you want to assign for this administrator and click >. Click >> to assign all the roles for this administrator.
Assigned Roles	The roles that apply to this administrator.

Step 4 Click **Submit**.

The new account is saved. The Administrators page appears, with the new account that you created or duplicated.

Related Topics

- Understanding Roles, page 16-3

- Administrator Accounts and Role Association, page 16-6
- Viewing Predefined Roles, page 16-8
- Configuring Authentication Settings for Administrators, page 16-9

Viewing Predefined Roles

See Table 16-1 for description of the predefined roles included in ACS.

To view predefined roles:

Choose **System Administration > Administrators > Roles**.

The Roles page appears with a list of predefined roles. Table 16-4 describes the Roles page fields.

Table 16-4 Roles Page

Field	Description
Name	A list of all configured roles. See Predefined Roles, page 16-4 for a list of predefined roles.
Description	The description of each role.

Viewing Role Properties

Use this page to view the properties of each role.

Choose **System Administration > Administrators > Roles, and click a role or choose the role's radio button and click View**.

The Roles Properties page appears as described in Table 16-5:

Table 16-5 Roles Properties Page

Field	Description
Name	The name of the role. If you are duplicating a role, you must enter a unique name as a minimum configuration; all other fields are optional. Roles cannot be created or edited. See Table 16-4 for a list of predefined roles.
Description	The description of the role. See Predefined Roles, page 16-4 for more information.
Permissions List	
Resource	A list of available resources.
Privileges	The privileges that can be assigned to each resource. If a privilege does not apply, the privilege check box is dimmed (not available). **Note** Row color is irrelevant to availability of a given privilege and is determined by the explicit text in the Privileges column.

Related Topics

- Understanding Roles, page 16-3
- Administrator Accounts and Role Association, page 16-6
- Configuring Authentication Settings for Administrators, page 16-9

Configuring Authentication Settings for Administrators

Authentication settings are a set of rules that enhance security by forcing administrators to use strong passwords, regularly change their passwords, and so on. Any password policy changes that you make apply to all ACS system administrator accounts.

To configure a password policy:

Step 1 Choose **System Administration > Administrators > Settings > Authentication**.

The Password Policies page appears with the Password Complexity and Advanced tabs.

Step 2 In the **Password Complexity** tab, check each check box that you want to use to configure your administrator password. Table 16-6 describes the fields in the Password Complexity tab.

Table 16-6 Password Complexity Tab

Option	Description
Applies to all ACS system administrator accounts	
Minimum length	The required minimum length; the valid options are 4 to 20.
Password may not contain the username or its characters in reversed order	Check to specify that the password cannot contain the username or reverse username. For example, if your username is john, your password cannot be john or nhoj.
Password may not contain ‘cisco’ or its characters in reversed order	Check to specify that the password cannot contain the word *cisco* or its characters in reverse order, that is, *ocsic*.
Password may not contain ‘’ or its characters in reversed order	Check to specify that the password does not contain the string that you enter or its characters in reverse order. For example, if you specify a string, polly, your password cannot be polly or yllop.
Password may not contain repeated characters four or more times consecutively	Check to specify that the password cannot repeat characters four or more times consecutively. For example, you cannot have the string apppple as your password. The letter p appears four times consecutively.
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	Password must contain at least one lowercase alphabetic character.
Upper case alphabetic characters	Password must contain at least one uppercase alphabetic character.
Numeric characters	Password must contain at least one numeric character.
Non alphanumeric characters	Password must contain at least one nonalphanumeric character.

Step 3 In the **Advanced** tab, enter the values for the criteria that you want to configure for your administrator authentication process. Table 16-7 describes the fields in the Advanced tab.

Table 16-7 Advanced Tab

Options	Description
Password History	
Password must be different from the previous *n* versions	Specifies the number of previous passwords for this administrator to be compared against. This option prevents the administrators from setting a password that was recently used. Valid options are 1 to 99.
Password Lifetime: Administrators are required to periodically change password	

Table 16-7 Advanced Tab

Options	Description
Display reminder after *n* days	Displays a reminder after *n* days to change password; the valid options are 1 to 365. This option, when set, only displays a reminder. It does not prompt you for a new password.
Require a password change after *n* days	Specifies that the password must be changed after *n* days; the valid options are 1 to 365. This option, when set, ensures that you change the password after n days.
Disable administrator account after *n* days if password is not changed	Specifies that the administrator account must be disabled after *n* days if the password is not changed; the valid options are 1 to 365. **Note** ACS does not allow you to configure this option without configuring the Display reminder after *n* days option.
Account Inactivity	
Inactive accounts are disabled	
Require a password change after *n* days of inactivity	Specifies that the password must be changed after *n* days of inactivity; the valid options are 1 to 365. This option, when set, ensures that you change the password after *n* days. **Note** ACS does not allow you to configure this option without configuring the Display reminder after *n* days option.
Disable administrator account after *n* days of inactivity	Specifies that the administrator account must be disabled after *n* days of inactivity; the valid options are 1 to 365. **Note** ACS does not allow you to configure this option without configuring the Display reminder after *n* days option.
Incorrect Password Attempts	
Disable account after *n* successive failed attempts	Specifies the maximum number of login retries after which the account is disabled; the valid options are 1 to 10.

Note ACS automatically deactivates or disables your account based on your last login, last password change, or number of login retries. The CLI and PI user accounts are blocked and they receive a notification that they can change the password through the web interface. If your account is disabled, contact another administrator to enable your account.

Step 4 Click **Submit**.

The administrator password is configured with the defined criteria. These criteria will apply only for future logins.

Related Topics

- Understanding Roles, page 16-3
- Administrator Accounts and Role Association, page 16-6
- Viewing Predefined Roles, page 16-8

Configuring Session Idle Timeout

A GUI session, by default, is assigned a timeout period of 30 minutes. You can configure a timeout period for anywhere from 5 to 90 minutes.

To configure the timeout period:

Step 1 Choose **System Administration > Administrators > Settings > Session**.

The GUI Session page appears.

Step 2 Enter the Session Idle Timeout value in minutes. Valid values are 5 to 90 minutes.

Step 3 Click **Submit**.

Note The CLI client interface has a default session timeout value of 6 hours. You cannot configure the session timeout period in the CLI client interface.

Configuring Administrator Access Settings

ACS 5.1 allows you to restrict administrative access to ACS based on the IP address of the remote client. You can filter IP addresses in any one of the following ways:

- Allow All IP Addresses to Connect, page 16-11
- Allow Remote Administration from a Select List of IP Addresses, page 16-11
- Reject Remote Administration from a Select List of IP Addresses, page 16-12

Allow All IP Addresses to Connect

You can choose the Allow all IP addresses to connect option to allow all connections; this is the default option.

Allow Remote Administration from a Select List of IP Addresses

To allow administrators to access ACS remotely:

Step 1 Choose **System Administration > Administrators > Settings > Access**.

The IP Addresses Filtering page appears.

Step 2 Click Allow only listed IP addresses to connect radio button.

The IP Range(s) area appears.

Step 3 Click **Create** in the IP Range(s) area.

A new window appears. Enter the IP address of the machine from which you want to allow remote access to ACS. Enter a subnet mask for an entire IP address range.

Step 4 Click **OK.**

The IP Range(s) area is populated with the IP addresses. Repeat Step 3 to add other IP addresses or ranges for which you want to provide remote access.

Step 5 Click **Submit**.

Reject Remote Administration from a Select List of IP Addresses

To reject administrators from accessing ACS remotely:

Step 1 Choose **System Administration > Administrators > Settings > Access**.

The IP Addresses Filtering page appears.

Step 2 Click Reject connections from listed IP addresses radio button.

The IP Range(s) area appears.

Step 3 Click **Create** in the IP Range(s) area.

A new window appears. Enter the IP address of the machine that you do not want to access ACS remotely. Enter a subnet mask for an entire IP address range.

Step 4 Click **OK**.

The IP Range(s) area is populated with the IP addresses. Repeat Step 3 to add other IP addresses or ranges that you want to reject.

Step 5 Click **Submit**.

Note It is possible to reject connection from all IP addresses. You cannot reset this condition through the ACS web interface. However, you can use the following CLI command:

access-setting accept-all

Refer to the *CLI Reference Guide for Cisco Secure Access Control System 5.1* for more information.

Resetting the Administrator Password

While configuring administrator access settings, it is possible for all administrator accounts to get locked out, with none of the administrators able to access ACS from any IP address in your enterprise. If this happens, you must reset the administrator password from the ACS Config CLI. You must use the following command to reset all administrator passwords:

access-setting accept-all

For more information on this command, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/command/reference/cli_app_a.html#wp1697683.

Note You cannot reset the administrator password through the ACS web interface.

Changing the Administrator Password

ACS 5.1 introduces a new role Change Admin Password that entitles an administrator to change another administrator's password. If an administrator's account is disabled, any other administrator who is assigned the Change Admin Password role can reset the disabled account through the ACS web interface. This section contains the following topics:

- Changing Your Own Administrator Password, page 16-13
- Resetting Another Administrator's Password, page 16-13

Changing Your Own Administrator Password

Note All administrators can change their own passwords. You do not need any special roles to perform this operation.

To change your password:

Step 1 Choose **My Workspace > My Account**.

The My Account page appears. See My Account Page, page 5-2 for valid values.

Step 2 In the **Password field** section, enter the current administrator password.

Step 3 In the New Password field, enter a new administrator password.

Step 4 In the Confirm Password field, re-enter the new administration password.

Step 5 Click **Submit**.

The administrator password is created.

You can also use the **acs reset-password** command to reset your ACSAdmin account password. For more information on this command, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/command/reference/cli_app_a.html#wp1208469.

Resetting Another Administrator's Password

To reset another administrator's password:

Step 1 Choose **System Administration > Administrators > Accounts**.

The Accounts page appears with a list of administrator accounts.

Step 2 Check the check box next to the administrator account for which you want to change the password and click **Change Password**.

The Authentication Information page appears, listing the date when the administrator's password was last changed.

Step 3 In the Password field, enter a new administrator password.

Step 4 In the Confirm Password field, re-enter the new administrator password.

Step 5 Check the **Change password on next login** check box for the other administrator to change password at first login.

Step 6 Click **Submit**.

The administrator password is reset.

Related Topics

- Configuring Authentication Settings for Administrators, page 16-9
- Understanding Roles, page 16-3
- Administrator Accounts and Role Association, page 16-6
- Viewing Predefined Roles, page 16-8

CHAPTER 17

Configuring System Operations

You can configure and deploy ACS instances so that one ACS instance becomes the *primary instance* and the other ACS instances can be registered to the primary as *secondary instances*. An ACS instance represents ACS software that runs on a network. An ACS deployment may consist of a single instance, or multiple instances deployed in a distributed manner, where all instances in a system are managed centrally. All instances in a system will have an identical configuration.

Use the Distributed System Management page to manage all the instances in a deployment. You can only manage instances from the primary instance. You can invoke the Deployment Operations page from any instance in the deployment but it only controls the operations on the local server.

Note You can register any primary instance or any secondary instance to another primary instance; however, the primary instance you wish to register cannot have any secondary instances registered to it.

The primary instance, created as part of the installation process, centralizes the configuration of the registered secondary instances. Configuration changes made in the primary instance are automatically replicated to the secondary instance. You can force a *full replication* to the secondary instance if configuration changes do not replicate to the secondary instance.

Related Topic

- Understanding Distributed Deployment, page 17-1
- Understanding Software Updates, page 17-22

Understanding Distributed Deployment

You can configure multiple ACS servers in a deployment. Within any deployment, you designate one server as the *primary* server and all the other servers are *secondary* servers. In general, you make configuration changes on the primary server only, and the changes are propagated to all secondary servers, which can then view the configuration data as read-only data. A small number of configuration changes can be performed on a secondary server, including configuration of the server certificate, and these changes remain local to the server.

Secondary servers do not know the status of other secondary servers. However, a low-level communication is required and traffic should be allowed between secondary servers in an ACS distributed server domain.

ACS allows you to deploy an ACS instance behind a firewall. Table 17-1 lists the ports that must be open on the firewall for you to access ACS through the various management interfaces.

Table 17-1 Ports to Open in Firewalls

Service	Port
ACS Web Interface/Web Service	443
Database replication	TCP 2638
RADIUS server	• 1812 and 1645 (RADIUS authentication and authorization) • 1813 and 1646 (RADIUS accounting) If your RADIUS server uses port 1812, ensure that your PIX firewall software is version 6.0 or later. Then, issue the following command to use port 1812: **aaa-server radius-authport** *1812*
Replication over the Message Bus	TCP 61616
RMI	TCP 2020 (for RMI registry service)
	TCP 2030 (for incoming calls)
SNMP (for request)	UDP 161
SNMP (for notifications)	UDP 162
SSH	22
TACACS+ server	TCP 49
View Collector	UDP 20514

The Distributed System Management page can be used to monitor the status of the servers in a deployment and perform operations on the servers.

Related Topics

- Activating Secondary Servers, page 17-2
- Removing Secondary Servers, page 17-3
- Promoting a Secondary Server, page 17-3
- Understanding Local Mode, page 17-3
- Understanding Full replication, page 17-4
- Specifying a Hardware Replacement, page 17-4

Activating Secondary Servers

To add a server to a deployment, you must perform two steps:

1. From the secondary server, issue a request to register on the primary server by selecting the Deployment Operations option.
2. Activate the secondary instance on the primary server. You must activate the secondary instance on the primary instance in order for the secondary instance to receive configuration information; this provides a mechanism of admission control. However, there is an option to automatically activate newly added secondary instances, rather than performing a manual activation request.

Related Topics

- Removing Secondary Servers, page 17-3
- Promoting a Secondary Server, page 17-3
- Understanding Local Mode, page 17-3
- Understanding Full replication, page 17-4
- Specifying a Hardware Replacement, page 17-4

Removing Secondary Servers

To permanently removed a secondary server from a deployment, you must first deregister the secondary server and then delete it from the primary. You can make the request to deregister a server from either the secondary server to be deregistered or from the primary server.

Related Topics

- Activating Secondary Servers, page 17-2
- Understanding Distributed Deployment, page 17-1

Promoting a Secondary Server

There can be one server only that is functioning as the primary server. However, you can promote a secondary server so that is assumes the primary role for all servers in the deployment. The promotion operation is performed either on the secondary server that is to assume the primary role or on the primary server.

Note When the primary server is down, do not simultaneously promote two secondary servers.

Related Topics

- Activating Secondary Servers, page 17-2
- Removing Secondary Servers, page 17-3
- Understanding Local Mode, page 17-3
- Understanding Full replication, page 17-4

Understanding Local Mode

You can use the local mode option:

- If the primary server is unreachable from a secondary server (for example, there is a network disconnection) and a configuration change must be made to a secondary server, you can specify that the secondary server go into *Local Mode*.
- If you want to perform some configuration changes on a trial basis that would apply to only one server and not impact all the servers in your deployment, you can specify that one of your secondary servers go into *Local Mode*.

In Local Mode, you can make changes to a single ACS instance through the local web interface, and the changes take effect on that instance only. The Configuration Audit Report available in the Monitoring & Report Viewer has an option to report only those configuration changes that were made in the local mode. You can generate this report to record the changes that you made to the secondary server in Local Mode. For more information on reports and how to generate them from ACS, see Chapter 13, "Managing Reports".

When the connection to the primary server resumes, you can reconnect the disconnected secondary instance in Local Mode to the primary server. From the secondary instance in Local Mode, you specify the Admin username and password to reconnect to the primary instance. All configuration changes made while the secondary server was in Local Mode are lost.

Related Topics

- Activating Secondary Servers, page 17-2
- Understanding Full replication, page 17-4

Understanding Full replication

Under normal circumstances, each configuration change is propagated to all secondary instances. Unlike ACS 4.x where full replication was performed, in ACS 5.1, only the specific changes are propagated. As configuration changes are performed, the administrator can monitor (on the Distributed System Management page) the status of the replication and the last replication ID to ensure the secondary server is up to date.

If configuration changes are not being replicated as expected, the administrator can request a full replication to the server. When you request full replication, the full set of configuration data is transferred to the secondary server to ensure the configuration data on the secondary server is re synchronized.

Note Replication on the Message Bus happens over TCP port 61616. Full replication happens over the Sybase DB TCP port 2638.

Related Topics

- Activating Secondary Servers, page 17-2
- Promoting a Secondary Server, page 17-3
- Understanding Local Mode, page 17-3

Specifying a Hardware Replacement

You can perform a hardware replacement to allow new or existing ACS instance hardware to re-register to a primary server and take over an existing configuration already present in the primary server. This is useful when an ACS instance fails and needs physical replacement. There are three steps required to perform the hardware replacement procedure:

1. From the web interface of the primary instance, you must mark the server to be replaced as deregistered.

2. From the secondary server, register to the primary server. In addition to the standard admin credentials for connecting to the primary server (username/password), you must specify the replacement keyword used to identify the configuration in the primary server. The keyword is the hostname of the instance that is to be replaced.
3. You must active the secondary server on the primary, either automatically or by issuing a manual request.

Related Topics

- Viewing and Editing a Primary Instance, page 17-8
- Viewing and Editing a Secondary Instance, page 17-12
- Activating a Secondary Instance, page 17-13
- Registering a Secondary Instance to a Primary Instance, page 17-14
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-16
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-18
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-21

Scheduled Backups

You can schedule backups to be run at periodic intervals. You can schedule backups from the primary web interface or through the local CLI. The Scheduled Backups feature backs up ACS configuration data.

Note You cannot back up data from an earlier version of ACS and restore it to a later version. Backup and restore must be performed on the same version of ACS. If you need the data on a different version of the ACS, you can perform an upgrade after you restore the data. Refer to the *Installation and Setup Guide for Cisco Secure Access Control System 5.1* for more information on upgrading ACS to later versions.

Related Topic

Creating, Duplicating, and Editing Scheduled Backups, page 17-5

Creating, Duplicating, and Editing Scheduled Backups

You can create a scheduled backup only for the primary instance. To create, duplicate, or edit a scheduled backup:

Step 1 Choose **System Administration > Operations > Scheduled Backups**.

The Scheduled Backups page appears. Table 17-2 describes the fields listed in the Scheduled Backups page.

Table 17-2 Scheduled Backups Page

Option	Description
Backup Data	
Filename created by backup includes a time stamp and file type information appended to the prefix entered	
Filename Prefix	Enter a filename prefix to which ACS appends the backup time stamp. For example, if you enter ACSBackup as the filename prefix and backup is run on June 05, 2009 at 20:37 hours, then ACS creates the backup file ACSBackup-090506-2037.tar.gpg. **Note** In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name.
Repository	Click **Select** to open the Software Update and Backup Repositories dialog box, from which you can select the appropriate repository in which to store the backup file.
Schedule Options	
Time of Day	Choose the time of the day at which you want ACS to back up the ACS configuration data. Backups can be scheduled on a daily, weekly, or monthly basis. • Daily—Choose this option for ACS to back up the ACS configuration data at the specified time every day. • Weekly—Choose this option and specify the day of the week on which you want ACS to back up the ACS configuration data every week. • Monthly—Choose this option and specify the day of the month on which you want ACS to back up the ACS configuration data every month.

Step 2 Click **Submit** to schedule the backup.

Related Topic

Backing Up Primary and Secondary Instances, page 17-6

Backing Up Primary and Secondary Instances

ACS provides you the option to back up the primary and secondary instances at any time apart from the regular scheduled backups. For a primary instance, you can back up the following:

- ACS configuration data only
- ACS configuration data and ADE-OS configuration data

Note For secondary instances, ACS only backs up the ADE-OS configuration data.

To run an immediate backup:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

Step 2 From the Primary Instance table or the Secondary Instances table, select the instance that you want to back up.

Note You can select only one primary instance, but many secondary instances for a backup.

Step 3 Click **Backup**.

The Distributed System Management - Backup page appears with the fields described in Table 17-3.

Table 17-3 Distributed System Management - Backup Page

Option	Description
Backup Data	
Filename created by backup includes a time stamp and file type information appended to the prefix entered	
Filename Prefix	Enter a filename prefix to which ACS appends the backup time stamp. For example, if you enter ACSBackup as the filename prefix and backup is run on June 05, 2009 at 20:37 hours, then ACS creates the backup file ACSBackup-090506-2037.tar.gpg. **Note** In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name.
Repository	Click **Select** to open the Software Update and Backup Repositories dialog box, from which you can select the appropriate repository in which to store the backup file.
Backup Options (only applicable for primary instances)	
ACS Configuration Backup	Click this option if you want to back up only the ACS configuration data.
ACS Configuration and ADE-OS Backup	Click this option if you want to back up both the ACS configuration data and the ADE-OS configuration data.

Step 4 Click **Submit** to run the backup immediately.

Related Topic

Scheduled Backups, page 17-5

Synchronizing Primary and Secondary Instances After Backup and Restore

When you specify that a system backup is restored on a primary instance, the secondary instance is not updated to the newly restored database that is present on the primary instance.

To make sure the secondary instance is updated, from the secondary instance, you need to request a hardware replacement to rejoin the restored primary instance. First, you must deregister the secondary instance from the primary instance. From the web interface of the secondary instance, choose **Systems Administration > Operations > Local Operations > Deployment Operations**, then click **Deregister from Primary**. After this step, you can perform the hardware replacement of the secondary instance to the primary instance again by choosing **Systems Administration > Operations > Local Operations >**

Deployment Operations; then specify the primary hostname or IP address and the admin credential, select Hardware Replacement, specify the hostname of the secondary instance, and click **Register to Primary**.

Editing Instances

When you Choose **System Administration > Operations > Distributed System Management**, you can edit either the primary or secondary instance. You can take a backup of primary and secondary instances. The Distributed System Management page allows you to do the following:

- Viewing and Editing a Primary Instance, page 17-8
- Viewing and Editing a Secondary Instance, page 17-12
- Backing Up Primary and Secondary Instances, page 17-6
- Synchronizing Primary and Secondary Instances After Backup and Restore, page 17-7

Viewing and Editing a Primary Instance

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To edit a primary instance:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with two tables:

- Primary Instance table—Shows the primary instance.

Note The primary instance is created as part of the installation process.

- Secondary Instances table—Shows a listing and the status of the secondary instances. See Viewing and Editing a Secondary Instance, page 17-12 for more information.

The Distributed System Management Page displays the information described in Table 17-4:

Table 17-4 Distributed System Management Page

Option	Description
Primary Instance	
Name	The hostname of the primary instance.
IP Address	The IP address of the primary instance.
Online Status	Indicates if the primary instance is online or offline. A check mark indicates that the primary instance is online; **x** indicates that the primary instance is offline.

Table 17-4 Distributed System Management Page (continued)

Option	Description
Replication ID	The transaction ID that identifies the last configuration change on the primary instance. This value increases by 1 for every configuration change. Valid values are 1 to infinity.
Last Update	Time stamp of the last database configuration change. The time stamp is in the form *hh:mm dd:mm:yyyy*.
Version	The current version of the ACS software running on the primary ACS instance. Valid values can be the version string or, if a software upgrade is initiated, *Upgrade in progress*.
Description	A description of the primary instance.
Edit	Select the primary instance and click this button to edit the primary instance.
Backup	Select the primary instance and click this button to back up the primary instance. See Backing Up Primary and Secondary Instances, page 17-6 for more information.
Secondary Instances	
Name	The hostname of the secondary instance.
IP Address	The IP address of the secondary instance.
Online Status	Indicates if the secondary instance is online or offline. A check mark indicates that the secondary instance is online; **x** indicates that the secondary instance is offline.
Replication Status	Replication status values are: • UPDATED—Replication is complete on the secondary instance. Both Management and Runtime services are current with configuration changes from the primary instance. • PENDING—Request for full replication has been initiated or the configuration changes made on the primary have not yet been propagated to the secondary. • REPLICATING—Replication from the primary to the secondary is processing. • LOCAL MODE—The secondary instance does not receive replication updates from the deployment and maintains its own local configuration. • DEREGISTERED—The secondary instance is deregistered from the primary instance and is not part of the deployment. • INACTIVE—The secondary instance is inactive. You must select this instance and click **Activate** to activate this instance. • N/A—No replication on primary instance.
Replication Time	Time stamp of the last replication. The time stamp is in the form *hh:mm dd:mm:yyyy*.
Version	The current version of the ACS software running on the secondary ACS instance. Valid values can be the version string or, if a software upgrade is initiated, *Upgrade in progress*.
Description	A description of the secondary instance.
Edit	Select the secondary instance that you want to edit and click this button to edit it.
Delete	Select the secondary instance that you want to delete and click this button to delete it.
Activate	If the option to auto-activate the newly registered secondary instance is disabled, the secondary is initially placed in the inactive state. Click **Activate** to activate these inactive secondary instances.

Table 17-4 Distributed System Management Page (continued)

Option	Description
Deregister[1]	Disconnects the secondary instance from the primary instance. Stops the secondary instance from receiving configuration updates from the primary instance. Deregistration restarts the deregistered node. **Note** When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance.
Promote	Requests to promote a secondary instance to the primary instance. All updates to the current primary instance are stopped so that all replication updates can complete. The secondary instance gets primary control of the configuration when the replication updates complete. **Note** The secondary instance must be active before you can promote it to the primary instance.
Full Replication	Replicates the primary instance's database configuration for the secondary instance. ACS is restarted. **Note** When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance.
Backup	Select the secondary instance that you want to back up and click this button to take a backup. See Backing Up Primary and Secondary Instances, page 17-6 for more information.

1. Deregistration restarts the deregistered node, but does not restart ACS. Registration and Full Replication restart ACS because the database is replaced.

Step 2 From the Primary Instance table, click the primary instance that you want to modify, or check the **Name** check box and click **Edit**.

Step 3 Complete the fields in the Distributed System Management Properties page as described inTable 17-5:

Table 17-5 Distributed System Management Properties Page

Option	Description
Instance Data	
Hostname	The name of the ACS host machine.
Launch Session for Local GUI	Click this button to launch a new instance of the selected ACS machine. You are required to log in to the primary or secondary instance. **Note** This option appears only when you view or edit another instance.
Role	Specifies a primary or secondary instance or Local.
IP Address	The IP address of the primary or secondary instance.
Port	The port for Management service.
MAC Address	MAC address for the instance.
Description	A description of the primary or secondary instance.
Check Secondary Every (only applies for primary instance)	The rate at which the primary instance sends a heartbeat status request to the secondary instance. The default value is 60 seconds. The minimum value is 30 seconds and the maximum value is 30 minutes.

Table 17-5 Distributed System Management Properties Page (continued)

Option	Description
Statistics Polling Period (only applies for primary instance)	The rate at which the primary instance polls the secondary instance for statistical and logging information. The default value is 60 seconds. The minimum value is 60 seconds; however, you can specify a value of 0 which indicates to turn off polling and logging. The maximum value is 30 minutes.
Enable Auto Activation for Newly Registered Instances (only applies for primary instance)	Check this check box to automatically activate the registered secondary instance.
Instance Status	
Status	Indicates if the primary instance or secondary instance is online or offline.
Version	The current version of the ACS software.
Replication Status (only applies for secondary instances)	Replication status values are: • UPDATED—Replication is complete on ACS instance. Both management and runtime services are current with configuration changes from the primary instance. • PENDING—Request for full replication has been initiated. • REPLICATING—Replication from the primary to the secondary is processing. • DEREGISTERED—Deregistered the secondary instance from the primary. • N/A—No replication on primary instance.
Last Update Time (only applies for primary instance)	Time stamp of the last database configuration change. The time stamp is in the form *hh:mm dd:mm:yyyy*.
Last Replication Time (only applies for secondary instances)	Time stamp of the last replication. The time stamp is in the form *hh:mm dd:mm:yyyy*.
Last Replication ID (only applies for primary instance)	The transaction ID that identifies the last configuration change on the secondary instances. This value increases by 1 for every configuration change. Valid values are 1 to infinity.
Primary Replication ID (only applies for secondary instances)	The transaction ID that identifies the last configuration change on the primary instance. This value increases by 1 for every configuration change. Valid values are 1 to infinity.

Step 4 Click **Submit**.

The Primary Instance table on the Distributed System Management page appears with the edited primary instance.

Related Topics

- Replicating a Secondary Instance from a Primary Instance, page 17-19
- Viewing and Editing a Secondary Instance, page 17-12

Viewing and Editing a Secondary Instance

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To edit a secondary instance:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with two tables:

- Primary Instance table—Shows the primary instance.
- Secondary Instances table—Shows a listing and the status of the secondary instances registered to the primary instance.

See Table 17-4 to view column definitions.

Step 2 From the Secondary Instances table, click the secondary instances that you want to modify; or, check the check box for the Name and click **Edit**.

Step 3 Complete the fields in the Distributed System Management Properties page as described inTable 17-5.

Step 4 Click **Submit**.

The Secondary Instances table on the Distributed System Management page appears with the edited secondary instance.

Related Topics

- Editing Instances, page 17-8
- Viewing and Editing a Primary Instance, page 17-8

Deleting a Secondary Instance

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To delete a secondary instance:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Secondary Instances table on the Distributed System Management page appears with a list of secondary instances.

Step 2 Deregister the secondary instance you wish to delete. Refer to Deregistering Secondary Instances from the Distributed System Management Page, page 17-16.

Step 3 Check one or more check boxes next to the secondary instances that you want to delete.

Step 4 Click **Delete**.

The following warning message appears:

Are you sure you want to delete the selected item/items?

Step 5 Click **OK**.

The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instance(s).

Activating a Secondary Instance

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To activate a secondary instance:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with two tables:

- Primary Instance table—Shows the primary instance.
- Secondary Instances table—Shows a listing and the status of the secondary instances registered to the primary instance.

See the Table 17-4 to view column descriptions.

Step 2 From the Secondary Instances table, check the check box next to the secondary instances that you want to activate.

Step 3 Click **Activate**.

Step 4 The Secondary Instances table on the Distributed System Management page appears with the activated secondary instance. See the Table 17-5 for valid field options.

Related Topics

- Viewing and Editing a Secondary Instance, page 17-12
- Deleting a Secondary Instance, page 17-12
- Replicating a Secondary Instance from a Primary Instance, page 17-19
- Registering a Secondary Instance to a Primary Instance, page 17-14
- Deregistering a Secondary Instance from the Deployment Operations Page, page 17-17
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-18
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-21

Registering a Secondary Instance to a Primary Instance

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To register a secondary instance to a primary instance:

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

The Deployment Operations page appears, displaying the information described in Table 17-6:

Table 17-6 System Operations: Deployment Operations Page

Option	Description
Instance Status	
Current Status	Identifies the instance of the node you log into as primary or secondary, and identifies whether you are running in local mode.
Primary Instance	The hostname of the primary instance.
Primary IP	The IP address of the primary instance.
Registration (only active for an instance not running in Local Mode)	
Primary Instance	The hostname of the primary server that you wish to register with the secondary instance.
Admin Username	Username of an administrator account.
Admin Password	The password for the administrator's account.
Hardware Replacement	Check to enable a new or existing ACS instance hardware to re-register to a primary instance and acquire the existing configuration already present in the primary instance. This is useful when an instance fails and needs physical replacement.
Recovery Keyword	The name of the instance that is to be replaced. This value is the hostname of the system that is being replaced. After you submit this information, this instance connects to the primary instance. The primary instance finds the associated ACS instance records based on the keyword, and marks each record as registered.
Register to Primary	Connects to the remote primary and registers the secondary instance to the primary instance.
Backup	
Backup	Backs up the current instance.
Local Mode	
Admin Username	Username of an administrator account.
Admin Password	The password for the administrators account.

Table 17-6 System Operations: Deployment Operations Page (continued)

Option	Description
Reconnect **Note** This option appears only on the local mode node and prompts you for credentials.	Click **Reconnect** to reconnect to the primary instance. Once you reconnect to the primary instance, you lose the configuration changes that you have made to the local secondary instance. If you want to retain the configuration changes that you have made to the local secondary instance, you must: 1. Deregister the local secondary instance (this instance would become your new primary) 2. Deregister all the instances from the deployment. 3. Register all the instances to the new primary, whose configuration changes you want to retain.
Request Local Mode **Note** This option appears only on a registered secondary page.	Request to place the secondary instance in local mode. This enables administrators to make configuration changes only to this instance. Any changes made to the secondary instance are not automatically updated when you reconnect to the primary instance. You must manually enter your changes for the secondary instance.
Deregistration	
Deregister from Primary	Deregisters the secondary from the primary instance. The secondary instance retains the database configuration from when it was deregistered. All nodes are marked as deregistered and inactive, and the secondary instance becomes the primary instance. **Note** When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance.
Promotion	
Promote to Primary	Request to promote a secondary instance to primary instance. All updates to the current primary instance are stopped so that all replication updates can complete. The secondary instance gets primary control of the configuration when the replication updates complete.
Replication	
Force Full Replication	Replicates the primary instance's database configuration for the secondary instance. **Note** When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance.

Step 2 Specify the appropriate values in the **Registration** section.

Step 3 Click **Register to Primary**.

The system displays the following warning message:

This operation will register this ACS Instance as a secondary to the specified Primary Instance. ACS will be restarted. You will be required to login again. Do you wish to continue?

Step 4 Click **OK**.

Note When you register a secondary to a primary instance, you can use any account created on the primary instance. The credentials that you create on the primary instance are applied to the secondary instance.

Step 5 Log in to the ACS machine after restart.

Step 6 Choose **System Administration > Operations > Local Operations > Deployment Operations.**

The Deployment Operations page appears with the secondary instance registered to the primary instance.

Deregistering Secondary Instances from the Distributed System Management Page

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To deregister secondary instances from the Distributed System Management page:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

Step 2 From the Secondary Instances table, check one of check boxes next to the secondary instances that you want to deregister.

Step 3 Click **Deregister**.

The system displays the following warning message:

This operation will deregister this server as a secondary with the primary server. ACS will be restarted. You will be required to login again. Do you wish to continue?

Step 4 Click **OK**.

Step 5 Log in to the ACS machine.

Step 6 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with the secondary instance deregistered from the primary instance.

Related Topics

- Viewing and Editing a Secondary Instance, page 17-12
- Deleting a Secondary Instance, page 17-12
- Activating a Secondary Instance, page 17-13
- Deregistering a Secondary Instance from the Deployment Operations Page, page 17-17
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-18
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-21

Deregistering a Secondary Instance from the Deployment Operations Page

Note In this case, the secondary instance is the local machine you are logged in to.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To deregister a secondary instance from the Deployment Operations page:

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

The Deployment Operations page appears with the secondary instance that you are logged in to. See Table 17-6 for valid field options.

Step 2 Click **Deregister from Primary**.

The system displays the following warning message:

This operation will deregister this server as a secondary with the primary server. ACS will be restarted. You will be required to login again. Do you wish to continue?

Step 3 Click **OK**.

Step 4 Log in to the ACS machine.

Step 5 Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears with the secondary instance you were logged in to deregistered from the primary instance.

Related Topics

- Viewing and Editing a Secondary Instance, page 17-12
- Deleting a Secondary Instance, page 17-12
- Activating a Secondary Instance, page 17-13
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-16
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-18
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-21

Promoting a Secondary Instance from the Distributed System Management Page

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To promote a secondary instance to a primary instance from the Distributed System Management page:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears. See Table 17-4 for valid field options.

Step 2 From the Secondary Instances table, check the box next to the secondary instance that you want to promote to a primary instance.

Step 3 Click **Promote**.

The Distributed System Management page appears with the promoted instance.

Related Topics

- Viewing and Editing a Secondary Instance, page 17-12
- Deleting a Secondary Instance, page 17-12
- Activating a Secondary Instance, page 17-13
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-16
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-21

Promoting a Secondary Instance from the Deployment Operations Page

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To promote a secondary instance to a primary instance from the Deployment Operations page:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Deployment Operations page appears. See the Table 17-6 for valid field options.

Step 2 Register the secondary instance to the primary instance. See Registering a Secondary Instance to a Primary Instance, page 17-14.

Step 3 Choose **System Administration > Operations > Distributed System Management**.

The Deployment Operations page appears.

Step 4 Check the box next to the secondary instance that you want to promote to a primary instance.

Step 5 Click **Promote to Primary**.

The Distributed System Management page appears with the promoted instance.

Related Topics

- Viewing and Editing a Secondary Instance, page 17-12
- Deleting a Secondary Instance, page 17-12
- Replicating a Secondary Instance from a Primary Instance, page 17-19
- Activating a Secondary Instance, page 17-13
- Deregistering Secondary Instances from the Distributed System Management Page, page 17-16
- Promoting a Secondary Instance from the Distributed System Management Page, page 17-18
- Using the Deployment Operations Page to Create a Local Mode Instance, page 17-21

Replicating a Secondary Instance from a Primary Instance

You can use two different pages to replicate a secondary instance:

- Replicating a Secondary Instance from the Distributed System Management Page
- Replicating a Secondary Instance from the Deployment Operations Page

Note For more information on replication, see ACS 4.x and 5.1 Replication, page 1-2.

Replicating a Secondary Instance from the Distributed System Management Page

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Note All ACS appliances must be in sync with the AD domain clock.

To replicate a secondary instance:

Step 1 Choose System Administration > Operations > Distributed System Management.

The Distributed System Management page appears.

Step 2 From the Secondary Instances table, check one of check boxes next to the secondary instances that you want to replicate.

Step 3 Click **Full Replication**.

The system displays the following warning message:

This operation will force a full replication for this secondary server. ACS will be restarted. You will be required to login again. Do you wish to continue?

Step 4 Click **OK**.

Step 5 Log in to the ACS machine.

Step 6 Choose **System Administration > Operations > Distributed System Management.**

The Distributed System Management page appears. On the Secondary Instance table, the Replication Status column shows **UPDATED**. Replication is complete on the secondary instance. Management and runtime services are current with configuration changes from the primary instance.

Replicating a Secondary Instance from the Deployment Operations Page

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Note All ACS appliances must be in sync with the AD domain clock.

To replicate a secondary instance:

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

The Deployment Operations page appears. See the Table 17-6 for valid field options.

Step 2 Click **Force Full Replication**.

Note The Force Full Replication button only appears if the secondary instance is the local machine you are logged in to.

The system displays the following warning message:

This operation will force a full replication for this secondary server. ACS will be restarted. You will be required to login again. Do you wish to continue?

Step 3 Click **OK**.

Step 4 Log in to the ACS machine.

Step 5 Choose **System Administration > Operations > Distributed System Management.**

The Distributed System Management page appears. On the Secondary Instance table, the Replication Status column shows **UPDATED**. Replication is complete on the secondary instance. Management and runtime services are current with configuration changes from the primary instance.

Using the Deployment Operations Page to Create a Local Mode Instance

When the secondary instance is in local mode it does not receive any configuration changes from the primary instance. The configuration changes you make to the secondary instance are local and do not propagate to the primary instance.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Choose **System Operations > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears. See the Table 17-4 for valid field options.

Step 2 Specify the appropriate values in the Registration section for the secondary instance you want to register.

Step 3 Click **Register to Primary**.

The system displays the following warning message:

This operation will register this ACS Instance as a secondary to the specified Primary Instance. ACS will be restarted. You will be required to login again. Do you wish to continue?

Step 4 Click **OK**.

Step 5 Log in to the ACS local machine.

Step 6 Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears.

Step 7 Click **Request Local Mode.**

The secondary instance is now in local mode.

Note Once you reconnect the secondary instance to a primary instance you will lose the configuration changes you made to the local secondary instance. You must manually restore the configuration information for the primary instance. You can use the configuration information on the ACS Configuration Audit report to manually restore the configuration information for this instance.

Understanding Software Updates

You can use the ACS web interface to apply software patches for updating your ACS instances. A software patch is represented by the fifth digit in the software version. For example, ACS 5.1.0.34.1 is a patch for software version 5.1.0.34.

A software update is different than an upgrade. You must use the Command Line Interface (CLI) to upgrade your ACS. For information on upgrade, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/installation/guide/acs5_1_install_guide.html.

When you define a software patch in the Centralized Software Updates page, ACS retrieves the specified patch file from the repository or from your local disk and checks for the format of the software file (whether it is a patch file).

When you apply a software patch, ACS checks whether the software file is intended for the ACS version that is installed on selected ACS instances. For example, a software patch file, ACS 5.1.0.34.1 can only be installed on ACS instances that run ACS 5.1.0.34.

You can use a file browser to obtain the software patch file from your local hard disk. Alternatively, ACS can retrieve the software patch file from a repository that you choose.

Note If you specify a repository, ensure that the software patch file is available in that repository.

Creating, Duplicating, Editing, and Deleting Software Repositories

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, edit, or delete a software repository:

Step 1 Choose **System Administration > Operations > Software Repositories**.

The Software Repositories page appears with the information described in Table 17-7:

Table 17-7 Software Repositories Page

Option	Description
Name	The name of the software repository. **Note** In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name.
Protocol	The name of the protocol (DISK, FTP, SFTP, TFTP, NFS) you want to use to transfer the upgrade file.
Server Name	The name of the server.
Path	The name of the path for the directory containing the upgrade file. You must specify the protocol and the location of the upgrade file; for example, ftp://acs-home/updates.
Description	A description of the software repository.

Step 2 Perform one of these actions:

- Click **Create**.
- Check the check box next to the software repository that you want to duplicate and click **Duplicate**.
- Click the software repository that you want to modify; or, check the check box for the name and click **Edit**.
- Check one or more check boxes next to the software repository that you want to delete and click **Delete**.

The Software Update Repositories Properties Page page appears.

Step 3 Complete the fields in the Software Repositories Properties Page as described in Table 17-8:

Table 17-8 Software Update Repositories Properties Page

Option	Description
General	
Name	Name of the software repository. **Note** In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name.
Description	Description of the software repository.
Repository Information	
Protocol	The name of the protocol that you want to use to transfer the upgrade file. Valid options are: • DISK—If you choose this protocol, you must provide the path. • FTP—If you choose this protocol, you must provide the server name, path, and credentials. • SFTP—If you choose this protocol, you must provide the server name, path, and credentials. • TFTP—If you choose this protocol, you must enter the name of the TFTP server. You can optionally provide the path. • NFS—If you choose this protocol, you must provide the server name and path. You can optionally provide the credentials. If you choose this protocol, make sure that ACS has full access to the NFS file system. You must have read-write and allow root access permissions on the NFS file system.
Server Name	Name of the FTP, SFTP, TFTP, or NFS server.
Note that the actual location that the repository points to is /localdisk/<path>	
Path	The name of the path for the directory containing the upgrade file. You must specify the protocol and the location of the upgrade file; for example, ftp://acs-home/updates.
User Credentials	
Username	Administrator name.
Password	Administrator password.

Step 4 Click **Submit**.

The new software repository is saved. The Software Repository page appears, with the new software repository that you created, duplicated, or edited.

Related Topics

- Creating, Duplicating, Editing, and Deleting a Software File or Patch, page 17-24
- Managing Software Repositories from the Web Interface and CLI, page 17-27

Creating, Duplicating, Editing, and Deleting a Software File or Patch

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, edit, or delete a software image or patch:

Step 1 Choose **System Administration > Operations > Centralized Software Updates**.

The Centralized Software Updates page appears with the information displayed in Table 17-9:

Table 17-9 Centralized Software Updates Page

Option	Description
Name	The name of the software file or patch.
Version	The current version of the ACS software.
Software Repository	The name of the repository location you wish to store your software update and patch files as well as ACS back up files.
Software Filename	The name of the software update or patch files.
Description	The description of the software update or patch files.

Step 2 Perform one of these actions:

- Click **Create**.
- Check the check box next to the software file or patch that you want to duplicate and click **Duplicate**.
- Click the software file or patch that you want to modify; or, check the check box for the Name and click **Edit**.
- Check one or more check boxes next to the software file or patch that you want to delete and click **Delete**.

The Centralized Software Updates Properties Create page appears.

Step 3 Complete the fields in the Centralized Software Updates Properties Create page as described in Table 17-10:

Table 17-10 Centralized Software Updates Properties Create Page

Option	Description
Software Update Information	
Name	The name of the upgrade or patch file.

Table 17-10 Centralized Software Updates Properties Create Page (continued)

Option	Description
Description	Description of the upgrade or patch file.
Software File Location	
Upload Software Update	Choose this radio button to browse for the software file that you wish to use to upgrade from your local hard drive.
Retrieve Software Update from Repository	Choose this radio button to select the software file that you wish to use to upgrade from a repository. If you choose this option, you must: • Select the repository that contains the software file. • Enter the name of the software file.

Step 4 Click **Submit**.

The new software file or patch is saved. The Centralized Software Updates page appears, with the new software file or patch that you created, duplicated, or edited.

Related Topics

- Creating, Duplicating, Editing, and Deleting Software Repositories, page 17-22
- Managing Software Repositories from the Web Interface and CLI, page 17-27

Applying Local Software Updates

You can select the local ACS instance to which to apply an upgrade or patch.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Choose **Operations > Local Operations > Local Software Updates**.

Step 2 Complete the fields as described in Table 17-11:

Table 17-11 Apply Local Software Updates Page

Option	Description
Name	The name of the software file or patch.
Version	The current version of the ACS software.
Software Repository	The name of the repository location that contains your software update and patch files.
Software Filename	The name of the software update or patch files.
Description	The description of the software update or patch files.

Step 3 Click **Apply Software Update**.

Applying a Software Update to the ACS Instance

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To apply a software update to an ACS Instance:

Step 1 Choose **System Administration > Operations > Centralized Software Updates**.

The Centralized Software Updates page appears. See Table 17-9for valid field options.

Step 2 Check the check box next to the software file you want to use for the update.

Step 3 Click **Apply Software Update**.

The Centralized Software Updates Apply page appears.

Step 4 Complete the fields in the Centralized Software Updates Apply page as described in Table 17-12:

Table 17-12 Centralized Software Updates Apply Page

Option	Description
Name	The name of the ACS instance you wish to upgrade.
IP Address	The IP address of the ACS instance you wish to upgrade
Role	Specifies the instance type: primary or secondary.
Version	The current version number of the ACS application.
Description	The description of the ACS instance you wish to upgrade.
Apply Software Update	Click this button to apply the software update to the selected instance.

Step 5 Check the check box next to the ACS instance you want to update.

Step 6 Click **Apply Software Update** to update the ACS instance software by using the software file.

You get the following message:

```
This operation will update the software version on the selected ACS instance.
After the new version is loaded the ACS instance will be restarted and any connected
administrators will need to login again.
Do you wish to continue?
```

Step 7 Click **OK** to apply the software update.

Related Topics

- Creating, Duplicating, Editing, and Deleting Software Repositories, page 17-22
- Managing Software Repositories from the Web Interface and CLI, page 17-27

Managing Software Repositories from the Web Interface and CLI

You can manage repositories from the web interface or the CLI. Keep in mind the rules for creating or deleting repositories from the web interface or CLI:

- If you create a repository from the CLI, that repository is not visible from the web interface, and can only be deleted from the CLI.
- If you create a repository from the web interface, it can be deleted from the CLI; however, that repository still exists in the web interface. If you use the web interface to create a repository for a software update, the repository is automatically created again in the CLI.
- If you delete a repository using the web interface, it is also deleted in the CLI.

Related Topics

- Creating, Duplicating, Editing, and Deleting Software Repositories, page 17-22
- Creating, Duplicating, Editing, and Deleting a Software File or Patch, page 17-24

CHAPTER 18

Managing System Administration Configurations

After you install Cisco Secure ACS, you must configure and administer it to manage your network efficiently. The ACS web interface allows you to easily configure ACS to perform various operations. For a list of post-installation configuration tasks to get started with ACS, see Chapter 6, "Post-Installation Configuration Tasks".

When you select **System Administration > Configuration** you can access pages that allow you do the following:

- Configure global system options, including settings for TACACS+, EAP-TTLS, PEAP, and EAP-FAST. See Configuring Global System Options, page 18-1.
- Configure protocol dictionaries. See Managing Dictionaries, page 18-5.
- Manage local sever certificates. See Configuring Local Server Certificates, page 18-14.
- Manage log configurations. See Configuring Logs, page 18-21.
- Manage licensing. See Licensing Overview, page 18-35.

Configuring Global System Options

From the **System Administration > Configuration > Global System Options** pages, you can view these options:

- Configuring TACACS+ Settings, page 18-1
- Configuring EAP-TLS Settings, page 18-2
- Configuring PEAP Settings, page 18-3
- Configuring EAP-FAST Settings
- Generating EAP-FAST PAC

Configuring TACACS+ Settings

Use the TACACS+ Settings page to configure TACACS+ runtime characteristics.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Select **System Administration > Configuration > Global System Options > TACACS+ Settings.**

The TACACS+ Settings page appears as described in Table 18-1:

Table 18-1 TACACS+ Settings

Option	Description
Port to Listen	The port number on which to listen. By default, the port number is displayed as 49 and you cannot edit this field.
Connection Timeout	Number of minutes before the connection times out.
Session Timeout	Number of minutes before the session times out.
Maximum Packet Size	Maximum packet size (in bytes).
Single Connect Support	Check to enable single connect support.
Login Prompts	
Username Prompt	A text string to use as the username prompt.
Password Prompt	A text string to use as the password prompt.
Password Change Control	
Enable TELNET Change Password	Choose this option if you want to provide an option to change password during a TELNET session.
Prompt for Old Password:	A text string to use as the old password prompt.
Prompt for New Password	A text string to use as the new password prompt.
Prompt for Confirm Password	A text string to use as the confirm password prompt.
Disable TELNET Change Password	Choose this option if you do not want change password during a TELNET session.
Message when Disabled	The message that is displayed when you choose the Disable TELNET Change Password option.

Configuring EAP-TLS Settings

Use the EAP-TLS Settings page to configure EAP-TLS runtime characteristics.

Select **System Administration > Configuration > Global System Options > EAP-TLS Settings.**

The EAP-TLS Settings page appears as described in Table 18-2:

Table 18-2 EAP-TLS Settings

Option	Description
Enable EAP-TLS Session Resume	Check this box to support abbreviated reauthentication of a user who has passed full EAP-TLS authentication. This feature provides reauthentication of the user with only an SSL handshake and without the application of certificates. EAP-TLS session resume works only within the EAP-TLS session timeout value.
EAP-TLS session timeout	Enter the number of seconds before the EAP-TLS session times out.

Configuring PEAP Settings

Use the PEAP Settings page to configure PEAP runtime characteristics.

Select **System Administration > Configuration > Global System Options > PEAP Settings.**

The PEAP Settings page appears as described in Table 18-3:

Table 18-3 PEAP Settings

Option	Description
Enable PEAP Session Resume	When checked, ACS caches 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, ACS uses the cached TLS session, resulting in faster PEAP performance and a lessened AAA server load. You must specify a PEAP session timeout value for the PEAP session resume features to work.
PEAP Session Timeout	Enter the number of seconds before the PEAP session times out. The default value is 7200 seconds.
Enable Fast Reconnect	Check to allow a PEAP session to resume in ACS without checking user credentials when the session resume feature is enabled.

Related Topic

- Generating EAP-FAST PAC, page 18-4

Configuring EAP-FAST Settings

Use the EAP-FAST Settings page to configure EAP-FAST runtime characteristics.

Select **System Administration > Configuration > Global System Options > EAP-FAST > Settings.**

The EAP-FAST Settings page appears as described in Table 18-4:

Table 18-4 EAP-FAST Settings

Option	Description
General	
Authority Identity Info Description	A user-friendly string that describes the ACS server that sends credentials to a client. The client can discover this string in the Protected Access Credentials Information (PAC-Info) Type-Length-Value (TLV). The default value is Cisco Secure ACS.

Table 18-4 EAP-FAST Settings (continued)

Option	Description
Master Key Generation Period	The value is used to encrypt or decrypt and sign or authenticate PACs. The default is one week.
Revoke	
Revoke	Click **Revoke** to revoke all previous master keys and PACs. This operation should be used with caution. **Note** If the ACS node is a secondary node, the Revoke option is disabled.

Generating EAP-FAST PAC

Use the EAP-FAST Generate PAC page to generate a user or machine PAC.

Step 1 Select **System Administration > Configuration > Global System Options > EAP-FAST > Generate PAC.**

The Generate PAC page appears as described in Table 18-5:

Table 18-5 Generate PAC

Option	Description
Tunnel PAC	Select to generate a tunnel PAC.
Machine PAC	Select to generate a machine PAC.
Identity	Specifies the username or machine name presented as the “inner username” by the EAP-FAST protocol. If the Identity string does not match that username, authentication will fail.
PAC Time To Live	Enter the equivalent maximum value in days, weeks, months and years, and enter a positive integer.
Password	Enter the password.

Step 2 Click **Generate PAC**.

Configuring RSA SecurID Prompts

You can configure RSA prompts for an ACS deployment. The set of RSA prompts that you configure is used for all RSA realms and ACS instances in a deployment. To configure RSA SecurID Prompts:

Step 1 Choose **System Administration > Configuration > Global System Options > RSA SecurID Prompts**.

The RSA SecurID Prompts page appears.

Step 2 Modify the fields described in Table 18-6.

Table 18-6 RSA SecurID Prompts Page

Option	Description
Next Token Prompt	A text string to request for the next token. The default value is “Enter Next TOKENCODE:”.
Choose PIN Type Prompt	A text string to request the PIN type. The default value is “Do you want to enter your own pin?”.
Accept System PIN Prompt	A text string to accept the system-generated PIN. The default value is “ARE YOU PREPARED TO ACCEPT A SYSTEM-GENERATED PIN?”.
Note: For the two PIN entry prompts below, if the prompt contains the following strings, they will be substituted as follows: **{MIN_LENGTH}- will be replaced by the minimum PIN length configured for the RSA Realm** **{MAX_LENGTH}- will be replaced by the maximum PIN length configured for the RSA Realm**	
Alphanumeric PIN Prompt	A text string for requesting an alphanumeric PIN.
Numeric PIN Prompt	A text string for requesting a numeric PIN.
Re-Enter PIN Prompt	A text string to request the user to re-enter the PIN. The default value is “Reenter PIN:”.

Step 3 Click **Submit** to configure the RSA SecurID Prompts.

Managing Dictionaries

The following tasks are available when you select **System Administration > Configuration > Dictionaries**:

- Viewing RADIUS and TACACS+ Attributes, page 18-5
- Configuring Identity Dictionaries, page 18-10

Viewing RADIUS and TACACS+ Attributes

The RADIUS and TACACS+ Dictionary pages display the available protocol attributes in these dictionaries:

- RADIUS (IETF)
- RADIUS (Cisco)
- RADIUS (Microsoft)
- RADIUS (Ascend)
- RADIUS (Cisco Airespace)
- RADIUS (Cisco Aironet)
- RADIUS (Cisco BBSM)
- RADIUS (Cisco VPN 3000)
- RADIUS (Cisco VPN 5000)

- RADIUS (Juniper)
- RADIUS (Nortel [Bay Networks])
- RADIUS (RedCreek)
- RADIUS (US Robotics)
- TACACS+

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To view and choose attributes from a protocol dictionary, select **System Administration > Configuration > Dictionaries > Protocols;** then choose a dictionary.

The Dictionary page appears with a list of available attributes as shown in Table 18-7:

Table 18-7 Protocols Dictionary Page

Option	Description
Attribute	The name of the attribute.
ID	(RADIUS only) The VSA ID.
Type	The data type of the attribute.
Direction	(RADIUS only) Specifies where the attribute is in use: in the request, in the response, or both. Single or bidirectional authentication.
Multiple Allowed	(RADIUS only) Multiple attributes are allowed. Attributes that specify *multiple allowed* can be used more than once in one request or response.

Use the arrows to scroll through the attribute list.

ACS 5.1 also supports RADIUS vendor-specific attributes (VSAs). A set of predefined RADIUS VSAs are available. You can define additional vendors and attributes from the ACS web interface. You can create, edit, or delete RADIUS VSAs. After you have defined new VSAs, you can use them in policies, authorization profiles, and RADIUS token servers in the same way as predefined VSAs. For more information, see:

- RADIUS VSAs, page A-6.
- Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-6

Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes

Vendor-Specific Attributes (VSAs) allow vendors to create extension to the RADIUS attributes. The vendors have a specific vendor number assigned to them. VSAs are attributes that contain subattributes. ACS 5.1 allows you to create, duplicate, or edit RADIUS VSA (VSAs). To do this:

Note Some of the internally used attributes cannot be modified.

Note You cannot modify an attribute's type if the attribute is used by any policy or policy element.

Step 1 Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS VSA**.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the RADIUS VSA that you want to duplicate, then click **Duplicate**.
- Check the check box next to the RADIUS VSA that you want to edit, then click **Edit**.

The Create RADIUS VSA page appears. Modify the fields as described in Table 18-8.

Table 18-8 RADIUS VSA - Create, Duplicate, Edit Page

Option	Description
Attribute	Name of the RADIUS VSA.
Description	(Optional) A brief description of the RADIUS VSA.
Vendor ID	ID of the RADIUS vendor.
Attribute Prefix	(Optional) Prefix that you want to prepend to the RADIUS attribute so that all attributes for the vendor start with the same prefix.
Use Advanced Vendor Options	
Vendor Length Field Size	A vendor length field of 8 bits for specifying the length of the VSA. Choose the vendor length of the VSA. Valid options are 0 and 1. The default value is 1.
Vendor Type Field Size	A vendor type field of 8 bits. Choose the vendor type of the VSA. Valid options are 1, 2, and 4. The default value is 1.

Step 3 Click **Submit** to save the changes.

Related Topics

Viewing RADIUS and TACACS+ Attributes, page 18-5

Creating, Duplicating, and Editing RADIUS Vendor-Specific Subattributes

To create, duplicate, and edit RADIUS vendor-specific subattributes:

Step 1 Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA**.

You can alternatively choose the RADIUS VSA from the navigation pane.

Step 2 Do one of the following:

- Click **Create** to create a subattribute for this RADIUS VSA.
- Check the check box next to the RADIUS VSA that you want to duplicate, then click **Duplicate**.
- Check the check box next to the RADIUS VSA that you want to edit, then click **Edit**.

Step 3 The RADIUS VSA subattribute create page appears.

Step 4 Complete the fields described in Table 18-9.

Table 18-9 Creating, Duplicating, and Editing RADIUS Subattributes

Option	Description
General	
Attribute	Name of the subattribute. The name must be unique.
Description	(Optional) A brief description of the subattribute.
RADIUS Configuration	
Vendor Attribute ID	Enter the vendor ID field for the subattribute. This value must be unique for this vendor.
Direction	Specifies where the attribute is in use: in the request, in the response, or both. Single or bidirectional authentication.
Multiple Allowed	Multiple attributes are allowed. Attributes that specify *multiple allowed* can be used more than once in one request or response.
Include attribute in the log	Check this check box to include the subattribute in the log. For sensitive attributes, you can uncheck this check box so to they are not logged.
Attribute Type	
Attribute Type	Type of the attribute. Valid options are: • String • Unsigned Integer 32 • IPv4 Address • HEX String • Enumeration—If you choose this option, you must enter the ID-Value pair **Note** You cannot use attributes of type HEX String in policy conditions.

Table 18-9 Creating, Duplicating, and Editing RADIUS Subattributes

Option	Description
ID-Value	(Optional) *For the Enumeration attribute type only.* • ID—Enter a number from 0 to 999. • Value—Enter a value for the ID. • Click **Add** to add this ID-Value pair to the ID-Value table. To edit, replace, and delete ID-Value pairs: • Select the ID-Value pair from the ID-Value table. • Click **Edit** to edit the ID and Value fields. Edit the fields as required. • Click **Add** to add a new entry after you modify the fields. • Click **Replace** to replace the same entry with different values. • Click **Delete** to delete the entry from the ID-Value table.
Attribute Configuration	
Add Policy Condition	Check this check box to enter a policy condition in which this subattribute will be used.
Policy Condition Display Name	Enter the name of the policy condition that will use this subattribute.

Step 5 Click **Submit** to save the subattribute.

Viewing RADIUS Vendor-Specific Subattributes

To view the attributes that are supported by a particular RADIUS vendor:

Step 1 Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA**.

The RADIUS VSA page appears.

Step 2 Check the check box next to the vendor whose attribute you want to view, then click **Show Vendor Attributes**.

The vendor-specific attributes and the fields listed in Table 18-7 are displayed. You can create additional VSAs, and duplicate or edit these attributes. For more information, see Creating, Duplicating, and Editing RADIUS Vendor-Specific Subattributes, page 18-7.

Related Topic

Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-6

Configuring Identity Dictionaries

This section contains the following topics:

- Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-10
- Deleting an Internal User Identity Attribute, page 18-12
- Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-13
- Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-13
- Deleting an Internal Host Identity Attribute, page 18-13

Creating, Duplicating, and Editing an Internal User Identity Attribute

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, and edit an internal user identity attribute:

Step 1 Select **System Administration > Configuration > Dictionaries > Identity > Internal Users**.

The Attributes list for the Internal Users page appears.

Step 2 Perform one of these actions:

- Click **Create**.
- Check the check box next to the attribute that you want to duplicate and click **Duplicate**.
- Click the attribute name that you want to modify; or, check the check box for the name and click **Edit**.

The Identity Attribute Properties page appears.

Step 3 Modify the fields in the Identity Attributes Properties page as required. See Configuring Internal Identity Attributes, page 18-11 for field descriptions.

Step 4 Click **Submit**.

The internal user attribute configuration is saved. The Attributes list for the Internal Users page appears with the new attribute configuration.

Related Topics

- Deleting an Internal User Identity Attribute, page 18-12
- Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-13
- Policies and Identity Attributes, page 3-16

Configuring Internal Identity Attributes

Table 18-10 describes the fields in the internal <*users* | *hosts*> identity attributes.

Table 18-10 Identity Attribute Properties Page

Option	Description
General	
Attribute	The name of the attribute.
Description	A description of the attribute.
Attribute Type	
Attribute Type	(Optional) Use the drop-down list box to choose an attribute type. Valid options are: • String—Populates the Maximum Length and Default Value fields in the page. • Unsigned Integer 32—Populates the Valid Range From and To fields in the page. • IPv4 Address—Populates the Default Value field in the page. • Boolean—Populates the Default Value check box in the page. • Date—Populates the Default Value field and calendar icon in the page. • Enumeration—Populates the ID and Value fields and the Add, Edit, Replace, and Delete buttons.
Maximum Length	(Optional) *For the String attribute type only.* Enter the maximum length of your attribute. The valid range is from 1 to 256. (Default = 32)
Value Range	(Optional) *For the Unsigned Integer attribute type only.* • From—Enter the lowest acceptable integer value. The valid range is from 0 to 2^31-1 (2147483647). This value must be smaller than the Valid Range To value. • To—Enter the highest acceptable integer value. The valid range is from 0 to 2^31-1 (2147483647). This value must be larger than the Valid Range From value.
Default Value	Enter the default value for the appropriate attribute: • String—Up to the maximum length. (Follow the UTF-8 standard.) You can use the letters a to z, A to Z, and the digits 0 to 9. • Unsigned Integer 32—An integer in the range from 0 to 2^31-1 (2147483647). • IPv4 Address—Enter IP address you want to associate with this attribute, in the format: *x.x.x.x*, where *x.x.x.x* is the IP address (no subnet mask). • Date—Click the calendar icon to display the calendar popup and select a date. • Boolean Value—Select True or False.

Table 18-10 Identity Attribute Properties Page (continued)

Option	Description
ID-Value	(Optional) *For the Enumeration attribute type only.* • ID—Enter a number from 0 to 999. • Value—Enter a value for the ID. • Click **Add** to add this ID-Value pair to the ID-Value table. To edit, replace, and delete ID-Value pairs: • Select the ID-Value pair from the ID-Value table. • Click **Edit** to edit the ID and Value fields. Edit the fields as required. • Click **Add** to add a new entry after you modify the fields. • Click **Replace** to replace the same entry with different values. • Click **Delete** to delete the entry from the ID-Value table.
Attribute Configuration	
Mandatory Fields	Check the check box to make this attribute a requirement in the User Properties page.
Add Policy Condition	Check the check box to create a custom condition from this attribute. When you check this option, you must enter a name in the Policy Condition Display Name field.
Policy Condition Display Name	Enter a name for the policy condition. After you submit this page, the condition appears in the **Policy Elements > Session Conditions > Custom** page.

Deleting an Internal User Identity Attribute

To delete an internal user identity attribute:

Step 1 Select **System Administration > Configuration > Dictionaries > Identity > Internal Users**.

The Attributes list for the internal user page appears.

Step 2 Check the check box next to the attribute you want to delete. Because deleting an identity attribute can take a long time to process, you can delete only one attribute at a time.

Step 3 Click **Delete**.

Step 4 For confirmation, click **OK** or **Cancel**.

The Attributes list for the internal user page appears without the deleted attribute.

Related Topics

- Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-10
- Policies and Identity Attributes, page 3-16

Creating, Duplicating, and Editing an Internal Host Identity Attribute

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create, duplicate, and edit an internal host identity attribute:

Step 1 Select **System Administration > Configuration > Dictionaries > Identity > Internal Hosts**.

The Attributes list for the Internal Hosts page appears.

Step 2 Perform one of these actions:

- Click **Create**.
- Check the check box next to the attribute that you want to duplicate and click **Duplicate**.
- Click the attribute name that you want to modify; or, check the check box for the name and click **Edit**.

The Identity Attribute Properties page appears.

Step 3 Modify the fields in the Identity Attributes Properties page as required. See Table 18-10 for field descriptions.

Step 4 Click **Submit**.

The internal host attribute configuration is saved. The Attributes list for the Internal Hosts page appears with the new attribute configuration.

Related Topics

- Deleting an Internal Host Identity Attribute, page 18-13
- Policies and Identity Attributes, page 3-16

Deleting an Internal Host Identity Attribute

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To delete an internal host identity attribute:

Step 1 Select **System Administration > Configuration > Dictionaries > Identity > Internal User**.

The Attributes list for the Internal Hosts page appears.

Step 2 Check the check box next to the attribute you want to delete. Because deleting an attribute can take a long time to process, you can delete only one attribute at a time.

Step 3 Click **Delete**.

Step 4 For confirmation, click **OK** or **Cancel**.

The Attributes list for the Internal Hosts page appears without the deleted attribute.

Related Topics

- Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-13
- Policies and Identity Attributes, page 3-16

Configuring Local Server Certificates

Local server certificates are also known as ACS server certificates. ACS uses the local server certificates to identify itself to the clients. The local server certificates are used by:

- EAP protocols that use SSL/TLS tunneling.
- Management interface to authenticate the web interface (GUI).

This section contains the following topics:

- Adding Local Server Certificates, page 18-14
- Importing Server Certificates and Associating Certificates to Protocols, page 18-15
- Generating Self-Signed Certificates, page 18-16
- Generating a Certificate Signing Request, page 18-17
- Binding CA Signed Certificates, page 18-18
- Editing and Renewing Certificates, page 18-19
- Deleting Certificates, page 18-20
- Exporting Certificates, page 18-20
- Viewing Outstanding Signing Requests, page 18-21

Adding Local Server Certificates

You can add a local server certificate, also known as an ACS server certificate, to identify the ACS server to clients.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **System Administration > Configuration > Local Server Certificates > Local Certificates**. The Local Certificates page appears displaying the information in Table 18-11:

Table 18-11 Local Certificates Page

Option	Description
Friendly Name	The name that is associated with the certificate.
Issued To	The entity to which the certificate is issued. The name that appears is from the certificate subject.
Issued By	Trusted party that issued the certificate.
Valid From	The date the certificate is valid from.
Valid To (Expiration)	The date the certificate is valid to.
Protocol	The protocol associated with the certificate.

Step 2 Click **Add**.

Step 3 Enter the information in the Local Certificate Store Properties page as described in Table 18-12:

Table 18-12 Local Certificate Store Properties Page

Option	Description
Import Server Certificate	Select to browse the client machine for the Local Certificate file and import the private key and private key password. See Importing Server Certificates and Associating Certificates to Protocols, page 18-15. **Note** Supported certificate formats include, DER, PEM, or Microsoft private key proprietary format.
Generate Self Signed Certificate	Select to generate a self-signed certificate. See Generating Self-Signed Certificates, page 18-16.
Generate Certificate Signing Request	Select to generate a certificate signing request. See Generating a Certificate Signing Request, page 18-17.
Bind CA Signed Certificate	Select to bind the CA certificate. After the RA signs the request, you can install the returned signed certificate on ACS and bind the certificate with its corresponding private key. See Binding CA Signed Certificates, page 18-18.

Importing Server Certificates and Associating Certificates to Protocols

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Note The supported certificate formats are either DER or PEM.

Step 1 Select **System Administration > Configuration > Local Server Certificates > Certificate Installations >Add**, then select **Import Server Certificate** > **Next**.

Step 2 Enter the information in the ACS Import Server Certificate as described in Table 18-13:

Table 18-13 Import Server Certificate Page

Option	Description
Certificate File	Select to browse the client machine for the local certificate file.
Private Key File	Select to browse to the location of the private key.
Private Key Password	Enter the private key password. The value may be minimum length = 0 and maximum length = 256.
Protocol	
EAP	Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP.
Management Interface	Check to associate the certificate with the management interface.
Override Policy	
Replace Certificate	Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections.

Step 3 Click **Finish.**

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

Generating Self-Signed Certificates

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **System Administration > Configurations > Local Server Certificates > Certificate Installations > Add** and then select **Generate Self Signed Certificate> Next**.

Step 2 Enter the information in the ACS Import Server Certificate as described in Table 18-14:

Table 18-14 Generate Self Signed Certificate Step 2

Option	Description
Certificate Subject	Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field is prefixed with “cn=”.
Key Length	Key length entered during generation of this request.Values may be 512, 1024, 2048, or 4096.

Table 18-14 Generate Self Signed Certificate Step 2

Option	Description
Digest to Sign with	This field is populated with the value SHA1 for ACS 5.1.
Expiration TTL	Select the equivalent maximum value in days, weeks, months, and years, and enter a positive integer.
Protocol	
EAP	Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP.
Management Interface	Check to associate the certificate with the management interface.
Override Policy	
Replace Certificate	Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections.

Step 3 Click **Finish.**

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

Generating a Certificate Signing Request

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **System Administration > Configurations > Local Server Certificates > Certificate Installations > Add** and then select **Generate Certificate Signing Request > Next**.

Step 2 Enter the information in the ACS Import Server Certificate as described in Table 18-15:

Table 18-15 Generate Signing Requests Step 2

Option	Description
Certificate Subject	Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field is prefixed with “cn=”.
Key Length	Key length entered during generation of this request.Values may be 512, 1024, 2048, or 4096.
Digest to Sign with	This field is populated with the value SHA1 for ACS 5.1.

Step 3 Click **Finish.**

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

Binding CA Signed Certificates

Use this page to bind a CA signed certificate to the request that was used to obtain the certificate from the CA.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **System Administration > Configurations > Local Server Certificates > Certificate Installations > Add** and then select **Bind CA Signed Certificate > Next**.

Step 2 Enter the information in the ACS Import Server Certificate as described in Table 18-16:

Table 18-16 Bind CA Signed Certificate Step 2

Option	Description
Certificate File	Browse to the client machine and select the certificate file to be imported.
Protocol	
EAP	Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP.
Management Interface	Check to associate the certificate with the management interface.
Override Policy	
Replace Certificate	Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections.

Step 3 Click **Finish.**

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

Related Topics

- Configuring Local Server Certificates, page 18-14
- Certificate-Based Network Access for EAP-TLS, page 4-9

Editing and Renewing Certificates

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

You can renew an existing self-signed certificate without having to remove it and adding a new certificate. This ensures that any service that uses the local certificate continues without any interruption. To renew or extend a local server certificate:

Step 1 Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.

Step 2 Click the name that you want to modify; or, check the check box for the Name, and click **Edit**.

Step 3 Enter the certificate properties as described in Table 18-17:

Table 18-17 Edit Certificate Store Properties Page

Option	Description
Issuer	
Friendly Name	The name that is associated with the certificate.
Description	A description of the certificate.
Issued To	*Display only.* The entity to which the certificate is issued. The name that appears is from the certificate subject.
Issued By	*Display only.* The certification authority that issued the certificate.
Valid From	*Display only.* The start date of the certificate's validity. An X509 certificate is valid only from the start date to the end date (inclusive).
Valid To (Expiration)	*Display only.* The last date of the certificate's validity.
Serial Number	*Display only.* The serial number of the certificate.
Protocol	
EAP	Check for ACS to use the local certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP.
Management Interface	Check for ACS to use the local certificate for SSL client authentication.
Renew Self Signed Certificate	
Certificate Expires On	*Display only.* Date the certificate expires.
Renew Self Signed Certificate	Check to allow the renewal of a self signed certificate that expired.
Expiration TTL	Expiration TTL is the number of days, months, weeks, or years that you want to extend the existing certificate for. Valid options are: one day, one month, one week, and one year. **Note** At a maximum, you can extend the certificate for a period of one year.

Step 4 Click **Submit** to extend the existing certificate's validity.

The Local Certificate Store page appears with the edited certificate.

Related Topic

- Configuring Local Server Certificates, page 18-14

Deleting Certificates

To delete a certificate:

Step 1 Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.

Step 2 Check one or more check boxes next to the certificates that you want to delete.

Step 3 Click **Delete**.

Step 4 For confirmation, click **Yes** or **Cancel**.

The Certificate Store page appears without the deleted certificate(s).

Related Topic

- Configuring Local Server Certificates, page 18-14

Exporting Certificates

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To export a certificate:

Step 1 Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.

Step 2 Check the box next to the certificates that you want to export, then click **Export**.

The Export Certificate dialog box appears.

Step 3 Select one of the following options:

- Export Certificate Only
- Export Certificate and Private Key

Step 4 Enter your private key password in the Private Key Password field.

Step 5 Enter the same password in the Confirm Password field.

Note Exporting the private key is not a secure operation and could lead to possible exposure of the private key.

Step 6 Click **OK** or **Cancel**.

Related Topic

- Configuring Local Server Certificates, page 18-14

Viewing Outstanding Signing Requests

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Select **System Administration > Configurations > Local Server Certificates > Outstanding Signing Request**.

The Certificate Signing Request page appears displaying the information described in Table 18-18:

Table 18-18 Certificate Signing Request Page

Option	Description
Name	Name of the certificate.
Certificate Subject	Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field should automatically prefixed with “cn=”.
Key Length	Key length entered during generation of this request.Values may be 512, 1024, 2048, or 4096.
Timestamp	Date certificate was created.
Friendly Name	The name that is associated with the certificate.

Click **Export** to export the local certificate to a client machine.

Configuring Logs

Log records are generated for:

- Accounting messages
- AAA audit and diagnostics messages
- System diagnostics messages
- Administrative and operational audit messages

The messages are arranged in tree hierarchy structure within the logging categories (see Configuring Logging Categories, page 18-25 for more information).

You can store log messages locally or remotely, based on the logging categories and maintenance parameters.

This section contains the following topics:

- Configuring Remote Log Targets, page 18-22
- Configuring the Local Log, page 18-24
- Configuring Logging Categories, page 18-25
- Configuring Global Logging Categories, page 18-25
- Configuring Per-Instance Logging Categories, page 18-30
- Displaying Logging Categories, page 18-33
- Configuring the Log Collector, page 18-33
- Viewing the Log Message Catalog, page 18-34

See Chapter 19, "Understanding Logging" for a description of the preconfigured global ACS logging categories and the messages that each contains.

Configuring Remote Log Targets

You can configure specific remote log targets (on a syslog server only) to receive the logging messages for a specific logging category. See Chapter 19, "Understanding Logging" for more information on remote log targets. See Configuring Logging Categories, page 18-25 for more information on the preconfigured ACS logging categories.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To create a new remote log target:

Step 1 Select **System Administration > Configuration > Log Configuration > Remote Log Targets**.

The Remote Log Targets page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the remote log target that you want to duplicate and click **Duplicate**.
- Click the name of the remote log target that you want to modify; or check the check box next to the name of the remote log target that you want to modify and click **Edit**.

One of these pages appears:

- Remote Log Targets > Create, if you are creating a new remote log target.
- Remote Log Targets > Duplicate: "<*log_target*>", where <*log_target*> is the name of the remote log target you selected in Step 2, if you are duplicating a remote log target.
- Remote Log Targets > Edit: "<*log_target*>", where <*log_target*> is the name of the remote log target you selected in Step 2, if you are modifying a remote log target.

Step 3 Complete the required fields as described in Table 18-19:

Table 18-19 Remote Log Targets Configuration Page

Option	Description
General	
Name	The name of the remote log target. Maximum name length is 32 characters.
Description	The description of the remote log target. Maximum description length is 1024 characters.
Type	The type of remove log target—Syslog (the only option).
Target Configuration	
IP Address	IP address of the remote log target, in the format *x.x.x.x*.
Use Advanced Syslog Options	Click to enable the advanced syslog options—port number, facility code, and maximum length.
Port	The port number of the remote log target used as the communication channel between the ACS and the remote log target (default = 514). This option is only visible if you click Use Syslog Options.
Facility Code	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) This option is only visible if you click Use Advanced Syslog Options.
Maximum Length	The maximum length of the remote log target messages. Valid options are from 200 to 1024. This option is only visible if you click Use Advanced Syslog Options.

Step 4 Click **Submit**.

The remote log target configuration is saved. The Remote Log Targets page appears with the new remote log target configuration.

Related Topic

- Deleting a Remote Log Target, page 18-24

Deleting a Remote Log Target

To delete a remote log target:

Step 1 Select **System Administration > Configuration > Log Configuration > Remote Log Targets**.

The Remote Log Targets page appears, with a list of configured remote log targets.

Step 2 Check one or more check boxes next to the remote log targets you want to delete.

Step 3 Click **Delete**.

The following error message appears:

Are you sure you want to delete the selected item/items?

Step 4 Click **OK**.

The Remote Log Targets page appears without the deleted remote log targets.

Related Topic

- Configuring Remote Log Targets, page 18-22

Configuring the Local Log

Use the Local Configuration page to configure the maximum days to retain your local log data.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **System Administration > Configuration > Log Configuration > Local Log Target**.

The Local Configuration page appears.

Step 2 In the Maximum log retention period box, enter the number of days for which you want to store local log message files, where <*num*> is the number of days you enter. Valid options are 1 to 365. (Default = 7.)

Note If you reduce the number of days for which to store the local log message files, the log message files older than the number of days you specify are deleted automatically.

You can click **Delete Logs Now** to delete the local logs, including all non-active log files, immediately. See Deleting Local Log Data, page 18-25 for more information on deleting log data.

Step 3 Click **Submit** to save your changes. Your configuration is saved and the Local Configuration page is refreshed.

Deleting Local Log Data

Use the Local Configuration page to manually delete your local log data. You can use this option to free up space when the local store is full. See Local Store Target, page 19-5 for more information about the local store.

Step 1 Select **System Administration > Configuration > Log Configuration > Local Log Target**.

The Local Configuration page appears.

Step 2 Click **Delete Logs Now** to immediately delete all local log data files, except the log data in the currently active log data file.

The Local Configuration page is refreshed.

Configuring Logging Categories

This section contains the following topics:

- Configuring Global Logging Categories, page 18-25
- Configuring Per-Instance Logging Categories, page 18-30

All configuration performed for a parent logging category affects the children within the logging category. You can select a child of a parent logging category to configure it separately, and it does not affect the parent logging category or the other children.

Configuring Global Logging Categories

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To view and configure global logging categories:

Step 1 Select **System Administration > Configuration > Log Configuration > Logging Categories > Global**.

The Logging Categories page appears; from here, you can view the logging categories.

Step 2 Click the name of the logging category you want to configure; or, click the radio button next to the name of the logging category you want to configure and click **Edit**.

Step 3 Complete the fields as described in Table 18-20.

Table 18-20 Global: General Page

Option	Descriptions
Configure Log Category	
Log Severity	For diagnostic logging categories, use the drop-down list box to select the severity level. (For audit and accounting categories, there is only one severity, NOTICE, which cannot be modified.) Valid options are: • FATAL—Emergency. ACS is not usable and you must take action immediately. • ERROR—Critical or error condition. • WARN—Normal, but significant condition. (Default) • INFO—Informational message. • DEBUG—Diagnostic bug message.
Configure Local Setting for Category	
Log to Local Target	Check to enable logging to the local target. **Note** For administrative and operational audit logging category types, logging to local target is enabled by default and cannot be disabled.
Local Target is Critical	*Usable for accounting and for AAA audit (passed authentication) logging category types only.* Check the check box to make this local target the critical target. **Note** For administrative and operational audit logging category types, the check box is checked by default and cannot be unchecked; the local target is the critical target.
Configure Logged Attributes	
—	*Display only.* All attributes are logged to the local target.

If you have completed your configuration, proceed to Step 6.

Step 4 To configure a remote syslog target, click the **Remote Syslog Target** and proceed to Step 5.

Step 5 Complete the Remote Syslog Target fields as described in Table 18-21:

Table 18-21 Global: Remote Syslog Target Page

Option	Description
Configure Syslog Targets	
Available targets	List of available targets. You can select a target from this list and move it to the Selected Targets list.
Selected targets	List of selected targets. You can select a target from this list and move it to the Available Targets list to remove it from your configuration.

Step 6 Click **Submit**.

The Logging Categories page appears, with your configured logging category.

Note Administrative and operational audit messages include audit messages of the following types:

- Configuration changes
- Internal user change password
- Administrator access
- Operational audit

  Some of the operational audit messages are not logged in the local log target. See Table 18-22 for a list of administrative and operational logs that are not logged in the local target. See Viewing ADE-OS Logs, page 18-29 for information on how you can view these logs from the ACS CLI.

Table 18-22 lists a set of administrative and operational logs under various categories that are not logged to the local target.

Table 18-22 Administrative and Operational Logs Not Logged in the Local Target

Category	Log and Description
Process-Management	• ACS_START_PROCESS—ACS process started • ACS_STOP_PROCESS—ACS process stopped • ACS_START—All ACS processes started • ACS_STOP—All ACS processes stopped • WD_RESTART_PROCESS—ACS process restarted by watchdog • WD_CONFIG_CHANGE—Watchdog configuration reloaded • ACS_START_STOP_ERROR—ACS process reported start/stop error
DB-Management	• CARS_BACKUP—CARS backup complete • CARS_RESTORE—CARS restore complete • ACS_BACKUP—ACS DB backup complete • ACS_RESTORE—ACS DB restore complete • ACS_SUPPORT—ACS support bundle collected • ACS_RESET—ACS DB reset
File-Management	• ACS_DELETE_CORE—ACS core files deleted • ACS_DELETE_LOG—ACS log files deleted

Table 18-22 Administrative and Operational Logs Not Logged in the Local Target (continued)

Category	Log and Description
Software-Management	• ACS_UPGRADE—ACS upgraded • ACS_PATCH—ACS patch installed • UPGRADE_SCHEMA_CHANGE—ACS schema upgrade complete • UPGRADE_DICTIONARY—ACS dictionary upgrade complete • UPGRADE_DATA_MANIPULATION—ACS upgrade - data manipulation stage complete • UPGRADE_AAC—ACS AAC upgrade complete • UPGRADE_PKI—ACS PKI upgrade complete • UPGRADE_VIEW—ACS View upgrade complete • CLI_ACS_UPGRADE—ACS upgrade started • CLI_ACS_INSTALL—ACS install started
System-Management	• ACS_MIGRATION_INTERFACE—ACS migration interface enabled/disabled • ACS_ADMIN_PSWD_RESET—ACS administrator password reset • CLI_CLOCK_SET—Clock set • CLI_TZ_SET—Time zone set • CLI_NTP_SET—NTP Server set • CLI_HOSTNAME_SET—Hostname set • CLI_IPADDRESS_SET—IP address set • CLI_IPADDRESS_STATE—IP address state • CLI_DEFAULT_GATEWAY—Default gateway set • CLI_NAME_SERVER—Name server set • ADEOS_XFER_LIBERROR—ADE OS Xfer library error • ADEOS_INSTALL_LIBERROR—ADE OS install library error • AD_JOIN_ERROR—AD agent failed to join AD domain • AD_JOIN_DOMAIN—AD agent joined AD domain • AD_LEAVE_DOMAIN—AD agent left AD domain • IMPORT_EXPORT_PROCESS_ABORTED—Import/Export process aborted • IMPORT_EXPORT_PROCESS_STARTED—Import/Export process started • IMPORT_EXPORT_PROCESS_COMPLETED—Import/Export process completed • IMPORT_EXPORT_PROCESS_ERROR—Error while Import/Export process

Related Topic

- Configuring Per-Instance Logging Categories, page 18-30
- Viewing ADE-OS Logs, page 18-29

Viewing ADE-OS Logs

The logs listed in Table 18-22 are written to the ADE-OS logs. From the ACS CLI, you can use the following command to view the ADE-OS logs:

show logging system

This command lists all the ADE-OS logs and your output would be similar to the following example.

```
Sep 29 23:24:15 cd-acs5-13-179 sshd(pam_unix)[20013]: 1 more authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95
user=admin
Sep 29 23:24:34 cd-acs5-13-179 sshd(pam_unix)[20017]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 29 23:24:36 cd-acs5-13-179 sshd[20017]: Failed password for admin from 10.77.137.95
port 3635 ssh2
Sep 30 00:47:44 cd-acs5-13-179 sshd(pam_unix)[20946]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 30 00:47:46 cd-acs5-13-179 sshd[20946]: Failed password for admin from 10.77.137.95
port 3953 ssh2
Sep 30 00:54:59 cd-acs5-13-179 sshd(pam_unix)[21028]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=ad
min
Sep 30 00:55:01 cd-acs5-13-179 sshd[21028]: Failed password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:35 cd-acs5-13-179 last message repeated 5 times
Sep 30 00:55:39 cd-acs5-13-179 sshd[21028]: Accepted password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:39 cd-acs5-13-179 sshd(pam_unix)[21038]: session opened for user admin by
(uid=0)
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[118] [admin]:
Invoked carsGetConsoleConfig
Sep 30 00:55:40 cd-acs5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[135] [admin]:
No Config file, returning defaults
Sep 30 01:22:20 cd-acs5-13-179 sshd[21038]: Received disconnect from 10.77.137.95: 11:
Connection discarded by broker
Sep 30 01:22:20 cd-acs5-13-179 sshd(pam_unix)[21038]: session closed for user admin
Sep 30 01:22:22 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 01:22:22 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 02:48:54 cd-acs5-13-179 sshd[22500]: Accepted password for admin from 10.77.137.58
port 4527 ssh2
Sep 30 02:48:54 cd-acs5-13-179 sshd(pam_unix)[22504]: session opened for user admin by
(uid=0)
Sep 30 02:48:55 cd-acs5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 02:48:55 cd-acs5-13-179 debugd[2597]: successfully loaded debug config
```

You can view the logs grouped by the module that they belong to. For example, the monitoring and troubleshooting logs contain the string **MSGCAT** and the debug logs contain the string **debug**.

From the ACS CLI, you can enter the following two commands to view the monitoring and troubleshooting logs and the administrative logs respectively:

- **show logging system | include MSGCAT**
- **show logging system | include debug**

The output of the **show logging system | include MSGCAT** would be similar to:

```
Sep 27 13:00:02 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 28 13:00:03 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 06:28:17 cd-acs5-13-103 MSGCAT58007: Killing Tomcat 8363
```

```
Sep 29 06:28:28 cd-acs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 06:31:41 cd-acs5-13-103 MSGCAT58037/admin: Installing ACS
Sep 29 09:52:35 cd-acs5-13-103 MSGCAT58007: Killing Tomcat 32729
Sep 29 09:52:46 cd-acs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 09:53:29 cd-acs5-13-103 MSGCAT58004/admin: ACS Starting
Sep 29 10:37:45 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 29 13:00:02 cd-acs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 13:56:36 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:02 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:25 cd-acs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 30 10:57:10 cd-acs5-13-103 MSGCAT58010/admin: info:[ACS backup] ACS backup completed
```

For more information on the **show logging** command, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/command/reference/cli_app_a.html#wp1748398.

Configuring Per-Instance Logging Categories

You can define a custom logging category configuration for specific, overridden ACS instances, or return all instances to the default global logging category configuration.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To view and configure per-instance logging categories:

Step 1 Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**.

The Per-Instance page appears; from here, you can view the individual ACS instances of your deployment.

Step 2 Click the radio button associated with the name of the ACS instance you want to configure, and choose one of these options:

- Click **Override** to override the current logging category configuration for selected ACS instances.
- Click **Configure** to display the Logging Categories page associated with the ACS instance. You can then edit the logging categories for the ACS instance. See Displaying Logging Categories, page 18-33 for field descriptions.
- Click **Restore to Global** to restore selected ACS instances to the default global logging category configuration.

Your configuration is saved and the Per-Instance page is refreshed.

Related Topic

- Configuring Per-Instance Security and Log Settings, page 18-31

Configuring Per-Instance Security and Log Settings

You can configure the severity level and local log settings in a logging category configuration for a specific overridden or custom ACS instance. Use this page to:

- View a tree of configured logging categories for a specific ACS instance.
- Open a page to configure a logging category's severity level, log target, and logged attributes for a specific ACS instance.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.

The Per-Instance: Configuration page appears as described in Table 18-23:

Table 18-23 Per-Instance: Configuration Page

Option	Description
Name	Expandable tree structure of AAA service logging categories.
Edit	Click to display a selected Logging Categories > Edit: "<*lc_name*>" page, where <*lc_name*> is the name of the logging category.

Step 2 Perform one of the following:

- Click the name of the logging category you want to configure.
- Select the radio button associated with the name of the logging category you want to configure, and click **Edit**.

The Per-Instance: General page appears; from here, you can configure the security level and local log settings in a logging category configuration for a specific ACS instance. See Table 18-24:

Table 18-24 Per-Instance: General Page

Option	Description
Configure Log Category	
Log Severity	Use the list box to select the severity level for diagnostic logging categories. (For audit and accounting categories, there is only one severity, NOTICE, which cannot be modified.) Valid options are: • FATAL—Emergency. The ACS is not usable and you must take action immediately. • ERROR—Critical or error condition. • WARN—Normal, but significant condition. (Default) • INFO—Informational message. • DEBUG—Diagnostic bug message.
Configure Local Setting for Category	
Log to Local Target	Check to enable logging to the local target. **Note** For administrative and operational audit logging category types, logging to local target is enabled by default and cannot be disabled.
Local Target is Critical	*Usable for accounting and for passed authentication logging category types only.* Check the check box to make this local target the critical target. **Note** For administrative and operational audit logging category types, the check box is checked by default and cannot be unchecked; the local target is the critical target. If you make local target as the critical target and the logging operation fails, authentication request will be rejected and accounting response will not be sent to the device.
Configure Logged Attributes	
—	*Display only.* All attributes are logged to the local target.

Configuring Per-Instance Remote Syslog Targets

Use this page to configure remote syslog targets for logging categories.

Step 1 Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.

The Per-Instance: Configuration page appears as described in Table 18-23.

Step 2 Perform one of the following actions:

- Click the name of the logging category you want to configure.
- Select the radio button associated with the name of the logging category you want to configure, and click **Edit**.

Step 3 Click the **Remote Syslog Target** tab. The Per-Instance: Remote Syslog Targets page appears as described in Table 18-25:

Table 18-25 Per-Instance: Remote Syslog Targets Page

Option	Description
Configure Syslog Targets	
Available targets	A list of available targets. You can select a target from this list and move it to the Selected Targets list.
Selected targets	A list of selected targets. You can select a target from this list and move it to the Available Targets list to remove it from your configuration.

Displaying Logging Categories

You can view a tree of configured logging categories for a specific ACS instance. In addition, you can configure a logging category's severity level, log target, and logged attributes for a specific ACS instance.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.

Step 2 Complete the fields as described in Table 18-26:

Table 18-26 Per-Instance: Configuration Page

Option	Description
Name	Expandable tree structure of AAA services logging categories.
Edit	Click to display a selected Logging Categories > Edit: "<*lc_name*>" page, where <*lc_name*> is the name of the logging category.

Configuring the Log Collector

Use the Log Collector page to select a log data collector and suspend or resume log data transmission.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Step 1 Select **System Administration > Configuration > Log Configuration > Log Collector**.

The Log Collector page appears.

Step 2 Complete the Log Collector fields as described in Table 18-27:

Table 18-27 Log Collector Page

Option	Description
Log Data Collector	
Current Log Collector	*Display only.* Identifies the machine on which the local log messages are sent.
Select Log Collector	Use the drop-down list box to select the machine on which you want local log messages sent.
Set Log Collector	Click to configure the log collector according to the selection you make in the Select Log Collector option.

Step 3 (Optional) Do one of the following:

- Click **Suspend** to suspend the log data transmission to the configured log collector.
- Click **Resume** to resume the log data transmission to the configured log collector.

Your configuration is saved and the Log Collector page is refreshed.

Viewing the Log Message Catalog

Use the Log Message Catalog page to view all possible log messages.

Select **System Administration > Configuration > Log Configuration > Log Message Catalog**.

The Log Message Catalog page appears, with the fields described in Table 18-28, from which you can view all possible log messages that can appear in your log files.

Table 18-28 Log Messages Page

Option	Description
Message Code	*Display only.* A unique message code identification number associated with a message.
Severity	*Display only.* The severity level associated with a message.
Category	*Display only.* The logging category to which a message belongs.
Message Class	*Display only.* The group to which a message belongs.
Message Text	*Display only.* English language message text (name of the message).
Description	Display only. English language text that describes the associated message.

Licensing Overview

To operate ACS, you must install a valid license. ACS prompts you to install a valid base license when you first access the web interface. Each ACS instance (primary or secondary) in a distributed deployment requires a unique base license.

Note Each server requires a unique base license in a distributed deployment.

Types of Licenses

Table 18-29 shows the ACS 5.1 license support:

Table 18-29 ACS License Support

License	Description
Base License	The base license is required for all software instances deployed, as well as for all appliances. The base license enables you to use all the ACS functionality except license controlled features, and it enables all reporting features. Base license is: • Required for each ACS instance, primary and secondary. • Required for all appliances. • Supports deployments with up to 500 managed devices. Base licenses are of two types: • Permanent—Supports up to 500 devices. • Eval—Supports up to 50 devices and expires in 90 days. **Note** The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256. If your evaluation license expires or is about to expire, you cannot use another evaluation license or extend your current license. Before your evaluation license expires, you must upgrade to a Permanent license.
Add-on Licenses	Supports an unlimited number of managed devices. Requires an existing ACS permanent base license. There are also evaluation-type licenses for add-on licenses. The TrustSec feature licenses are of two types: Permanent, and Eval. However, the permanent TrustSec feature license can be used only with a permanent base license. Also, the large deployment license can only be used only with a permanent base license.
Evaluation License (standard)	Enables standard centralized reporting features. • Cannot be reused on the same platform. • You can only install one evaluation license per platform. You cannot install additional evaluation licenses. • Supports 50 managed devices. • Expires 90 days from the time the license is installed.

Related Topics

- Licensing Overview, page 18-35
- Installing a License File, page 18-36
- Viewing the Base License, page 18-36
- Adding Deployment License Files, page 18-40
- Deleting Deployment License Files, page 18-41

Installing a License File

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

You can obtain a valid license file using the Product Activation Key (PAK) supplied with the product. To install a license file:

Step 1 Log in to the ACS web interface.

The Initial Licenses page appears when you log in to the ACS machine for the first time.

Step 2 Click **Cisco Secure ACS License Registration.** This link directs you to Cisco.com to purchase a valid license file from a Cisco representative.

Step 3 Click **Install** to install the license file that you purchased.

The ACS web interface log in page reappears. You can now work with the ACS application.

Note You cannot upgrade a base permanent license. You can only upgrade a base evaluation license.

Related Topics

- Licensing Overview, page 18-35
- Viewing the Base License, page 18-36
- Adding Deployment License Files, page 18-40
- Deleting Deployment License Files, page 18-41

Viewing the Base License

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To upgrade the base license:

Step 1 Select **System Administration > Configuration > Licensing > Base Server License**.

The Base Server License page appears with a description of the ACS deployment configuration and a list of the available deployment licenses. See Types of Licenses for a list of deployment licenses.

Table 18-30 describes the fields in the Base Server License page.

Table 18-30 Base Server License Page

Option	Description
ACS Deployment Configuration	
Primary ACS Instance	The name of the primary instance created when you logged into the ACS 5.1 web interface.
Number of Instances	The current number of ACS instances (primary or secondary) in the ACS database.
Current Number of Configured IP Addresses in Network Devices	The total number of IP addresses in all the subnetworks that you have configured as part of network device configuration. **Note** The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.
Maximum Number of IP Addresses in Network Devices	The maximum number of IP addresses that your license supports: • Base License—Supports 500 IP addresses. **Note** The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256. • Evaluation License—Supports 50 IP addresses. • Large Deployment—Supports an unlimited number of IP addresses.
Use this link to obtain a valid License File	Directs you to Cisco.com to generate a valid license file using the Product Activation Key (PAK)
Base License Configuration	
ACS Instance	The name of the ACS instance, either primary or secondary.
Identifier	The name of the base license.
License Type	Specifies the base license type (permanent, evaluation).
Expiration	Specifies the expiration date for evaluation licenses. For permanent licenses, the expiration field indicates *permanent*.
Licensed to	The name of the company that this product is licensed to.
PAK	The name of the Product Activation Key (PAK) received from Cisco.
Version	The current version of the ACS software.

Step 2 You can select one or more radio buttons next to the instance whose license you want to upgrade. Click **Upgrade**. See Upgrading the Base Server License, page 18-38 for valid field options.

Related Topic

- Upgrading the Base Server License, page 18-38

Upgrading the Base Server License

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

You can upgrade the base server license.

Step 1 Select **System Administration > Configuration > Licensing > Base Server License**.

The Base Server License page appears with a description of the ACS deployment configuration and a list of the available deployment licenses. See Types of Licenses for a list of deployment licenses.

Step 2 Select a license, then click **Upgrade**.

The Base Server License Edit page appears.

Step 3 Complete the fields as described in Table 18-31:

Table 18-31 Base Server License Edit Page

Option	Description
ACS Instance License Configuration	
Version	Displays the current version of the ACS software.
ACS Instance	Displays the name of the ACS instance, either primary or secondary.
License Type	Specifies the license type.
Use this link to obtain a valid License File	Directs you to Cisco.com to purchase a valid license file from a Cisco representative.
License Location	
License File	Click **Browse** to navigate to the directory that contains the license file and select it.

Step 4 Click **Submit**.

Related Topics

- Licensing Overview, page 18-35
- Types of Licenses, page 18-35
- Installing a License File, page 18-36
- Adding Deployment License Files, page 18-40
- Deleting Deployment License Files, page 18-41

Viewing License Feature Options

You can add, upgrade, or delete existing deployment licenses. The configuration pane at the top of the page shows the deployment information.

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

Select **System Administration > Configuration > Licensing > Feature Options**.

The Feature Options Page appears as described in Table 18-32:

Table 18-32 Feature Options Page

Option	Description
ACS Deployment Configuration	
Primary ACS Instance	The name of the primary instance created when you login into the ACS 5.1 web interface.
Number of Instances	The current number of ACS instances (primary or secondary) in the ACS database.
Current Number of Configured IP Addresses in Network Devices	The total number of IP addresses in all the subnetworks that you have configured as part of network device configuration. **Note** The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.
Maximum Number of IP Addresses in Network Devices	The maximum number of IP addresses that your license supports: • Base License—Supports 500 IP addresses. **Note** The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256. • Evaluation License—Supports 50 IP addresses. • Large Deployment—Supports an unlimited number of IP addresses.
Use this link to obtain a valid License File	Directs you to Cisco.com to purchase a valid license file from a Cisco representative.
Installed Deployment License Options	
Feature	• Large Deployment—Supports an unlimited number of managed devices. • TrustSec Access Control—Enables Cisco Trusted Server (CTS) management functionality. This requires an existing ACS base license.
Licensed to	The name of the company that this product is licensed to.
License Type	Specifies the license type (permanent, evaluation).
Expiration	The expiration date for the following features: • Large Deployment • CTS

Table 18-32 Feature Options Page (continued)

Option	Description
Add/Upgrade	Click **Add/Upgrade** to access the Viewing License Feature Options and add a license file.
Delete	Select the radio button next to the license feature you wish to delete and click **Delete**.

Adding Deployment License Files

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To add a new base deployment license file:

Step 1 Select **System Administration > Configuration > Licensing > Feature Options**.

The Feature Options page appears with a description of the ACS deployment configuration and a list of the available deployment licenses and their configurations. See Add-on Licenses in Types of Licenses for a list of deployment licenses. See Viewing License Feature Options, page 18-39 for field descriptions.

Step 2 Click **Add.**

The Feature Options Create page appears.

Step 3 Complete the fields as described in Table 18-33 to add a license:

Table 18-33 Feature Options Create Page

Option	Description
ACS Deployment Configuration	
Primary ACS Instance	The name of the primary instance created when you login into the ACS 5.1 web interface.
Number of Instances	The current number of ACS instances (primary or secondary) in the ACS database.
Current Number of Configured IP Addresses in Network Devices	The total number of IP addresses in all the subnetworks that you have configured as part of network device configuration. **Note** The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.

Table 18-33 Feature Options Create Page (continued)

Option	Description
Maximum Number of IP Addresses in Network Devices	The maximum number of IP addresses that your license supports: • Base License—Supports 500 IP addresses. **Note** The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256. • Evaluation License—Supports 50 IP addresses. • Large Deployment—Supports an unlimited number of IP addresses.
Use this link to obtain a valid License File	Directs you to Cisco.com to purchase a valid license file from a Cisco representative.
License Location	
License File	• Click **Browse** to browse to the location of the purchased license file you wish to install and select it.

Step 4 Click **Submit** to download the license file.

The Feature Options page appears with the additional license.

Related Topics

- Licensing Overview, page 18-35
- Types of Licenses, page 18-35
- Installing a License File, page 18-36
- Viewing the Base License, page 18-36
- Deleting Deployment License Files, page 18-41

Deleting Deployment License Files

Note Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. See Configuring System Administrators and Accounts, page 16-3 to configure the appropriate administrator privileges.

To delete deployment license files:

Step 1 Select **System Administration > Configuration > Licensing > Feature Options**.

The Feature Options page appears with a description of the ACS deployment configuration and a list of the available deployment licenses and their configurations. See Add-on Licenses in Types of Licenses for a list of deployment licenses. See the Table 18-32 for field descriptions.

Step 2 Select the radio button next to the deployment you wish to delete.

Step 3 Click **Delete to delete the license file.**

Related Topics

- Licensing Overview, page 18-35
- Types of Licenses, page 18-35
- Installing a License File, page 18-36
- Viewing the Base License, page 18-36
- Adding Deployment License Files, page 18-40

Available Downloads

This section contains information about the utilities and files that are available for download from the ACS web interface:

- Downloading Migration Utility Files, page 18-42
- Downloading UCP WSDL Files, page 18-42
- Downloading Sample Python Scripts, page 18-43

Downloading Migration Utility Files

To download migration application files and the migration guide for ACS 5.1:

Step 1 Choose **System Administration > Downloads > Migration Utility**.

The Migration from 4.x page appears.

Step 2 Click **Migration application files**, to download the application file you want to use to run the migration utility.

Step 3 Click **Migration Guide**, to download *Migration Guide for the Cisco Secure Access Control System 5.1*.

Downloading UCP WSDL Files

You can download the WSDL file from this page to integrate ACS with your in-house portals and allow ACS users configured in the ACS internal identity store to change their own passwords. The UCP web service allows only the users to change their passwords. They can do so on the primary or secondary ACS servers.

The UCP web service compares the new password that you provide with the password policy that is configured in ACS for users. If the new password conforms to the defined criteria, your new password takes effect. After your password is changed on the primary ACS server, ACS replicates it to all the secondary ACS servers.

To download the UCP WSDL Files:

Step 1 Choose **System Administration > Downloads > User Change Password**.

The User Change Password (UCP) web service page appears.

Step 2 Click one of the following:

- **UCP WSDL** to download the WSDL file.
- **Python Script for Using the User Change Password Web Service** to download a sample Python script.

For more information on how to use the UCP web service, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/ucp.html.

Downloading Sample Python Scripts

The Scripts page contains sample Python scripts for:

- Using the UCP web service.
- Automating the bulk import and export operations.

To download these sample scripts:

Step 1 Choose **System Administration > Downloads > Sample Python Scripts**.

The Sample Python Scripts page appears.

Step 2 Click one of the following:

- **Python Script for Using the User Change Password Web Service**—To download the sample script for the UCP web service.
- **Python Script for Performing CRUD Operations on ACS Objects**—To download the sample script for the import and export process.

Step 3 Save the script to your local hard drive.

The scripts come with installation instructions. For more information on how to use the scripts, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/sdk/sdkguide.html.

Note The Cisco Technical Assistance Center (TAC) supports only the default Python Script. TAC does not offer any support for modified scripts.

CHAPTER 19

Understanding Logging

This chapter describes logging functionality in ACS 5.1. Administrators and users use the various management interfaces of ACS to perform different tasks. Using the administrative access control feature, you can assign permissions to administrators and users to perform different tasks. Apart from this, you also need an option to track the various actions performed by the administrators and users. ACS offers you several logs that you can use to track these actions and events.

This chapter contains the following sections:

- About Logging, page 19-1
- ACS 4.x Versus ACS 5.1 Logging, page 19-11

About Logging

You can gather the following logs in ACS:

- Customer Logs—For auditing and troubleshooting your ACS, including logs that record daily operations, such as accounting, auditing, and system-level diagnostics.
- Debug logs—Low-level text messages that you can export to Cisco technical support for evaluation and troubleshooting. You configure ACS debug logs via the command line interface. Specifically, you enable and configure severity levels of the ACS debug logs using the command line interface. See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.0* for more information.
- Platform logs—Log files generated by the ACS appliance operating system.

Debug and platform logs are stored locally on each ACS server. Customer logs can be viewed centrally for all servers in a deployment.

You can use the following ACS interfaces for logging:

- Web interface—This is the primary logging interface. You can configure which messages to log and to where you want the messages logged.
- Command line interface (CLI)—Allows you to display and download logs, debug logs, and debug backup logs to the local target. The CLI also allows you to display and download platform logs. See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.0* for more information.

Using Log Targets

You can specify to send customer log information to multiple consumers or *Log Targets* and specify whether the log messages are stored locally in text format or forwarded to syslog servers. By default, a single predefined local Log Target called *Local Store* stores data in text format on an ACS server and contains log messages from the local ACS server only. You can view records stored in the Local Store from the CLI.

In addition, you can specify that logs be forwarded to a syslog server. ACS uses syslog transport to forward logs to the Monitoring and Reports component. You can also define additional syslog servers to receive ACS log messages. For each additional syslog server you specify, you must define a remote log target.

In a distributed deployment, you should designate one of the secondary ACS servers as the Monitoring and Reports server, and specify that it receive the logs from all servers in the deployment. By default, a Log Target called the *LogCollector* identifies the Monitoring and Reports server. In cases where a distributed deployment is used, the Log Collector option on the web interface designates which server collects the log information. It is recommended that you designate a secondary server within the deployment to act as the Monitoring and Reports server.

This section contains the following topics:

- Logging Categories, page 19-2
- Log Message Severity Levels, page 19-4
- Local Store Target, page 19-5
- Viewing Log Messages, page 19-10
- Debug Logs, page 19-11

Logging Categories

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.

A logging category is a bundle of message codes which describe a function of ACS, a flow, or a use case. The categories are arranged in a hierarchical structure and used for logging configuration. Each category has:

- Name—A descriptive name
- Type—Audit, Accounting, or Diagnostics
- Attribute list—A list of attributes that may be logged with messages associated with a category, if applicable

ACS provides these preconfigured global ACS logging categories, to which you can assign log targets (see Local Store Target, page 19-5):

- Administrative and Operational audit, which can include:
  - ACS configuration changes—Logs all configuration changes made to ACS. When an in item is added or edited, the configuration change events also include details of the attributes that were changed and their new values. If an edit request resulted in no attributes having new values, no configuration audit record is created.

Note For complex configuration items or attributes, such as policy or DACL contents, the new attribute value is reported as "New/Updated" and the audit does not contain the actual attribute value or values.

  - ACS administrator access—Logs all events that occur when an administrators accesses the system until the administrator logs out. It logs whether the administrator exits ACS with an explicit request or if the session has timed out. This log also includes login attempts that fail due to account inactivity. Login failures along with failure reasons are logged.
  - ACS operational changes—Logs all operations requested by administrators, including promoting an ACS from your deployment as the primary, requesting a full replication, performing software downloads, doing a backup or restore, generating and restoring PACs, and so on.
  - Internal user password change—Logs all changes made to internal user passwords across all management interfaces.

  In addition, the administrative and operational audit messages must be logged to the local store. You can optionally log these messages to remote logging targets (see Local Store Target, page 19-5).

- AAA audit, which can include RADIUS and TACACS+ successful or failed authentications, command-access passed or failed authentications, password changes, and RADIUS request responses.
- AAA diagnostics, which can include authentication, authorization, and accounting information for RADIUS and TACACS+ diagnostic requests and RADIUS attributes requests, and identity store and authentication flow information. Logging these messages is optional.
- System diagnostic, which can include system startup and system shutdown, and logging-related diagnostic messages:
  - Administration diagnostic messages related to the CLI and web interface
  - External server-related messages
  - Local database messages
  - Local services messages
  - Certificate related messages

  Logging these messages is optional.
- System statistics, which contains information on system performance and resource utilization. It includes data such as CPU and memory usage and process health and latency for handling requests.
- Accounting, which can contain TACACS+ network access session start, stop, and update messages, as well as messages that are related to command accounting. In addition, you can log these messages to the local store. Logging these messages is optional.

The log messages can be contained in the logging categories as described in this topic, or they can be contained in the logging subcategories. You can configure each logging subcategory separately, and its configuration does not affect the parent category.

In the ACS web interface, choose **System Administration > Configuration > Logging Categories > Global** to view the hierarchical structure of the logging categories and subcategories. In the web interface, choose **Monitoring and Reports > Catalog** to run reports based on your configured logging categories.

Each log message contains the following information:

- Event code—A unique message code.

- Logging category—Identifies the category to which a log message belongs.
- Severity level—Identifies the level of severity for diagnostics. See Log Message Severity Levels, page 19-4 for more information.
- Message class—Identifies groups of messages of similar context, for example, RADIUS, policy, or EAP-related context.
- Message text—Brief English language explanatory text.
- Description—English language text that describes log message reasons, troubleshooting information (if applicable), and external links for more information.
- Failure reason (optional)—Indicates whether a log message is associated with a failure reason.

Passwords are not logged, encrypted or not.

Global and Per-Instance Logging Categories

By default, a single log category configuration applies to all servers in a deployment. For each log category, the threshold severity of messages to be logged, whether messages are to be logged to the local target, and the remote syslog targets to which the messages are to be sent to, are defined. The log categories are organized in a hierarchical structure so that any configuration changes you make to a parent category are applied to all the child categories.

However, the administrator can apply different configurations to the individual servers in a deployment. For example, you can apply more intensive diagnostic logging on one server in the deployment. The per-instance logging category configuration displays all servers in a deployment and indicates whether they are configured to utilize the global logging configuration or have their own *custom* configuration. To define a custom configuration for a server, you must first select the *Override* option, and then configure the specific log category definitions for that server.

You can use the Log Message Catalog to display all possible log messages that can be generated, each with its corresponding category and severity. This information can be useful when configuring the logging category definitions.

Log Message Severity Levels

You can configure logs of a certain severity level, and higher, to be logged for a specific logging category and add this as a configuration element to further limit or expand the number of messages that you want to save, view, and export. For example, if you configure logs of severity level WARNING to be logged for a specific logging category, log messages for that logging category of severity level WARNING and those of a higher priority levels (ERROR and FATAL) are sent to any configured locations. Table 19-1 describes the severity levels and their associated priority levels.

Table 19-1 Log Message Severity Levels

ACS Severity Level	Description	Syslog Severity Level
FATAL	Emergency. ACS is not usable and you must take action immediately.	1 (highest)
ERROR	Critical or error conditions.	3
WARN	Normal, but significant condition.	4

Table 19-1 Log Message Severity Levels (continued)

ACS Severity Level	Description	Syslog Severity Level
NOTICE	Audit and accounting messages. Messages of severity NOTICE are always sent to the configured log targets and are not filtered, regardless of the specified severity threshold.	5
INFO	Diagnostic informational message.	6
DEBUG	Diagnostic message.	7

Local Store Target

Log messages in the local store are text files that are sent to one log file, located at */opt/CSCOacs/logs/localStore/*, regardless of which logging category they belong to. The local store can only contain log messages from the local ACS node; the local store cannot accept log messages from other ACS nodes. You can configure which logs are sent to the local store, but you cannot configure which attributes are sent with the log messages; *all* attributes are sent with sent log messages.

Administrative and operational audit log messages are always sent to the local store, and you can also send them to remote syslog server and Monitoring and Reports server targets.

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 19-2 describes the content of the local store syslog message format.

Table 19-2 Local Store and Syslog Message Format

Field	Description
<timestamp>	The date of the message generation, according to the local clock of the originating ACS, in the format <YYY- MM-DD hh:mm:ss:xxx +/-zh:zm>. Possible values are: • YYYY = Numeric representation of the year. • MM = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number. • DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number. • hh = The hour of the day—00 to 23. • mm = The minute of the hour—00 to 59. • ss = The second of the minute—00 to 59. • xxx = The millisecond of the second—000 to 999. • +/-zz:zz = The time zone offset from the ACS server's time zone, where zh is the number of offset hours and zm 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 an ACS node that is two hours ahead of the ACS server's time zone.
<sequence_num>	The 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.
<msg_code>	The message code as defined in the logging categories.
<msg_sev>	The message severity level of a log message (see Table 19-1).
<msg_class>	The message class, which identifies groups of messages with the same context.
<text_msg>	English language descriptive text message.
<attr=value>	A set of attribute-value pairs that provides details about the logged event. A comma (,) separates each pair. Attribute names are as defined in the ACS 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: Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=cts:security-group-tag=0000-00; }

You can use the web interface to configure the number of days to retain local store log files; however, the default setting is to purge data when it exceeds 5 MB or each day, whichever limit is first attained. If you do configure more than one day to retain local store files and the data size of the combined files

reaches 95000Mb, a FATAL message is sent to the system diagnostic log, and all logging to the local store is stopped until data is purged. Use the web interface to purge local store log files. Purging actions are logged to the current, active log file. See Deleting Local Log Data, page 18-25.

The current log file is named *acsLocalStore.log*. Older log files are named in the format *acsLocalStore.log.YYYY-MM-DD-hh-mm-ss-xxx*, where:

- acsLocalStore.log = The prefix of a non-active local store log file, appended with the time stamp.

Note The time stamp is added when the file is first created, and should match the time stamp of the first log message in the file.

  - YYYY = Numeric representation of the year.
  - MM = Numeric representation of the month. For single-digit months (1 to 9), a zero precedes the number.
  - DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number.
  - hh = Hour of the day—00 to 23.
  - mm = Minute of the hour—00 to 59.
  - ss = Second of the minute—00 to 59.
  - xxx = Millisecond of the second—000 to 999.

You can configure the local store to be a critical log target. See Viewing Log Messages, page 19-10 for more information on critical log targets.

You can send log messages to the local log target (local store) or to up to eight remote log targets (on a remote syslog server):

- Select **System Administration > Configuration > Log Configuration > Remote Log Targets** to configure remote log targets.
- Select **System Administration > Configuration > Log Configuration > Logging Categories** to configure which log messages you want to send to which targets.

Critical Log Target

The local store target can function as a critical log target—the primary, or mandatory, log target for a logging category. For example, administrative and operational audit messages are always logged to the local store, but you can also configure them to be logged to a remote syslog server or the Monitoring and Reports server log target. However, administrative and operational audit messages configured to be additionally logged to a remote log target are only logged to that remote log target if they are first logged successfully to the local log target.

When you configure a critical log target, and a message is sent to that critical log target, the message is also sent to the configured noncritical log target on a best-effort basis. When you configure a critical log target, and a message does not log to that critical log target, the message is also not sent to the configured noncritical log. When you do not configure a critical log target, a message is sent to a configured noncritical log target on a best-effort basis.

Select **System Administration > Configuration > Log Configuration > Logging Categories > Global > *<log_category>***, where <log_category> is a specific logging category to configure the critical log target for the logging categories.

Note Critical logging is applicable for accounting and AAA audit (passed authentications) categories only. You cannot configure critical logging for the following categories: AAA diagnostics, system diagnostics, and system statistics.

Remote Syslog Server Target

You can use the web interface to configure logging category messages so that they are sent to remote syslog server targets. Log messages are sent to the remote syslog server targets in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP.

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 19-2):

<pri_num> <YYYY Mmm DD hh:mm:ss> <xx:xx:xx:xx/host_name> <cat_name> <msg_id> <total_seg> <seg_num>

Table 19-3 describes the content of the remote syslog message header format.

Table 19-3 Remote Syslog Message Header Format

Field	Description
<pri_num>	The 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 Table 19-1 for severity values.
<time>	The date of the message generation, according to the local clock of the originating ACS, in the format <YYYY Mmm DD hh:mm:ss>. Possible values are: • YYYY = Numeric representation of the year. • Mmm = Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number. • hh = The hour of the day—00 to 23. • mm = The minute of the hour—00 to 59. • ss = The second of the minute—00 to 59. **Note** Some device send messages that specify a time zone in the format -/+hhmm, where - and + identifies the directional offset from the ACS 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 an ACS node that is two hours ahead of the ACS server's time zone.
<xx:xx:xx:xx/host_name>	The IP address of the originating ACS, or the hostname.
<cat_name>	The logging category name preceded by the `CSCOacs` string.
<msg_id>	The 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.
<total_seg>	Total number of segments in a log message. Long messages are divided into more than one segment.
<seg_num>	The segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

The syslog message data or payload is the same as the Local Store Message Format, which is described in Table 19-2.

The remote syslog server targets are identified by the facility code names *LOCAL0* to *LOCAL7* (*LOCAL6* is the default logging location.) Log messages that you assign to the remote syslog server are sent to the default location for Linux syslog (*/var/log/messages*), however; you can configure a different location on the server.

The remote syslog server cannot function as a critical log target. See Critical Log Target, page 19-7 for more information on critical log targets.

Monitoring and Reports Server Target

You can use the web interface to configure logging category messages so that they are sent to the Monitoring and Reports server target. Log messages are sent to the Monitoring and Reports server target in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP protocol.

Log messages are sent to the Monitoring and Reports server with the syslog message header format described in Table 19-3, which precedes the local store syslog message format (see Table 19-2).

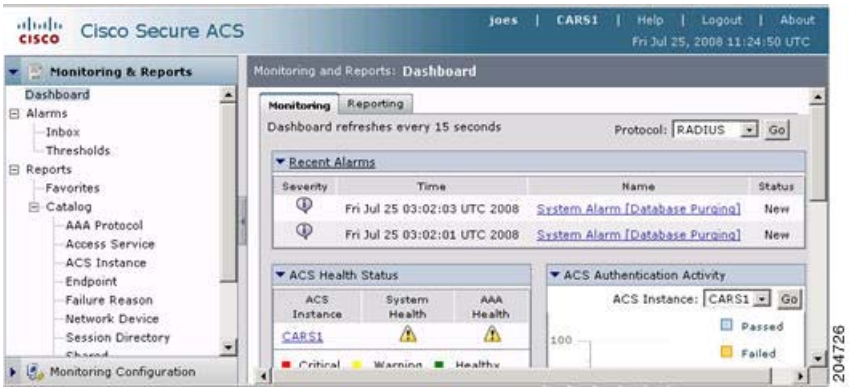
The Monitoring and Reports server cannot function as a critical log target. See Critical Log Target, page 19-7 for more information on critical log targets.

Viewing Log Messages

You can use the web interface and the CLI to view locally stored log messages. You cannot view log messages that are sent to remote syslog servers via the web interface or the CLI.

In the web interface, choose **Monitoring and Reports > Launch Monitoring & Report Viewer** to open the Monitoring and Reports Viewer in a secondary window (see Figure 19-1). See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.0* for more information about viewing log messages via the CLI.

Figure 19-1 Monitoring and Reports Viewer



The Monitoring & Report Viewer has two drawer options:

- Monitoring and Reports—Use this drawer to view and configure alarms, view log reports, and perform troubleshooting tasks.

- Monitoring Configuration—Use this drawer to view and configure logging operations and system settings.

In addition to the information that is captured in the log messages described in Logging Categories, page 19-2, the Viewer reports list successful and failed AAA authentication attempts with Step attributes. Step attributes provide information about other events that occurred within the same session. This information allows you to see the sequence of steps that resulted in an authentication success or failure.

You can use the Viewer to:

- Manage alarms, reports, and troubleshooting information.
- Manage system operations, including purging data, collecting logs, scheduling jobs, and monitoring status
- Manage system configuration, including editing failure reasons, and configuring e-mail, session directory, and alarm settings

See Monitoring and Reporting in ACS, page 11-1 for more information

Debug Logs

You can use the web interface and the CLI to send logs, including debug logs, to Cisco technical support personnel if you need troubleshooting assistance. In the web interface, choose **Monitoring and Reports > Launch Monitoring & Report Viewer > Monitoring and Reports > Troubleshooting > ACS Support Bundle**.

You can also use the CLI to view and export the hardware server in the Application Deployment Engine-OS 1.2 environment logs. These messages are sent to */var/log/boot.log* only and are unrelated to the way in which the CLI views or exports ACS debug log messages. See the *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.1* for information.

ACS 4.x Versus ACS 5.1 Logging

If you are familiar with the logging functionality in ACS 4.x, ensure that you familiarize yourself with the logging functionality of ACS 5.1, which is considerably different. Table 19-4 describes the differences between the logging functionality of ACS 4.x and ACS 5.1.

Table 19-4 ACS 4.x vs. ACS 5.1 Logging Functionality

This logging function…	is handled this way in ACS 4.x…	and this way in ACS 5.1
Log Types	• AAA-related logs contain information about the use of remote access services by users. • Audit logs contain information about the ACS system and activities and, therefore, record system-related events. These logs are useful for troubleshooting or audits. CSV audit logs are always enabled, and you can enable or disable audit logs to other loggers. You cannot configure the audit log content. Audit logs can display the actual changes administrators have made for each user. ACS audit logs list all the attributes that were changed for a given user.	See Logging Categories, page 19-2.
Available Log Targets	• CSV Logger • Syslog Logger • ODBC Logger • Remote Logging	See Remote Syslog Server Target, page 19-8 and Local Store Target, page 19-5.
Log File Locations	• CSV Logger: *sysdrive*`:\Program Files\CiscoSecure ACS v`*x.x*.	• Local store target logs: */opt/CSCOacs/logs/localStore/*. • Remote syslog server target logs: */var/log/messages*.
Report Types	• CSV • Dynamic Administration • Entitlement	See Monitoring and Reporting in ACS, page 11-1.
Error Codes and Message Text	For ACS 4.2, CSAuth diagnostic logs display a description of client requests and responses. Previous versions of ACS used a numeric code for client requests and responses.	All messages, see Viewing Log Messages, page 19-10.
Configuration	Use the **System Configuration > Logging** page to define: • Loggers and individual logs • Critical loggers • Remote logging • CSV log file • Syslog log • ODBC log	See Configuring Logs, page 18-21 and the *CLI Reference Guide for the Cisco Secure Access Control System 5.0*.

Table 19-4 ACS 4.x vs. ACS 5.1 Logging Functionality (continued)

This logging function…	is handled this way in ACS 4.x…	and this way in ACS 5.1
Viewing and Downloading Log Messages	Use the **Reports and Activity** pages.	See Viewing Log Messages, page 19-10.
Troubleshooting with Log Messages	Service log files reside in the *Logs* subdirectory of the applicable service directory.	See Debug Logs, page 19-11.

APPENDIX A

AAA Protocols

This section contains the following topics:

- Typical Use Cases, page A-1
- Access Protocols—TACACS+ and RADIUS, page A-4
- Overview of TACACS+, page A-5
- Overview of RADIUS, page A-5

Typical Use Cases

This section contains the following topics:

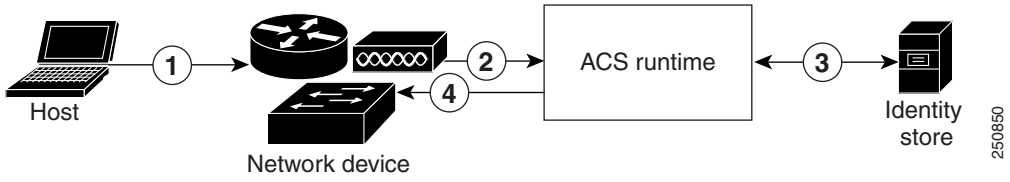
- Device Administration (TACACS+), page A-1
- Network Access (RADIUS with and without EAP), page A-2

Device Administration (TACACS+)

Figure A-1 shows the flows associated with device administration. The two primary triggers are:

- Session Access Requests (Device Administration [TACACS+]), page A-1.
- Command Authorization Requests, page A-2.

Figure A-1 Device Administration Flow



Session Access Requests (Device Administration [TACACS+])

Note The numbers refer to Figure A-1 on page A-1.

For session request:

1. An administrator logs in to a network device.
2. The network device sends a TACACS+ access request to ACS.
3. ACS uses an identity store to validate the user's credentials.
4. ACS sends a TACACS+ response to the network device that applies the decision. The response includes parameters, such as the privilege level that determines the level of administrator access for the duration of the session.

Command Authorization Requests

Note The numbers refer to Figure A-1 on page A-1.

For command authorization:

1. An administrator issues a command at a network device.
2. The network device sends a TACACS+ access request to ACS.
3. ACS optionally uses an identity store to retrieve user attributes for inclusion in policy processing.
4. The TACACS+ response indicates whether the administrator is authorized to issue the command.

Network Access (RADIUS with and without EAP)

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 ACS to authenticate and authorize the user.

ACS 5.1 supports the following categories of network access flows, depending on the protocol that is transported over the RADIUS protocol:

- RADIUS-based protocols that do not include EAP:
  - PAP
  - CHAP
  - MSCHAPv1
  - MSCHAPv2

  For more information on RADIUS-based protocols that do not include EAP, see RADIUS-Based Flow Without EAP Authentication, page A-3.
- EAP family of protocols transported over RADIUS, which can be further classified as:
  - Simple EAP protocols that do not use certificates:

    EAP-MD5

    LEAP
  - EAP protocols that involve a TLS handshake and in which the client uses the ACS server certificate to perform server authentication:

    PEAP, using one of the following inner methods: PEAP/EAP-MSCHAPv2 and PEAP/EAP-GTC

EAP-FAST, using one of the following inner methods: EAP-FAST/EAP-MSCHAPv2 and EAP-FAST/EAP-GTC

- EAP protocols that are fully certificate-based, in which the TLS handshake uses certificates for both server and client authentication:

  EAP-TLS

For more information on RADIUS-based flows with EAP authentication, see RADIUS-Based Flows with EAP Authentication, page A-3.

RADIUS-Based Flow Without EAP Authentication

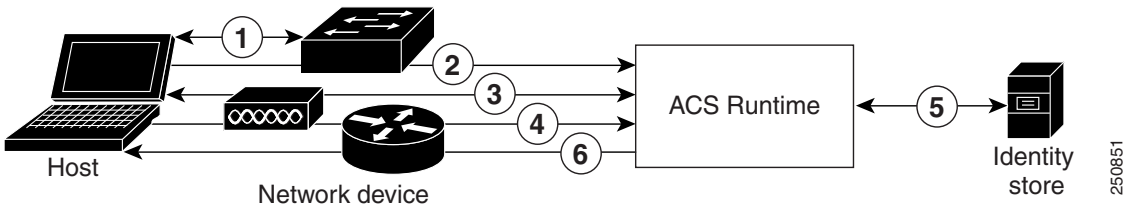
This section describes RADIUS-based workflow without EAP authentication.

For RADIUS with PAP authentication:

1. A host connects to a network device.
2. The network device sends a RADIUS Access-Request to ACS, containing RADIUS attributes appropriate to the specific protocol that is being used (PAP, CHAP, MSCHAPv1, or MSCHAPv2).
3. ACS uses an identity store to validate the user's credentials.
4. The RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

Figure A-2 shows a RADIUS-based authentication without EAP.

Figure A-2 RADIUS-Based Flow Without EAP Authentication



RADIUS-Based Flows with EAP Authentication

EAP provides an extensible framework that supports a variety of authentication types. Among them, the specific EAP methods supported by ACS are:

- Simple EAP methods that do not use certificates:
  - EAP-MD5
  - LEAP
- EAP methods in which the client uses the ACS server certificate to perform server authentication:
  - PEAP/EAP-MSCHAPv2
  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- EAP methods that use certificates for both server and client authentication
  - EAP-TLS

Whenever EAP is involved in the authentication process, it is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used.

For all EAP authentications:

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 ACS.
5. ACS 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.

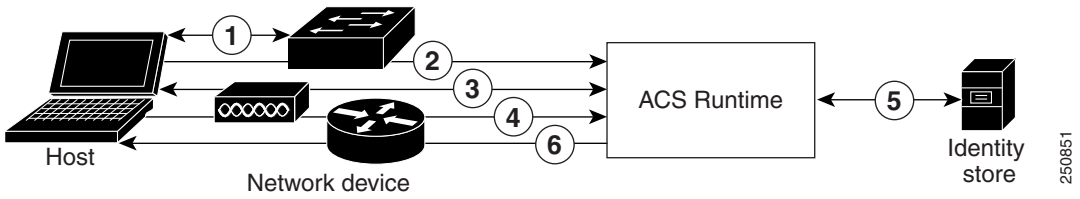
In this way, the host and ACS indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data needed to perform the actual authentication. If required by the specific EAP authentication method that is negotiated, ACS uses an identity store to validate the user's credentials.

After ACS 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 A-3 shows a RADIUS-based authentication with EAP.

Figure A-3 RADIUS-Based Authentication with EAP



For a list of known supplicant issues that might impact your ACS 5.1 experience, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/release/notes/acs_51_rn.html#wp123862.

Access Protocols—TACACS+ and RADIUS

This section contains the following topics:

- Overview of TACACS+, page A-5
- Overview of RADIUS, page A-5

ACS 5.1 can use the TACACS+ and RADIUS access protocols. Table A-1 compares the two protocols.

Table A-1 TACACS+ and RADIUS Protocol Comparison

Point of Comparison	TACACS+	RADIUS
Transmission Protocol	TCP—Connection-oriented transport-layer protocol, reliable full-duplex data transmission.	UDP—Connectionless transport-layer protocol, datagram exchange without acknowledgments or guaranteed delivery. UDP uses the IP to get a data unit (called a datagram) from one computer to another.
Ports Used	49	Authentication and Authorization: 1645 and 1812 Accounting: 1646 and 1813.
Encryption	Full packet-body encryption.	Encrypts only passwords up to 16 bytes.
AAA Architecture	Separate control of each service: authentication, authorization, and accounting.	Authentication and authorization combined as one service.
Intended Purpose	Device management.	User access control.

Overview of TACACS+

TACACS+ must be used if the network device is a Cisco device-management application, access server, router, or firewall. ACS 5.1 supports Cisco device-management applications by providing command authorization for network users who are using the management application to configure managed network devices. You provide support for command authorization for management application users by using unique command sets for each management application that is configured to use ACS for authorization.

ACS 5.1 uses TACACS+ to communicate with management applications. For a management application to communicate with ACS, you must configure the management application in ACS 5.1 as a AAA client that uses TACACS+. Also, you must provide the device-management application with a valid administrator name and password. When a management application initially communicates with ACS, these requirements ensure the validity of the communication.

Except for the packet-headers, all information that the client and TACACS+ server communicate, which is contained in the packet-bodies are encrypted through the use of a shared secret (which is, itself, not sent over the network directly).

Additionally, the administrator that the management application uses must have the Command Set privilege enabled.

Overview of RADIUS

This section contains the following topics:

- RADIUS VSAs, page A-6
- ACS 5.1 as the AAA Server, page A-6
- RADIUS Attribute Support in ACS 5.1, page A-7
- RADIUS Access Requests, page A-9

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. A company could use RADIUS to maintain user profiles in a central database that all remote servers can share. This protocol provides better security, and the company can use it to set up a policy that is applied at a single administered network point.

To support the older and newer RFCs, ACS 5.1 accepts authentication requests on port 1645 and port 1812. For accounting, ACS accepts accounting packets on ports 1646 and 1813.

RADIUS VSAs

ACS 5.1 provides a set of standard IETF RADIUS attributes. You can identify RADIUS IETF attributes that are currently unused by their names. These unused attributes are named in the following format: *attribute-nnn*, where *attribute* is the name of the attribute and *nnn* is the ID of the attribute.

In addition, ACS 5.1 supports RADIUS VSAs. The following set of predefined RADIUS VSAs are available after you install ACS 5.1:

- Cisco
- Cisco VPN 5000
- Microsoft
- US Robotics
- Ascend
- Nortel (Bay Networks)
- RedCreek
- Juniper
- Cisco VPN 3000
- Cisco Business Service Management (BSM)
- Cisco Aironet
- Cisco Airespace

You can modify these predefined RADIUS VSAs or define new RADIUS VSAs. You can create, edit, and duplicate RADIUS VSAs. For more information, see Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-6.

ACS 5.1 as the AAA Server

A AAA server is a server program that handles user requests for access to computer resources, and for an enterprise, provides AAA services. The AAA server typically interacts with network access and gateway servers, and databases and directories that contain user information. The current standard by which devices or applications communicate with an AAA server is RADIUS.

ACS 5.1 functions as a AAA server for one or more network access devices (NADs). The NADs are clients of the ACS server. You must specify the IP address of ACS on each client NAD, to direct user access requests to ACS by using the RADIUS protocol. RADIUS is universally used to secure the access of end-users to network resources. A RADIUS server can act as a proxy to other RADIUS servers or other kinds of authentication servers.

The NAD serves as the network gatekeeper and sends an Access-Request to ACS on behalf of the user. ACS verifies the username, password, and possibly other data by using either the internal identity store, or an externally configured LDAP or Windows Active Directory identity store. ACS ultimately responds to the NAD with either an Access-Reject message or an Access-Accept message that contains a set of authorization attributes.

ACS 5.1 provides network transport over UDP and implements the RADIUS protocol, including RADIUS packet parsing and assembling, necessary data validation, and tracking of duplicate requests.

Some reasons for using UDP are:

- The processing time is only a few seconds.
- No special handling is required for rebooting or offline clients and servers.
- UDP is a connectionless protocol.
- UDP easily implements multithreaded servers to serve multiple client requests.

The UDP-assigned port number for RADIUS are:

- 1812 for access requests
- 1813 for accounting
- 1645 for access requests
- 1646 for accounting

ACS 5.1 is the entrance point to the authentication system. ACS listens on specific configurable UDP ports. When data arrives from the network:

1. ACS tries to process the data as a RADIUS client request or proxy response packet.
2. ACS verifies that the packet arrived from the NAD that is registered in the configuration, and then prevents duplicate packet processing.
3. ACS parses the RADIUS packet and performs the necessary validations of its contents.
4. ACS then passes the data for processing to the appropriate flow.
5. When the system is ready to respond, ACS:
   a. Receives the result of the data processing.
   b. Creates a corresponding response to the client.
   c. Returns the response to the network.

RADIUS Attribute Support in ACS 5.1

ACS 5.1 supports the RADIUS protocol as RFC 2865 describes.

ACS 5.1 supports the following types of RADIUS attributes:

- IETF RADIUS attributes
- Generic and Cisco VSAs
- Other vendors' attributes

ACS 5.1 also supports attributes defined in the following extensions to RADIUS:

- Accounting-related attributes, as defined in RFC 2866.
- Support for Tunnel Protocol, as defined in RFCs 2867 and 2868.
- Support for EAP (via the EAP-Message attribute), as defined in RFCs 2869 and 3579.

Note When RADIUS parameters are referenced, the convention [*attribute-number*] [*attribute name*] is used. For example, [*1*]*User-Name*, where the number and name correspond to that assigned to the parameter in the specification.

RADIUS supports receiving, sending, and dictionary-based parsing and construction of any RADIUS attribute regardless of whether it is a regular attribute, VSA, or Cisco attribute-value (AV) pair. The RADIUS interface in ACS supports the attribute data types defined in RFC 2865, namely:

- *text* (UTF-8)
- *string* (binary)
- *address* (IP)
- *integer*
- *time*

Data types, integer, string, and text enumerated (ENUM) specifications of allowed values are supported. Attribute values are checked against these when packet parsing and construction occur.

ACS uses the RADIUS State attribute (24) to identify a specific conversation. Each conversation has a unique ID. Every conversation is processed under a specific configuration version—the latest available version at the moment the conversation was initiated.

Note The RADIUS State attribute (24) is not used for PAP authentication.

All transactions between the client and RADIUS server have their message integrity protected using the Request/Response Authenticator field inside each RADIUS packet, which makes use of a shared secret (that is, itself, not sent over the network directly). In addition, some forms of RADIUS packets that include all of those that contain encapsulated EAP-Message attributes have the integrity of all of their RADIUS attributes additionally protected using a Message-Authenticator RADIUS attribute (that also makes use of the shared secret). Furthermore, user passwords within the RADIUS packets sent between the client and RADIUS server are always encrypted to protect against the possibility that an unauthorized user on an insecure network could easily determine the password.

Authentication

ACS supports various authentication protocols transported over RADIUS. The supported protocols that do not include EAP are:

- PAP
- CHAP
- MSCHAPv1
- MSCHAPv2

In addition, various EAP-based protocols can be transported over RADIUS, encapsulated within the RADIUS EAP-Message attribute. These can be further categorized with respect to whether or not, and to what extent, they make use of certificates. These include:

- EAP methods that do not use certificates:
  - EAP-MD5
  - LEAP
- EAP methods in which the client uses the ACS server certificate to perform server authentication:

  - PEAP/EAP-MSCHAPv2
  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- EAP methods that use certificates for both server and authentication:
  - EAP-TLS

Authorization

Authorization is permitted according to the configured access policies.

Accounting

You can use the accounting functions of the RADIUS protocol independently of the RADIUS authentication or authorization functions. You can use some of the RADIUS accounting functions to send data at the start and end of sessions, and indicate the amount of resources (such as time, packets, bytes, and so on) that you used during the session. An ISP might use RADIUS access control and accounting software to meet special security and billing needs.

RADIUS Access Requests

A user login contains a query (Access-Request) from the network access device to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, password, NAD IP address, and NAD port, and other relevant attributes.

When the RADIUS server receives the access-request from the NAD, it searches a database for the username. Depending on the result of the database query, an accept or reject is sent. A text message can accompany the access-reject message to indicate the reason for the refusal.

In RADIUS, authentication and authorization are coupled. If the RADIUS server finds the username and the password is correct, the RADIUS server returns an access-accept response, including a list of attribute-value pairs that describe the parameters to use for this session. This list of parameters sets the authorization rights for the user.

Typical parameters include:

- Service type
- Protocol type
- IP address to assign the user (static or dynamic)
- Access list to apply
- A static route to install in the NAD routing table

The configuration information in the RADIUS server defines which parameters to set on the NAD during installation.

APPENDIX B

Authentication in ACS 5.1

Authentication verifies user information to confirm the user's identity. Traditional authentication uses a name and a fixed password. More secure methods use cryptographic techniques, such as those used inside the Challenge Authentication Handshake Protocol (CHAP), OTP, and advanced EAP-based protocols. ACS supports a variety of these authentication methods.

A fundamental implicit relationship exists between authentication and authorization. The more authorization privileges granted to a user, the stronger the authentication should be. ACS supports this relationship by providing various methods of authentication.

Authentication Considerations

Username and password 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. Simple unencrypted username and password is not considered a strong authentication mechanism but can be sufficient for low authorization or privilege levels such as Internet access.

You should use encryption to reduce the risk of password capture on the network. Client and server access-control protocols such as TACACS+ and RADIUS encrypt passwords to prevent them from being captured within a network. However, TACACS+ and RADIUS operate only between the AAA client and ACS. Before this point in the authentication process, unauthorized persons can obtain clear-text passwords; for example, in the following setups:

- The communication between an end-user client dialing up over a phone line
- An Integrated Services Digital Network (ISDN) line terminating at a network-access server
- Over a TELNET session between an end-user client and the hosting device

Authentication and User Databases

ACS supports a variety of user databases. It supports the ACS internal database and several external user databases, including:

- Windows Active Directory
- LDAP
- RSA SecurID Servers
- RADIUS Identity Servers

This appendix describes the following:

- RADIUS-based authentication that does not include EAP:
  - PAP, page B-2
  - CHAP, page B-29
  - MSCHAPv1
  - EAP-MSCHAPv2, page B-28
- EAP family of protocols transported over RADIUS, which can be further classified as:
  - Simple EAP protocols that do not use certificates:

    EAP-MD5—For more information, see EAP-MD5, page B-5.

    LEAP—For more information, see LEAP, page B-29.
  - EAP protocols that involve a TLS-handshake and in which the client uses the ACS server certificate to perform server authentication:

    PEAP, using one of the following inner methods: PEAP/EAP-MSCHAPv2 and PEAP/EAP-GTC—For more information, see PEAPv0/1, page B-14.

    EAP-FAST, using one of the following inner methods: EAP-FAST/EAP-MSCHAPv2 and EAP-FAST/EAP-GTC—For more information, see EAP-FAST, page B-18.
  - EAP protocols that are fully certificate-based, in which the TLS handshake uses certificates for both server and client authentication:

    EAP-TLS—For more information, see EAP-TLS, page B-5.
- Certificate Attributes, page B-30
- Machine Authentication, page B-32
- Authentication Protocol and Identity Store Compatibility, page B-33

For a list of known supplicant issues, refer to http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/release/notes/acs_51_rn.html#wp123862.

PAP

The Password Authentication Protocol (PAP) provides a simple method for a user to establish its identity by using a two-way handshake. The PAP password is encrypted with the shared secret and is the least sophisticated authentication protocol.

ACS checks the ID-Password pair against the external database, Identity Store, until ACS acknowledges the authentication or terminates the connection.

PAP is not a strong authentication method since it offers little protection from repeated trial-and-error attacks.

Note The RADIUS with PAP authentication flow includes logging of passed and failed attempts.

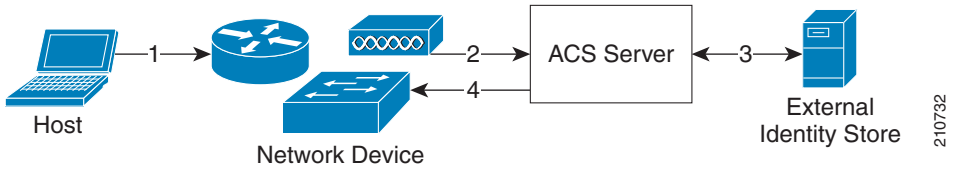
RADIUS PAP Authentication

You can use different levels of security concurrently with ACS for different requirements. PAP applies a two-way handshaking procedure. If authentication succeeds, ACS returns an acknowledgement; otherwise, ACS terminates the connection or gives the originator another chance.

The originator is in total control of the frequency and timing of the attempts. Therefore, any server that can use a stronger authentication method will offer to negotiate that method prior to PAP. RFC 1334 defines PAP.

Figure B-1 illustrates RADIUS with PAP authentication.

Figure B-1 RADIUS with PAP Authentication Use Case



1	A host connects to the network. Any communication protocol may be used depending on the host.	**3**	ACS uses an external identity store to validate the user's credentials.
2	The network device sends a RADIUS access request to ACS.	**4**	The RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

EAP

Extensible Authentication Protocol (EAP) is an authentication framework for wireless networks and point-to-point connections. EAP supports multiple authentication methods, and provides common functions and rules for negotiation of the desired authentication method:

- Server authentication request
- Client authentication response
- Server success authentication result
- Server failure authentication result
- Silent discard of client packets if they do not meet integrity and security conditions
- Rules for server-initiated EAP method negotiation
- Message sequencing, and tracking responses to requests
- Retransmit

EAP is a lock-step protocol; after the initial request, ACS cannot send a new request before receiving a valid response from the client.

In ACS 5.1, EAP is encapsulated in the RADIUS protocol. Incoming and outgoing EAP messages are stored in a RADIUS EAP-Message attribute (79). A single RADIUS packet can contain multiple EAP-Message attributes when the size of a particular EAP message is greater than the maximum RADIUS attribute data size (253 bytes). The RADIUS State attribute (24) stores the current EAP session reference information, and ACS stores the actual EAP session data.

The EAP standard is described in:

- RFC 3748—Extensible Authentication Protocol (EAP).
- RFC 3579—RADIUS Support For Extensible Authentication Protocol (EAP).

In the EAP process:

1. The network device sends an EAP Request to a host when the host connects to the network.
2. The host sends an EAP Response to the network device; the network device embeds the EAP packet that it received from the host into a RADIUS request and sends it to ACS, which is acting as the EAP server.
3. ACS negotiates the EAP method for authentication. The client can acknowledge the EAP method that the EAP server suggests or, it can respond with a negative acknowledgment (NAK) and suggest a list of alternative EAP methods. The server and client must reach agreement about the EAP method to use to instantiate authentication.

Table B-1 lists the EAP codes for each type of EAP message.

Table B-1 EAP Codes

EAP message type	EAP code
Accept-request	1
Response	2
Success	3
Failure	4

Table B-2 describes the EAP methods that ACS 5.1 supports.

Table B-2 Supported EAP methods

EAP Method	Description
EAP-MD5	Message Digest 5 Protocol. For more information see EAP-MD5, page B-5.
LEAP	Lightweight Extensible Authentication Protocol.
PEAPv0v1	Protected Extensible Authentication Protocol version 0 and version 1. For more information see PEAPv0/1, page B-14.
EAP-FAST	EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol. For more information see EAP-FAST, page B-18.
EAP-MSCHAPv2	Microsoft Challenge Handshake Authentication Protocol version 2. For more information see EAP-MSCHAPv2, page B-28.
EAP-GTC	EAP Generic Token Card.
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security. For more information, see Exporting Credentials, page B-11.

ACS supports full EAP infrastructure, including EAP type negotiation, message sequencing and message retransmission. All protocols support fragmentation of big messages.

In ACS 5.1, you configure EAP methods for authentication as part of access service configuration. For more information about access services, see Chapter 3, "ACS 5.x Policy Model."

EAP-MD5

This section contains the following topics:

- Overview of EAP-MD5, page B-5
- EAP- MD5 Flow in ACS 5.1, page B-5

Overview of EAP-MD5

EAP Message Digest 5-(EAP-MD5) provides one-way client authentication. The server sends the client a random challenge. The client proves its identity by hashing the challenge and its password with MD5. Because a man in the middle could see the challenge and response, EAP-MD5 is vulnerable to dictionary attack when used over an open medium. Since no server authentication occurs, it is also vulnerable to spoofing.

Related Topics

- Host Lookup, page 4-12
- Overview of Agentless Network Access, page 4-11

EAP- MD5 Flow in ACS 5.1

ACS supports EAP-MD5 authentication against the ACS internal identity store. Host Lookup is also supported when using the EAP-MD5 protocol. See Host Lookup, page 4-12.

Related Topics

- Authentication Protocol and Identity Store Compatibility, page B-33
- Overview of Agentless Network Access, page 4-11

EAP-TLS

This section contains the following topics:

- Overview of EAP-TLS, page B-6
- EAP-TLS Flow in ACS 5.1, page B-12

Overview of EAP-TLS

EAP-TLS is one of the methods in the EAP authentication framework, and is based on the 802.1x and EAP architecture. Components involved in the 802.1x and EAP authentication process are the:

- Host—The end entity, or end user's machine.
- AAA client—The network access point.
- Authentication server—ACS.

The EAP-TLS standard is described in:

- RFC 2716—PPP EAP-TLS Authentication Protocol
- RFC 3079—Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)

This section contains the following topics:

- User Certificate Authentication, page B-6
- PKI Authentication, page B-7

The host must support EAP-TLS authentication. The access point must support the EAP authentication process in the 802.1x environment (the access point is not aware of the EAP authentication protocol type).

Related Topics

- Configuring CA Certificates, page 8-61
- Certificate-Based Network Access, page 4-8
- ACS and Cisco TrustSec, page 4-22
- EAP-TLS Flow in ACS 5.1, page B-12

User Certificate Authentication

EAP-TLS is a mutual authentication method for certificate-based authentication; the client and server authenticate each other by using digital certificates. Certificates must meet specific requirements on the server and client for successful authentication. EAP and TLS are Internet Engineering Task Force (IETF) RFC standards. The EAP protocol carries initial authentication information, specifically the encapsulation of EAP over LANs (EAPOL) as established by IEEE 802.1x. TLS uses certificates for user authentication and dynamic ephemeral session key generation.

Once the peer is authenticated and a session is created, the information is cached on ACS for a certain amount of time. The session can be re-established by using the EAP-TLS session resume, without an additional certificate exchange. ACS 5.1 maintains the server certificate and private key in files on the ACS server, which it uses during EAP-TLS processing. You can choose the certificate authorities (CAs) that can be trusted to sign on client certificates.

EAP-TLS authentication involves two elements of trust:

- The EAP-TLS negotiation establishes end-user trust by validating, through RSA signature verifications, that the user possesses a keypair that a certificate signs. This process verifies that the end user is the legitimate keyholder for a given digital certificate and the corresponding user identification in the certificate. However, trusting that a user possesses a certificate only provides a username-keypair binding.

- Using a third-party signature, usually from a CA, that verifies the information in a certificate. This third-party binding is similar to the real-world equivalent of the stamp on a passport. You trust the passport because you trust the preparation and identity-checking that the particular country's passport office made when creating that passport. You trust digital certificates by installing the root certificate CA signature.

Some situations do not require this second element of trust that is provided by installing the root certificate CA signature. When such external validation of certificate legitimacy is not required, you can use the ACS self-signed certificate capability. Depending on the end-user client involved, the CA certificate for the CA that issued the ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer. For more information, see Adding a Certificate Authority, page 8-62.

EAP-TLS-compliant AAA clients include:

- Cisco 802.1x-enabled switch platforms (such as the Catalyst 6500 product line)
- Cisco Aironet Wireless solutions

To accomplish secure Cisco Aironet connectivity, EAP-TLS generates a dynamic, per-user, per-connection, unique session key.

Related Topics

- Configuring CA Certificates, page 8-61
- Certificate-Based Network Access, page 4-8

PKI Authentication

EAP-TLS uses public key infrastructures (PKI) concepts:

- A host requires a valid certificate to authenticate to the LAN network.
- The AAA server requires a server certificate to validate its identity to the clients.
- The certificate-authority-server infrastructure issues certificates to the AAA server(s) and the clients.

An SSL/TLS tunnel authentication is conducted by both peers and is initiated by the client. In ACS, the tunnel can be either authenticated by:

- both peers
- either one
- neither client or host

A tunnel that is constructed without an authentication is considered an anonymous tunnel, and is usually constructed by the Diffie-Hellman key exchange protocol. ACS supports the SSL/TLS session resume feature for TLS. ACS maintains the tunnel keys and cipher used to establish the tunnel communication in the cache for each session. Fetching an old session is based on the session ID which is unique for each client.

You can configure the timeout for each session in the cache, for each protocol individually. The lifetime of a session is measured from the beginning of the conversation and is determined when the TLS session is created.

ACS supports establishment of a tunnel from a commonly shared key known to the client and the server for the EAP-FAST protocol. The key that is securely agreed upon between the two peers is used to derive a shared tunnel TLS-master-key that is used to open a tunnel. This mechanism involves a shorter TLS negotiation.

An anonymous Diffie-Hellman tunnel relates to the establishment of a completely anonymous tunnel between a client and a server for cases where none of the peers authenticates itself. ACS runtime supports anonymous Diffie-Hellman tunnels for EAP-FAST with a predefined prime and a predefined generator of two. There is no server authentication conducted within anonymous Diffie-Hellman tunnel cipher-suites.

An authenticated Diffie-Hellman tunnel is similar to an anonymous Diffie-Hellman tunnel. The additional factor of the authenticated Diffie-Hellman tunnel is that peer authentication is conducted through an RSA certificate. ACS supports Authenticated-Diffie-Hellman tunnels for EAP-FAST where the server authenticates by using its own certificate.

Additional client authentications are conducted within the tunnel by using other protocols, such as EAP-MSCHAPv2 or EAP-GTC for the inner EAP method.

Related Topics

- Configuring Local Server Certificates, page 18-14
- Configuring CA Certificates, page 8-61
- Configuring Certificate Authentication Profiles, page 8-66

PKI Credentials

This section contains the following topics:

- PKI Usage, page B-8
- Fixed Management Certificates, page B-8
- Importing Trust Certificates, page B-9
- Exporting Credentials, page B-11

PKI Usage

ACS supports using certificates for various PKI use cases. The main use case is the EAP-TLS protocol, where the PKI is used to authenticate not only the server, but also the client (PEAP and EAP-FAST also make use of certificates for server authentication, but do not perform client authentication). Other protocols which use the PKI credentials are LDAPS, HTTPS Management protocol, SSH, and SFTP.

For TLS related EAP protocols, a single local certificate is used to authenticate the server for all the TLS related EAP protocols. You can pick the certificate to use from any of the certificates containing a private-key in the Local Certificate store.

For other protocols, such as HTTPS, SFTP, and SSH, and for the message-bus ActiveMQ authentication, a single certificate should be configured to authenticate ACS. You can pick the certificate to use from any of the certificates containing a private-key in the Local Certificate store. You can configure the same local certificate for the TLS-related EAP protocols and for HTTPS Management protocol.

For HTTPS, SFTP, SSH and ActiveMQ, an auto-generated self-signed certificates can be used as the means for server authentication.

Fixed Management Certificates

ACS generates and uses self-signed certificates to identify various management protocols such as the Web browser, HTTPS, ActiveMQ SSH, and SFTP.

Self-signed certificates are generated when ACS is installed and are maintained locally in files outside of the ACS database. You cannot modify or export these certificates. You can, however, assign imported certificates to management interfaces.

Importing Trust Certificates

ACS supports PEM or DER formatted X509 certificate files. You can add a trust certificate to the trust certificate store. ACS verifies that an imported certificate complies with the X509 format and does not perform any hierarchical certificate signature verification. ACS also supports the Microsoft proprietary private key format.

You can mark the acquired certificate for immediate trust for TLS related EAP protocols as the EAP CTL. The trust certificate store does not allow for duplicate trust certificates. These are the rules for rejecting certificates:

- Two certificates cannot have the same subject.
- Two certificates cannot have the same issuer and the same serial-number.

Acquiring Local Certificates

This topic describes the methods for ACS to acquire PKI credentials, and the ways that you can sets the public or private keys pairs to each ACS server in the ACS domain.

An X509 certificate contains the credentials which include the public key, and a PKCS#12 [?10.1] that holds the private key protected with a password that goes with it.

The ACS domain may have more than a single ACS server; each domain should have its own set of PKI key pairs to identify itself through the appropriate interfaces. Some interfaces may require that the certificate that identifies ACS, contain the IP or FQDN of the ACS server, in its Common Name (CN) for better binding of the certificate to the IP of the server, for example, the HTTPS ACS server certificate which is used for the Web interface. For other interfaces, it may be possible to use a common certificate that can be shared between the servers, however, Cisco does not recommend that you use a common certificate. Each ACS PKI credentials may be obtained either from a self-signed certificate or a certificate signed by a common certificate authority (CA). For protocols that require the ACS identification, clients should be deployed with at least the lowest common certificate that dominates all the ACS servers certificates that are used to identify each ACS.

You can pick the PKI policy to be used in your organization and configure the PKI credentials for the ACS domain.

The configured certificate with its private-key should not be used outside the ACS machine

Related Topics

- Importing the ACS Server Certificate, page B-9
- Initial Self-Signed Certificate Generation, page B-10
- Certificate Generation, page B-10

Importing the ACS Server Certificate

When you manually import and ACS server certificate you must supply the certificate file, the private key file, and the private key password used to decrypt the PKCS#12 private key. The certificate along with its private-key and private-key-password, is added to the Local Certificate store. For non-encrypted private-keys, the user supplied password may be ignored.

ACS supports PEM or DER formatted X509 certificate files. ACS verifies that an imported certificate complies with a the X509 format and does not perform any hierarchical certificate signature verification.

When importing a certificate, you can configure the certificate for protocol that require an ACS server certificate, such as TLS related EAP protocols and HTTPS Management protocol.

Note Only EAP and HTTPS Management protocols can be configured in ACS 5.1 for certificate-based authentication.

The input password and private-key, which are cryptographically sensitive information, are passed over the HTTPS channel. Using HTTPS with a non-authenticated server, for example, a self-signed certificate for HTTPS server authentication, is not a secure method of passing this sensitive information.

- Importing Trust Certificates, page B-9
- Initial Self-Signed Certificate Generation, page B-10
- Certificate Generation, page B-10

Initial Self-Signed Certificate Generation

An automatically generated, self-signed certificate is placed in the Local Certificate store for each ACS server. This certificate is used to identify ACS for TLS-related EAP protocols and for HTTPS Management protocols. The self-signed certificate is generated with the CN equal to the machine's hostname, as required for HTTPS certificates, and is generated when ACS is installed.

Certificate Generation

You an generate ACS server certificates through the Web interface. The output of this process is a certificate or a certificate request and it's corresponding private-key and password. The generated private-key is structured as PKCS#12 encrypted, by using a relatively strong automatically generated password based on at least 128 bit of randomness.

You can pick the generated private-key length, from 512, 1024, 2048 or 4096 bit. The certificate digest algorithm used by the ACS is SHA1.

You must input the certificate subject for the generated certificate or certificate request. ACS uses the common Name (CN) field in the subject. You can set the ACS server's IP address for the CN attributes, to the static IP address or the FQDN address of the server. The reason behind this, is that certificates that authenticate an HTTPS server must include the server's IP address as the CN, which is part of the protected information in that certificate. Other nonmandatory fields that ACS supports for certificate generation are O, OU, C, L, S, and E.

There are two types of certificate generation:

- Self signing certificate generation — ACS supports generation of an X.509 certificate and a PKCS#12 private key. The passphrase used to encrypt the private key in the PKCS#12 automatically generates stronger passwords, and the private key is hidden in the local certificate store. You can select the newly generated certificate for immediate use for HTTPS Management protocol, for TLS-related EAP protocols, or both.
- Certificate request generation—ACS supports generation of a PKCS#10 certificate request with a PKCS#12 private key. The request is downloaded through the Web interface and should be formatted with PEM representation with a REQ extension. The passphrase used to encrypt the private key in the PKCS#12 automatically generates stronger passwords, and the private-key is hidden in the ACS database. You can download the request file to be signed offline by the RA. After the RA signs the

request, you can install the returned signed certificate on ACS and bind the certificate with its corresponding private key. The binding of certificate and its private key is automatic. After binding the signed certificate with the private key, you can mark this certificate for immediate use for HTTPS Management protocol, for TLS-related EAP protocols, or both.

Related Topics

- Configuring CA Certificates, page 8-61
- Configuring Certificate Authentication Profiles, page 8-66
- EAP-TLS Flow in ACS 5.1, page B-12

Exporting Credentials

You can export a general trust certificates, an ACS server certificate with or without private keys, and previously generated certificates requests from the certificate stores. You cannot export the request for a private-key. You can download certificates file with a *.CER* extension. The file format is not changed from the format that is imported into ACS.

You can download the public certificate as a regular certificate with *.CER* extension for ACS server certificates, that also contain a private key. The file format is retained.

You can export a public request to re-issue a certificate request to an RA, for certificate-requests. The request is downloaded with an REQ extension and is formatted identically to the format that it was generated by.

Only administrators with the highest administrator privileges can export the certificate private key and its password. A warning about the security implications of such an action is conveyed twice, to approve the export operation. After this double check, the private-key files can be downloaded as a *.PVK* extension, and the private-key password can be downloaded as a *.PWD* extension. The private-key file format is retained.

Credentials Distribution

All certificates are kept in the ACS database which is distributed and shared between all ACS nodes. The ACS server certificates are associated and designated for a specific node, which uses that specific certificate.

Public certificates are distributed along with the private keys and the protected private key passwords by using the ACS distributed mechanism. ACS implements a method of protection to prevent a private-key to be used by other servers other than the one to which the private-key is designated to. This protection mechanism applies only to encrypted private-keys.

The PKI policy for private keys is that private keys are not supposed to be usable by other entities which are not associated with the ACS server to which they are designated to. ACS supports cryptographic protection of the private-keys to prevent possible use outside of the ACS server machine to which they are designated to.

Hardware Replacement and Certificates

When hardware fails, a new node is used for replacing a malfunctioning node. The malfunctioning node's certificates are removed from the distributed database of the primary server, and the new node's certificates are then being passed to the primary to be associated with the newly replaced node.

This process of certificate changing is conducted as part of the hardware replacement process when the new node registered to the domain, The certificate distribution is based on the server's IP address.

Securing the Cryptographic Sensitive Material

There are several types of PKI-related keys that are stored in the ACS database. These keys have different cryptographic storage requirements that must comply to SEC-RCV-CRED-2 which is part of the Cisco security baseline. These requirements include:

- Public keys that usually reside in a certificate may be stored plain open as they are used to pass on the clear text to clients and contain only public keys.
- Private keys must be stored encrypted as PKCS#12 by using a relatively strong password.
- The password for the PKCS#12 private-keys must be stored in the ACS database. Since the ACS database is encrypted, this does not pose a serious security concern. ACS 5.1 distributes the entire database between all the ACS servers. ACS encrypts the private-key passwords by using a password that exists only for the machine, thus preventing possible use of the private-keys by other machines. The private-key password key is maintained in */opt/CSCOacs/config/prikeypwd.key* on the ACS file-system.

Other certificate repositories such as the tomcat key-store should have the same properties as the ACS database. Private-keys are encrypted by a password that is kept secured in the database.

Private Keys and Passwords Backup

The entire ACS database is distributed and backed-up on the primary ACS along with all the certificates, private-keys and the encrypted private-key-passwords. The private-key-password-key of the primary server is also backed up with the primary's backup.

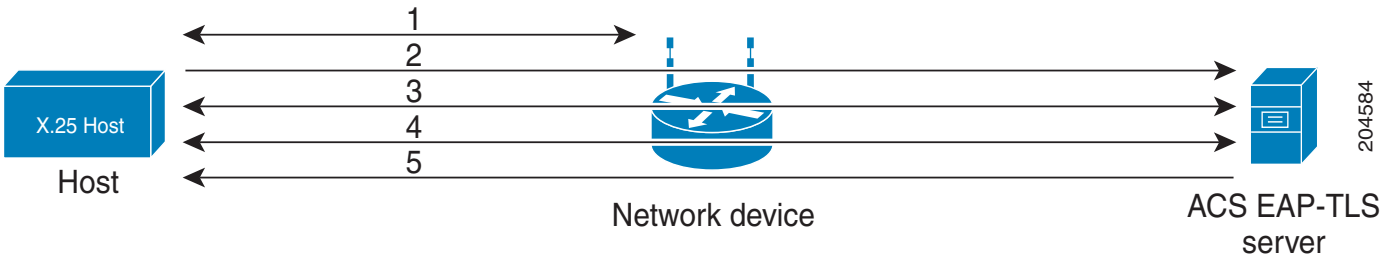
Other secondary ACS private-key-password-keys are not backed-up. Backups are encrypted and also can pass relatively secured in and out of the ACS servers. The private keys in backups are protected by the PKCS#12 and the backup file encryption. The passwords that are used to open the PKCS#12 private-keys are protected with the backup encryption.

EAP-TLS Flow in ACS 5.1

An EAP-TLS server exchanges data with a client by using packets based on the EAP Request and response packets; the packets are extended by specific EAP-TLS data. ACS acts as the EAP-TLS server, and uses the Open Secure Sockets Layer (OpenSSL) library to process the TLS conversation. The ACS EAP-TLS server produces 128-bit MPPE send and receive keys that are used for encrypted communication between the client and server. The ACS EAP-TLS server sends MPPE keys to the client in vendor-specific RADIUS attribute (26) by using vendor code Microsoft (311), and attributes MS-MPPE-Send-Key (16) and MS-MPPE-Recv-Key (17).

Figure B-2 shows the EAP-TLS processing flow between the host, network device, and ACS EAP-TLS server.

Figure B-2 EAP-TLS Flow



1	A host connects to the network. The network device sends an EAP Request to the host.	**2**	The host sends an EAP Response to the network device; the network device embeds the EAP packet that it received from the host into a RADIUS Access-Request and sends it to ACS.
3	ACS negotiates the EAP method for authentication. The server and client must reach agreement to use EAP-TLS (EAP Request method 13) during EAP method negotiation to instantiate EAP-TLS authentication.	**4**	The client (host) and server (ACS) exchange certificates; this exchange involves several messages. EAP-TLS authentication is successful after the client and server have authenticated each other, and each side is aware that the other side has authenticated them.
5	ACS returns an EAP Success (or EAP Failure) message to the host and returns a RADIUS Access-Accept (or RADIUS Access-Reject) that includes session keys to the network device.		

Note All communication between the host and ACS goes through the network device.

EAP-TLS authentication fails if the:

- Server fails to verify the client's certificate, and rejects EAP-TLS authentication.
- Client fails to verify the server's certificate, and rejects EAP-TLS authentication.

  Certificate validation fails if the:

  - Certificate has expired.
  - Server or client cannot find the certificate issuer.
  - Signature check failed.
- The client dropped cases resulting in malformed EAP packets.

EAP-TLS also supports the Session Resume feature. ACS supports the EAP-TLS session resume feature for fast reauthentication of a user who has already passed full EAP-TLS authentication. If the EAP-TLS configuration includes a session timeout period, ACS caches each TLS session for the duration of the timeout period. When a user reconnects within the configured EAP-TLS session timeout period, ACS resumes an EAP-TLS session, and the user reauthenticates by a TLS handshake only, without a certificate comparison.

Related Topics

- Types of PACs, page B-21
- User Certificate Authentication, page B-6

PEAPv0/1

This section contains the following topics:

- Overview of PEAP, page B-14
- EAP-MSCHAPv2, page B-28

ACS 5.1 supports these PEAP supplicants:

- Microsoft Built-In Clients 802.1x XP (PEAPv0 only)
- Microsoft Built-In Clients 802.1x Vista (PEAPv0 only)
- CSSC v.4.0
- CSSC v.5
- Funk Odyssey access client (latest version)
- Intel Supplicant 12.4.x

Overview of PEAP

PEAP is a client-server security architecture that you use to encrypt EAP transactions, thereby protecting the contents of EAP authentications. PEAP uses server-side public key certificates to authenticate the server. It then creates an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

PEAP is similar to EAP-TLS but uses a different client authentication method. PEAP provides authentication, by using server certificates, a TLS tunnel and client authentication through that encrypted tunnel. Unlike EAP-TLS, PEAP requires the client to use another EAP type, like EAP-MSCHAPv2.

PEAP authentications always involve two phases:

- In phase1, the end-user client authenticates ACS. This action requires a server certificate and authenticates ACS to the end-user client, ensuring that the user or machine credentials sent in phase two are sent to a AAA server that has a certificate issued by a trusted CA. The first phase uses a TLS handshake to establish an SSL tunnel between the end-user client and the AAA server.

Note Depending on the end-user client involved, the CA certificate for the CA that issued the ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer.

- In the second phase, ACS authenticates the user or machine credentials by using an EAP authentication protocol. The SSL tunnel that was created in phase1 protects the EAP authentication. The inner-method authentication type that is negotiated during phase 2 can be either EAP-MSCHAPv2 or EAP-GTC. The combination of the outer PEAP method with a specific inner EAP method is denoted using a slash character; for example, PEAP/EAP-MSCHAPv2 or PEAP/EAP-GTC.

  One improvement in security that PEAP offers is identity protection. This improvement is the potential for protecting the username in all PEAP transactions. After phase one of PEAP, all data is encrypted, including username information that is usually sent in clear text. The Microsoft PEAPv0 client does not provide identity protection; the Microsoft PEAPv0 client sends the username in clear text in phase one of PEAP authentication.

In ACS 5.1, PEAP is encapsulated in RADIUS protocol. Inner-method EAP messages are encapsulated in an EAP-TLV method.

Supported PEAP Features

This section contains the following topics:

- Server Authenticated and Unauthenticated Tunnel Establishment Modes, page B-15
- Fast Reconnect, page B-15
- Session Resume, page B-15
- Protected Exchange of Arbitrary Parameters, page B-16

Server Authenticated and Unauthenticated Tunnel Establishment Modes

Tunnel establishment helps prevent an attacker from injecting packets between the client and the network access server (NAS) or, to allow negotiation of a less secure EAP method. The encrypted TLS channel also helps prevent denial of service attacks against the ACS.

A 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 RADIUS Access-Accept message. The EAP Failure message is always carried in the RADIUS Access-Reject message. The client's PEAP message may cause the RADIUS client's message to drop unless the policy component is configured otherwise.

Fast Reconnect

When a session resumes, another method of decreasing the authentication time is to skip the inner method, also known as fast reconnect. After a tunnel is built, the authentication flow goes directly to exchange authentication information with a Result TLV Success (v0)/tunneled EAP Success message for successful authentication and an EAP Failure message in case of unsuccessful authentication. You can configure ACS to enable the fast reconnect option. After successful authentication, the client is able to perform a fast reconnect during a certain timeframe. PEAP fast reconnect reduces the delay in the time between an authentication request by a client and the response by ACS. Fast reconnect also allows wireless clients to move between access points without repeated requests for authentication, which reduces resource requirements for the client and the server.

The user identity and the protocol used for user authentication (inner method) should be cached along with the TLS session to allow fast reconnect.

Session Resume

ACS supports a session resume feature for PEAP-authenticated user sessions. When this feature is enabled, ACS caches the TLS session that is created during phase one of PEAP authentication, provided that the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, ACS uses the cached TLS session, resulting in faster PEAP performance and a lessened AAA server load.

ACS stores the session in the cache after a successful full authentication. A client may try to resume the same session during a specific timeframe. A server certificate is not presented and the tunnel is built by using the session information from the OpenSSL session cache. The authentication flow then goes directly to the inner method.

If a client attempts to perform session resume but the timeout elapsed, ACS reverts to the full authentication flow.

You can configure the session resume and timeout values.

Protected Exchange of Arbitrary Parameters

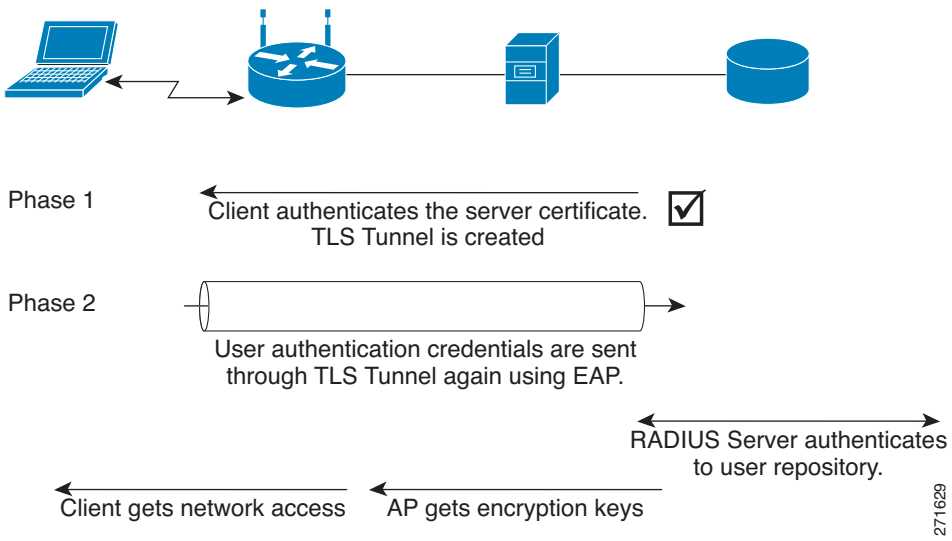
TLV tuples provide a way to exchange arbitrary information between the peer and ACS within a secure channel.

PEAP Flow in ACS 5.1

The PEAP protocol allows authentication between ACS and the peer by using the PKI-based secure tunnel establishment and the EAP-MSCHAPv2 protocol as the inner method inside the tunnel. The local certificate can be validated by the peer (server-authenticated mode) or not validated (server-unauthenticated mode).

Figure B-3 shows the PEAP processing flow between the host, access point, network device, and ACS EAP-TLS server.

Figure B-3 PEAP Processing Flow



Creating the TLS Tunnel

The following describes the process for creating the TLS tunnel:

1	After creating a logical link, the wireless AP sends an EAP-Request/Identity message to the wireless client.	**2**	The wireless client responds with an EAP-Response/Identity message that contains the identity (user or computer name) of the wireless client.
3	The wireless AP sends the EAP-Response/Identity message to ACS. From this point on, the logical communication occurs between ACS and the wireless client by using the wireless AP as a pass-through device.	**4**	ACS sends an EAP-Request/Start PEAP message to the wireless client.
5	The wireless client and ACS exchange a series of TLS messages through which the cipher suite for the TLS channel is negotiated. In ACS 5.1, the client certificate is not used in PEAP.	**6**	At the end of the PEAP negotiation, ACS has authenticated itself to the wireless client. Both nodes have determined mutual encryption and signing keys (by using public key cryptography, not passwords) for the TLS channel.

Authenticating with MSCHAPv2

After the TLS tunnel is created, follow these steps to authenticate the wireless client credentials with MSCHAPv2:

1	ACS sends an EAP-Request/Identity message.	**2**	The wireless client responds with an EAP-Response/Identity message that contains the identity (user or computer name) of the wireless client.
3	ACS sends an EAP-Request/EAP-MSCHAPv2 challenge message that contains a challenge string.	**4**	The wireless client responds with an EAP-Response/EAP-MSCHAPv2 Response message that contains the response to the ACS challenge string and a challenge string for ACS.
5	ACS sends an EAP-Request/EAP-MSCHAPv2 success message, which indicates that the wireless client response was correct and contains the response to the wireless client challenge string.	**6**	The wireless client responds with an EAP-Response/EAP-MSCHAPv2 acknowledgment message, indicating that the ACS response was correct.
7	ACS sends an EAP-Success message.		

At the end of this mutual authentication exchange, the wireless client has provided proof of knowledge of the correct password (the response to the ACS challenge string), and ACS has provided proof of knowledge of the correct password (the response to the wireless client challenge string). The entire exchange is encrypted through the TLS channel created in PEAP.

Related Topics

- Authentication Protocol and Identity Store Compatibility, page B-33
- Configuring PEAP Settings, page 18-3

EAP-FAST

This section contains the following topics:

- Overview of EAP-FAST, page B-18
- EAP-FAST Flow in ACS 5.1., page B-25
- EAP-FAST PAC Management, page B-26

Overview of EAP-FAST

The EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol is a new, publicly accessible IEEE 802.1x EAP type that Cisco developed to support customers that cannot enforce a strong password policy and want to deploy an 802.1x EAP type that does not require digital certificates. EAP-FAST supports a variety of user and password database types, password change and expiration, and is flexible, easy to deploy, and easy to manage. For more information about EAP-FAST and comparison with other EAP types, see:

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

EAP-FAST is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. While similar to PEAP in this respect, it differs significantly in that EAP-FAST tunnel establishment is based on strong secrets that are unique to users. These secrets are called Protected Access Credentials (PACs), which ACS generates by using a master key known only to ACS. Because handshakes based on shared secrets are intrinsically faster than handshakes based on PKI, EAP-FAST is by far the fastest of the advanced EAP protocols (including EAP-TLS and PEAP) that establish a TLS connection to encrypt the traffic between the supplicant and ACS. No certificate management is required to implement EAP-FAST.

EAP-FAST occurs in three phases:

- Phase zero—Unique to EAP-FAST, phase zero is a tunnel-secured means of providing an EAP-FAST end-user client with a PAC for the user requesting network access. (See Automatic In-Band PAC Provisioning, page B-22.) Providing a PAC to the end-user client is the sole purpose of phase zero. The tunnel is established based on an anonymous Diffie-Hellman key exchange for Anonymous In-band provisioning. Authenticated In-band provisioning uses other cipher suites. If EAP-MSCHAPv2 or EAP-GTC authentication succeeds, ACS provides the user with a PAC. To determine which databases support EAP-FAST phase zero, see Authentication Protocol and Identity Store Compatibility, page B-33.

  Note Phase zero is optional and PACs can be manually provided to end-user clients. (See Manual PAC Provisioning, page B-23.)

  The Allow Anonymous In-Band PAC provisioning option provides an end-user client with a PAC by using EAP-FAST phase zero. If this check box is checked, ACS establishes a secured connection with the end-user client for the purpose of providing the client with a new PAC. This option allows an anonymous TLS handshake between the end-user client and ACS (EAP-MSCHAPv2 and EAP-GTC are used as inner methods.)

  The Allow Authenticated In-Band PAC provisioning option provisions an end-user client with a PAC by using EAP-FAST phase zero with TLS server-side authentication. This option requires that you install a server certificate.

In general, phase zero of EAP-FAST does not authorize network access. However, if you choose the Accept Client on Authenticated Provisioning option, ACS sends a RADIUS Access-Accept (containing an EAP Success) at the end of a successful phase zero PAC provisioning, and the client is not forced to reauthenticate again. This option can be enabled only when the Allow Authenticated In-Band PAC Provisioning option is also enabled.

- Phase one—In phase one, ACS and the end-user client establish a TLS tunnel based on the PAC that the end-user client presents. This phase requires that the end-user client has been provided a PAC for the user who is attempting to gain network access and that the PAC is not expired. The means by which PAC provisioning has occurred is irrelevant; you can use automatic or manual provisioning.
- Phase two—In phase two, ACS authenticates the user's credentials from within the protected TLS tunnel that was constructed in phase one, using EAP-MSCHAPv2 or EAP-GTC as the inner EAP method. To determine which databases support EAP-FAST phase two, see Authentication Protocol and Identity Store Compatibility, page B-33.

Phase one and phase two are subsequent parts of the same EAP-FAST conversation.

EAP-FAST can protect the username in all EAP-FAST transactions. ACS does not perform user authentication based on a username that is presented in phase one, however, whether the username is protected during phase one depends on the end-user client. If the end-user client does not send the real username in phase one, the username is protected. After phase one of EAP-FAST, all data is encrypted, including username information that is usually sent in clear text.

ACS supports password aging with EAP-FAST for users who are authenticated by Windows user databases. Password aging can work with phase zero or phase two of EAP-FAST. If password aging requires a user to change passwords during phase zero, the new password would be effective in phase two.

EAP-FAST Benefits

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 clear text or hashed, by the peer to the EAP server.
- Immunity to man-in-the-middle (MitM) 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 MSCHAPv2 and 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 authentication server's per user authentication state requirements—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 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 it must cache and manage.

EAP-FAST in ACS 5.1

ACS supports in-band provisioning of the peer with a shared secret credential (PAC) based on PKI or ADHP (phase 0). Authentication of the peer and allowing the peer access to the network is implemented in phase 1 and phase 2.

ACS 5.1 supports EAP-FAST versions 1 and 1a.

This section contains the following topics:

- About Master-Keys, page B-20
- About PACs, page B-20
- Provisioning Modes, page B-21
- Types of PACs, page B-21
- Machine PAC Authentication, page B-24
- Proactive PAC Update, page B-24
- Accept Peer on Authenticated Provisioning, page B-24
- PAC-Less Authentication, page B-24
- Master Key Generation and PAC TTLs, page B-25

About Master-Keys

EAP-FAST master-keys are strong secrets that ACS automatically generates and of which only ACS is aware. Master-keys are never sent to an end-user client. EAP-FAST requires master-keys for two purposes:

- **PAC generation**—ACS generates PACs by using the active master-key. For details about PACs, see About PACs, page B-20.
- **EAP-FAST phase one**—ACS determines whether the PAC that the end-user client presents was generated by one of the master-keys it is aware of.

To increase the security of EAP-FAST, ACS changes the master-key that it uses to generate PACs. ACS uses Master Key Generation Period values that you define to determine when it generates a new master-key and the age of all master-keys.

An active master-key is the master-key used by ACS to generate PACs. The Master Key Generation Period setting determines the duration that a master-key remains active. At any time, only one master-key is active. For more information about how TTL values determine whether PAC refreshing or provisioning is required, see Master Key Generation and PAC TTLs, page B-25.

About PACs

PACs are strong shared secrets that enable ACS and an EAP-FAST end-user client to authenticate each other and establish a TLS tunnel for use in EAP-FAST phase two. ACS generates PACs by using the active master-key and a username.

PAC comprises:

- **PAC-Key**—Shared secret bound to a client (and client device) and server identity.
- **PAC Opaque**—Opaque field that the client caches and passes to the server. The server recovers the PAC-Key and the client identity to mutually authenticate with the client.

- **PAC-Info**—At a minimum, includes the Authority ID to enable the client to cache different PACs. Optionally, it includes other information such as the PACs expiration time.

An EAP-FAST end-user client stores PACs for each user accessing the network with the client. Additionally, a AAA server that supports EAP-FAST has a unique Authority ID. An end-user client associates a user's PACs with the Authority ID of the AAA server that generated them. PACs remove the need for PKI (digital certificates).

During EAP-FAST phase one, the end-user client presents the PAC that it has for the current user and Authority ID that ACS sends at the beginning of the EAP-FAST transaction. The means of providing PACs to end-user clients, known as PAC provisioning, are discussed in Automatic In-Band PAC Provisioning, page B-22 and Manual PAC Provisioning, page B-23.

Modifying the master key generation values does not affect already created PACs. Any modifications you make to the master key generation values specify the period when the next master keys are generated.

Provisioning Modes

ACS supports out-of-band and in-band provisioning modes. The in-band provisioning mode operates inside a TLS tunnel raised by Anonymous DH or Authenticated DH or RSA algorithm for key agreement.

To minimize the risk of exposing the user's credentials, a clear text password should not be used outside of the protected tunnel. Therefore, EAP-MSCHAPv2 or EAP-GTC are used to authenticate the user's credentials within the protected tunnel. The information contained in the PAC is also available for further authentication sessions after the inner EAP method has completed.

EAP-FAST has been enhanced to support an authenticated tunnel (by using the server certificate) inside which PAC provisioning occurs. The new cipher suites that are enhancements to EAP-FAST, and specifically the server certificate, are used.

At the end of a provisioning session that uses an authenticated tunnel, network access can be granted because the server and user have authenticated each other.

ACS supports the following EAP methods inside the tunnel for provisioning:

- EAP-MSCHAPv2
- EAP-GTC

Note By default, when you use EAP-MSCHAP inner methods, ACS allows authentication attempts up to the specified value you configured on the Service page inside the TLS tunnel if the initial authentication attempt fails. After the fourth failed authentication attempt inside the SSL tunnel, ACS terminates the EAP conversation, resulting in a RADIUS Access-Reject.

ACS supports issuing an out-of-band PAC file that allows you to generate a PAC that can be downloaded to ACS.

Types of PACs

ACS supports the following types of PACs:

- Tunnel v1 and v1a
- CTS
- Machine

- Authorization

ACS provisions supplicants with a PAC that contains a shared secret that is used in building a TLS tunnel between the supplicant and ACS. ACS provisions supplicants with PACs that have a wider contextual use.

The following types of PACs are provisioned to ACS, as per server policies:

- **Tunnel/Machine PAC**—Contains user or machine information, but no policy information.
- **User Authorization PAC**—Contains policy elements (for example, inner method used for user authentication). You can use the User Authorization PACs to allow a stateless server session to resume, as described in Session Resume, page B-15.

The various means by which an end-user client can receive PACs are:

- **PAC provisioning**—Required when an end-user client has no PAC. For more information about how master-key and PAC states determine whether PAC provisioning is required, see Master Key Generation and PAC TTLs, page B-25.

  The two supported means of PAC provisioning are:

  - **Automatic In-Band PAC Provisioning**—Sends a PAC by using a secure network connection. For more information, see Automatic In-Band PAC Provisioning, page B-22.
  - **Manual provisioning**—Requires that you use ACS to generate a PAC file for the user, copy the PAC file to the computer that is running the end-user client, and import the PAC file into the end-user client. For more information, see Manual PAC Provisioning, page B-23.
- **PAC refresh**—Occurs based on the value you specify in the Proactive PAC Update When field. For more information about how master-key and PAC states determine whether a PAC is refreshed, see Master Key Generation and PAC TTLs, page B-25.

PACs have the following two states, which the PAC TTL setting determines:

- **Active**—A PAC younger than the PAC TTL is considered active and can be used to complete EAP-FAST phase one.
- **Expired**—A PAC that is older than the PAC TTL is considered expired.At the end of EAP-FAST phase two, ACS generates a new PAC for the user and provides it to the end-user client.

Automatic In-Band PAC Provisioning

Automatic In-Band PAC Provisioning, which is the same as EAP-FAST phase zero, sends a new PAC to an end-user client over a secured network connection. Automatic In-Band PAC Provisioning requires no intervention of the network user or an ACS administrator, provided that you configure ACS and the end-user client to support Automatic In-Band PAC Provisioning.

Note Given that ACS associates each user with a single identity store, the use of Automatic In-Band PAC Provisioning requires that EAP-FAST users be authenticated with an identity store that is compatible with EAP-FAST phase zero. For the databases with which ACS can support EAP-FAST phase zero and phase two, see Authentication Protocol and Identity Store Compatibility, page B-33.

In general, phase zero of EAP-FAST does not authorize network access. In this general case, after the client has successfully performed phase zero PAC provisioning, the client must send a new EAP-FAST request in order to begin a new round of phase one tunnel establishment, followed by phase two authentication.

However, if you choose the Accept Client on Authenticated Provisioning option, ACS sends a RADIUS Access-Accept (that contains an EAP Success) at the end of a successful phase zero PAC provisioning, and the client is not forced to reauthenticate again. This option can be enabled only when the Allow Authenticated In-Band PAC Provisioning option is also enabled.

Note Because transmission of PACs in phase zero is secured by MSCHAPv2 authentication, when MSCHAPv2 is vulnerable to dictionary attacks, we recommend that you limit use of Automatic In-Band PAC Provisioning to initial deployment of EAP-FAST. After a large EAP-FAST deployment, PAC provisioning should be done manually to ensure the highest security for PACs. For more information about manual PAC provisioning, see Manual PAC Provisioning, page B-23.

To control whether ACS performs Automatic In-Band PAC Provisioning, use the options on the Global System Options pages in the System Administration drawer. For more information, see EAP-FAST, page B-18.

Manual PAC Provisioning

Manual PAC provisioning requires an ACS administrator to generate PAC files, which must then be distributed to the applicable network users. Users must configure end-user clients with their PAC files. You can use manual PAC provisioning to control who can use EAP-FAST to access your network. If you disable Automatic In-Band PAC Provisioning, any EAP-FAST user who is not provisioned with a PAC will not be able to access the network. If your ACS deployment includes network segmentation, wherein a separate ACS controls access to each network segment, manual PAC provisioning enables you to grant EAP-FAST access on a per-segment basis. For example, if your company uses EAP-FAST for wireless access in its Chicago and Boston offices and the Cisco Aironet Access Points at each of these two offices are configured to use different ACSs, you can determine, on a per-employee basis, whether Boston employees visiting the Chicago office can have wireless access.

While the administrative overhead of manual PAC provisioning is much greater than that of automatic in-band PAC provisioning, it does not risk sending the PAC over the network. Although manually provisioning the PACs requires a lot of effort early on, in configuring many end-user clients during the initial deployment, this type of provisioning is the most secure means for distributing PACs. We recommend that, after a large EAP-FAST deployment, you manually perform PAC provisioning to ensure the highest security for PACs.

You can generate PAC files for specific usernames. You can also generate a PAC for a machine and provision the PAC manually to the client.

The following parameters are required to create a PAC:

- Specifying whether it is a user or machine PAC.
- Identity stored in Internal Identity Store ID field.
- PAC Time to Live (TTL).
- PAC encryption on or off, and password for encryption.

The PAC could be encrypted with the specified password by using the RC4 or AES algorithm. The detailed decryption algorithm must be provided to the client to allow decryption of the manually received PAC data.

ACS-Supported Features for PACs

ACS 5.1 support these features for PACs.

Machine PAC Authentication

Machine PAC-based authentication allows the machine to gain restricted network access before user authentication.

Proactive PAC Update

ACS proactively provides a new PAC to the client after successful authentication when a configured percentage of the PAC TTL remains. The tunnel PAC update is initiated by the server after the first successful authentication that is performed before the PAC expiration. The proactive PAC update time is configured for the ACS server in the Allowed Protocols Page. This mechanism allows the client to be always updated with a valid PAC.

Note There is no proactive PAC update for Machine and Authorization PACs.

Accept Peer on Authenticated Provisioning

The peer may be authenticated during the provisioning phase.

PAC-Less Authentication

With PAC-less EAP-FAST Authentication, you can run EAP-FAST on ACS without issuing or accepting any tunnel or machine-generated PAC. The secure tunnel may be established by using a certificate rather than a PAC. Some PACs may be long-lived and not updated, which may cause authentication and security problems. When PAC-less EAP-FAST is enabled, requests for PACs are ignored. Authentication begins with EAP-FAST phase zero and all subsequent requests for PACs are ignored. The flow moves on to EAP-FAST phase two. ACS responds with a Success-TLV message, without a PAC. If a client attempts to establish a tunnel with a PAC, ACS responds with a PAC Invalid message. The tunnel establishment does not occur, and an Access-Reject is sent. The host or supplicant can reattempt to connect.

Anonymous phase zero, also known as ADHP is not supported for PAC-less authentication since the protocol does not support rolling over to phase two. PAC-less EAP-Fast supports configuration and does not require a client certificate.

Table B-3 displays the different types of PACs and the authentication and authorization methods you can use them for.

Table B-3 PAC Rules Summary

PAC Type	Tunnel v1/v1a/CTS	Machine	Authorization
Provide PAC on request on provisioning	Yes	Yes	Provide PAC on request on provisioning.
Provide PAC on request on authentication	Yes	Yes	Only if the PAC was not used in this authentication.
Proactive update	Yes	No	No
When PAC is expired	Reject, try to fall on TLS fallback, provide a new PAC after successful authentication only (tunnel PAC).	Reject, try to fall on TLS fallback, provide a new PAC after successful authentication only (machine PAC).	Reject and provide a new PAC after successful authentication only (authorization PAC).
Support ACS 3.x/4.x PACs	For Tunnel PAC v1/v1a only	Yes	No

Related Topics

- About PACs, page B-20
- Provisioning Modes, page B-21
- Types of PACs, page B-21
- Master Key Generation and PAC TTLs, page B-25

Master Key Generation and PAC TTLs

The values for master key generation and PAC TTLs determine their states, as described in About Master-Keys, page B-20 and Types of PACs, page B-21. Master key and PAC states determine whether someone requesting network access with EAP-FAST requires PAC provisioning or PAC refreshing.

Related Topics

- About PACs, page B-20
- Provisioning Modes, page B-21
- Types of PACs, page B-21
- ACS-Supported Features for PACs, page B-23

EAP-FAST Flow in ACS 5.1.

Note You must configure the end-user clients to support EAP-FAST. This procedure is specific to configuring ACS only.

Before You Begin

The steps in this procedure are a suggested order only. Enabling EAP-FAST at your site may require recursion of these steps or performing these steps in a different order. For example, in this procedure, determining how you want to support PAC provisioning comes after configuring a user database to support EAP-FAST; however, choosing Automatic In-Band PAC Provisioning places different limits on user database support.

To enable ACS to perform EAP-FAST authentication:

Step 1 Configure an identity store that supports EAP-FAST authentication. To determine which identity stores support EAP-FAST authentication, see Authentication Protocol and Identity Store Compatibility, page B-33. For information about configuring identity stores, see Chapter 8, "Managing Users and Identity Stores"

Step 2 Determine master key generation and PAC TTL values. For information about how master key generation and PAC TTL values determine whether PAC provisioning or PAC refreshing is required, see Master Key Generation and PAC TTLs, page B-25.

Step 3 Determine whether you want to use automatic or manual PAC provisioning. For more information about the two means of PAC provisioning, see Automatic In-Band PAC Provisioning, page B-22, and Manual PAC Provisioning, page B-23.

Note We recommend that you limit the use of Automatic In-Band PAC Provisioning to initial deployments of EAP-FAST, before you use manual PAC provisioning for adding small numbers of new end-user clients to your network and replacing PACs based on expired master keys.

Step 4 Using the decisions during Step 2 and Step 3, enable EAP-FAST in the Global Systems Options drawer. See EAP-FAST, page B-18 for more information.

ACS is ready to perform EAP-FAST authentication.

Note Inner-identity will not be logged when: `the workstation not allowed` error appears, the SSL Handshake fails, EAP-PAC is provisioned, and ACS receives an invalid PAC.

Related Topics

- Managing Internal Identity Stores, page 8-4
- Managing External Identity Stores, page 8-18

EAP-FAST PAC Management

The EAP-FAST master-key in ACS is used to encrypt or decrypt, sign and authenticate the PACs and PAC-Opaque's that are used by EAP-FAST to store server opaque data by a supplicant. EAP-FAST requires a distributed mechanism by which each server in the ACS domain is able to pack and unpack PACs securely, including those which were packed on a different server.

The EAP-FAST master-key must have a common secret that is known to all servers in the ACS domain. The master-key is periodically refreshed and keys are replaced securely and synchronized by all ACS servers. The keys are generated of high entropy to comply with strong cryptographic standards such as FIPS-140.

In previous versions of ACS, the master-key was distributed by the ACS distribution mechanism and was replaced from time to time to improve the security of those keys. ACS 5.1 introduces a new scheme that provides simplicity, correctness, robustness, and security for master -key distribution.

The ACS EAP-FAST new distribution scheme contains a secure way of distributing the common seed-key, from which each ACS server can deterministically derive the same set of master-keys. Each PAC contains the information that the master-key was derived from, and each server can securely reconstruct the master-key that encrypted and signed the PAC.

This scheme improves the security by reducing the amount of cryptographic sensitive material that is transmitted.

This section contains the following topics:

- Key Distribution Algorithm, page B-27
- EAP-FAST PAC-Opaque Packing and Unpacking, page B-27
- Revocation Method, page B-27
- PAC Migration from ACS 4.x, page B-27

Key Distribution Algorithm

The common seed-key is a relatively large and a completely random buffer that is generated by the primary ACS server. The seed-key is generated only once during installation, or it can be manually regenerated by an administrator. The seed-key should rarely be replaced, because if you change seed-key, of all the previous master-keys and PACs would automatically be deactivated.

The seed-key is generated by using a FIPS approved RNG generator that exists in the runtime cryptographic module (CryptoLib). The ACS primary server management determines when to generate the seed-key, and communicates with the ACS runtime to request a new seed-key to be generated.

The size of the seed-key may vary and should consist of at least 64 bytes (512 bit). A larger seed might have some performance implication as each master-key derivation is dependant on it subsequently.

At any given time, a single seed-key should be used by each ACS server and the primary ACS server should ensure to distribute the latest seed-key to all the servers. Old seed-keys must discarded.

The seed-key contains critical cryptographic sensitive information. Disclosing the seed-key information would expose the entire EAP-FAST PAC mechanism to a large set of possible identity vulnerabilities. Due to that, the mechanism which transports the seed-key between the primary and the secondary ACS servers must be fully secured. Further security measures must be taken with respect to storing the seed-key in the data-base. The seed-key should be protected with the strongest means of security.

EAP-FAST PAC-Opaque Packing and Unpacking

When the server generates a new PAC, it must derive the master-key to be used. When the server accepts a new PAC the same algorithm should be used for deriving the master-key with some additional verification used to prevent possible attacks on the master-key scheme. The derivation calculation may be skipped if the master-key was already placed in the cache in the past.

Revocation Method

You can revoke all PACs and all Master-Keys. For this type of extensive revocation, all you need to do is to revoke the seed-key and replace it by a new one.

Having only a single seed-key to be used in the system facilitates implementation.

PAC Migration from ACS 4.x

Although the configuration can be migrated from 4.x, the PACs themselves, as being stored only in supplicants, may still be issued from versions as far back as ACS 3.x. ACS 5.1 accepts PACs of all types according to migrated master-keys from versions 4.x and onwards, and re-issues a new 5.0 PAC, similar to the proactive PAC update for EAP-FAST 5.0.

When ACS 5.1, accepts a PAC from either ACS 3.x or 4.x, it decrypts and authenticates the PAC according to the 4.x master-key that was migrated from ACS 4.x configuration. The decryption and handling of this type of PAC is similar to the way the ACS 4.x PAC was handled.

The migration process involves converting the following data-items:

- EAP-FAST A-ID of ACS (Authority ID). The parameter replaces the deployment's A-ID of ACS 5.1.
- A list of retired ACS 4.x master-keys. The list is taken from the ACS 4.x configuration and placed in a new table in ACS 5.1. Each migrated master-key is associated with its expected time of expiration. The table is migrated along with the master-key identifier (index) and the PAC's-cipher assigned to each key.

EAP-MSCHAPv2

Microsoft Challenge Handshake Authentication Protocol (MSCHAP v2) provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server that it is dialing in to has access to the user's password.

This section contains the following topics:

- Overview of EAP-MSCHAPv2, page B-28
- EAP- MSCHAPv2 Flow in ACS 5.1, page B-29

Overview of EAP-MSCHAPv2

Some of the specific members of the EAP family of authentication protocols, specifically EAP-FAST and PEAP, support the notion of an “EAP inner method.” This means that another EAP-based protocol performs additional authentication within the context of the first protocol, which is known as the "EAP outer method."

One of the inner methods supported by the EAP-FAST and PEAP outer methods is EAP-MSCHAPv2, which is an adaptation of the MSCHAPv2 protocol that complies with the general framework established by EAP.

Using EAP-MSCHAPv2 as the inner EAP method facilitates the reuse of Microsoft directory technology (such as Windows Active Directory), with the associated database of user credentials for wireless authentication in the following contexts:

- MSCHAPv2 for User Authentication, page B-28
- MSCHAPv2 for Change Password, page B-28
- Windows Machine Authentication Against AD, page B-29

MSCHAPv2 for User Authentication

ACS supports the EAP-MSCHAPv2 authentication protocol as the inner method of EAP-FAST and PEAP. The protocol is an encapsulation of MSCHAPv2 into the EAP framework. Mutual authentication occurs against the configured credential database. The client does not send its password, but a cryptographic function of the password. Using EAP-MSCHAPv2 as the inner method of tunneling protocols, increases protection of secured communication. Every protocol message is encrypted inside the tunnel and server, and client challenges are not generated randomly but, derived from outer method cryptographic material.

EAP-MSCHAPv2 is supported for AD and the ACS internal identity store.

MSCHAPv2 for Change Password

When you use EAP-MSCHAPv2 (as an EAP inner method) to authenticate a user whose password has expired, ACS sends a specific EAP-MSCHAPv2 failure notification to the client. The client can prompt the user for new password and then provide it to ACS inside the same conversation. The new password is encrypted with the help of the old one. When a user password is changed successfully, the new user password is stored in the credential database.

EAP-MSCHAPv2 change password is supported for AD and ACS internal identity store.

Windows Machine Authentication Against AD

EAP-MSCHAPv2 can be used for machine authentication. EAP-MSCHAPv2 Windows machine authentication is the same as user authentication. The difference is that you must use the Active Directory of a Windows domain, since a machine password can be generated automatically on the machine and the AD, as a function of time and other parameters. The password generated cannot be stored in other types of credential databases.

EAP- MSCHAPv2 Flow in ACS 5.1

Components involved in the 802.1x and MSCHAPv2 authentication process are the:

- Host—The end entity, or end user's machine.
- AAA client—The network access point.
- Authentication server—ACS.

The MSCHAPv2 protocol is described in RFC 2759.

Related Topic

- Authentication Protocol and Identity Store Compatibility, page B-33

CHAP

CHAP uses a challenge-response mechanism with one-way encryption on the response. CHAP enables ACS 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 ACS internal database for authentication, you can use PAP or CHAP. CHAP does not work with the Windows 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.

LEAP

ACS currently uses 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 EAP-TLS, we recommend that you disable this option.

Note If users who access your network by using a AAA client that is defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, then you must enable LEAP, EAP-TLS, or both; otherwise, Cisco Aironet users cannot authenticate.

Certificate Attributes

ACS parses the following client certificate's attributes:

- Certificate serial-number (in binary format)
- Encoded certificate (in binary DER format)
- Subject's CN attribute
- Subject's O attribute (Organization)
- Subject's OU attribute (Organization Unit)
- Subject's L attribute (Location)
- Subject's C attribute (Country)
- Subject's ST attribute (State Province)
- Subject's E attribute (eMail)
- Subject's SN attribute (Subject Serial Number)
- SAN (Subject Alternative Name)

You can define a policy to set the principle username to use in the TLS conversation, as an attribute that is taken from the received certificate.

The attributes that can be used as the principle username are:

- Subject CN
- Subject Serial-Number (SN)
- SAN
- Subject
- SAN—email
- SAN—DNS
- SAN—otherName

If the certificate does not contain the configured attribute, authentication fails.

Note ACS 5.1 supports short hard-coded attributes and certificate attribute verification for the only the EAP-TLS protocol.

Certificate Binary Comparison

You can perform binary comparison against a certificate that ACS receives from an external identity store and determine the identity store's parameters that will be used for the comparison.

Note In ACS 5.1, LDAP is the only external identity store that holds certificates.

ACS uses the configured principle username to query for the user's certificate and then perform binary comparison between the certificate received from external identity store and the one received from the client. The comparison is performed on a DER certificate format.

Rules Relating to Textual Attributes

ACS collects client certificate textual attributes and places them in the ACS context dictionary. ACS can apply any rule based policy on these attributes as with any rule attributes in ACS.

The attribute that can be used for rule verification are:

- Subject's CN attribute
- Subject's O attribute (Organization)
- Subject's OU attribute (Organization Unit)
- Subject's L attribute (Location)
- Subject's C attribute (Country)
- Subject's ST attribute (State Province)
- Subject's E attribute (eMail)
- Subject's SN attribute (Subject Serial Number)
- SAN (Subject Alternative Name)
- Subject Serial-Number (SN)
- SAN
- Subject
- SAN—DNS
- SAN—otherName

Certificate Revocation

Every client certificate that ACS receives is verified with a Certificate Revocation List (CRL) according to a policy that is defined.

The CRL mechanism verifies whether or not you can still rely on a client certificate. This is done by checking the serial number of the certificate, and that of each member of the corresponding certificate chain, against a list of certificates that are known to have been revoked. Possible reasons for revocation of a certificate include suspicion that the associated private key has been compromised or the realization that the certificate was issued improperly. If either of these conditions exist, the certificate is rejected.

ACS supports a static-CRL that contains a list of URLs used to acquire the CRL files that are configured in ACS database.

You can configure a set of URLs used for CRL update for each trusted CA certificate,. By default, when adding a CA certificate, ACS automatically sets all the URLs stored in the certificate *crlDistributionPoint* as the initial static CRL for that CA. In most cases, the *crlDistributionPoint* is used to point to the CRL location used to revoke the CA certificate, but you can edit the URL to point to the CRL file issued by this CA. You can only configure a single HTTP based URL for each CA.

You can configure the parameters for each CA, which will apply to all the URLs that are configured to the CA. ACS supports two download modes, one for periodic download, and the other for downloading the next CRL update just before the previous is about to expire. For the periodic download, you can define the download periods. For automatic downloading, you define the amount of time before the CRL file expires, should ACS download it. The CRL expiration time is taken from the *CRL nextUpdate* field. For both modes, if the download somehow fails, you can define the amount of time that ACS will wait before trying to redownload the CRL file.

ACS verifies that the downloaded CRL file is signed correctly by any one of the CAs in the trust store, for each downloaded CRL file and whether they are trusted. ACS uses the CRL file only if the signature verification passes. The verified CRL file replaces the previous CRL file issued by the same CA.

Note CRL files are not kept persistent, and should be re-downloaded when you restart ACS.

The configuration of URLs and their association to CA's is distributed to the entire ACS domain. The downloaded CRLs are not distributed and are autonomously populated in parallel in each ACS server.

Machine Authentication

ACS supports the authentication of computers that are running the Microsoft Windows operating systems that support EAP computer authentication. Machine authentication, also called computer authentication, allows networks services only for computers known to Active Directory. This feature is especially useful for wireless networks, where unauthorized users outside the physical premises of your workplace can access your wireless access points.

When machine authentication is enabled, there are three different types of authentications. When starting a computer, the authentications occur in this order:

- **Machine authentication**—ACS authenticates the computer prior to user authentication. ACS checks the credentials that the computer provides against the Windows identity store. If you use Active Directory and the matching computer account in AD has the same credentials, the computer gains access to Windows domain services.
- **User domain authentication**—If machine authentication succeeded, the Windows domain authenticates the user. If machine authentication failed, the computer does not have access to Windows domain services and the user credentials are authenticated by using cached credentials that the local operating system retains. In this case, the user can log in to only the local system. When a user is authenticated by cached credentials, instead of the domain, the computer does not enforce domain policies, such as running login scripts that the domain dictates.

Tip If a computer fails machine authentication and the user has not successfully logged in to the domain by using the computer since the most recent user password change, the cached credentials on the computer will not match the new password. Instead, the cached credentials will match an older password of the user, provided that the user once successfully logged in to the domain from this computer.

- **User network authentication**—ACS authenticates the user, allowing the user to have network connectivity. If the user exists, the identity store that is specified is used to authenticate the user. While the identity store is not required to be the Windows identity store, most Microsoft clients can be configured to automatically perform network authentication by using the same credentials used for user domain authentication. This method allows for a single sign-on.

Note Microsoft PEAP clients may also initiate machine authentication whenever a user logs off. This feature prepares the network connection for the next user login. Microsoft PEAP clients may also initiate machine authentication when a user shuts down or restarts the computer rather than just logging off.

ACS supports EAP-TLS, EAP-FAST, PEAP (EAP-MSCHAPv2), and PEAP (EAP-GTC) for machine authentication. You can enable each separately on the Active Directory: General Page, which allows a mix of computers that authenticate with EAP-TLS, EAP-FAST, or PEAP (EAP-MSCHAPv2). Microsoft operating systems that perform machine authentication might limit the user authentication protocol to the same protocol that is used for machine authentication.

Related Topics

- Microsoft AD, page 8-38
- Managing External Identity Stores, page 8-18

Authentication Protocol and Identity Store Compatibility

ACS supports various authentication protocols to authenticate against the supported identity stores.

Table B-4 specifies non-EAP authentication protocol support.

Table B-4 Non-EAP Authentication Protocol and User Database Compatibility

Identity Store	ASCII/PAP	MSCHAPv1/MSCHAPv2	CHAP
ACS	Yes	Yes	Yes
Windows AD	Yes	Yes	No
LDAP	Yes	No	No
RSA Identity Store	Yes	No	No
RADIUS Identity Store	Yes	No	No

Table B-5 specifies EAP authentication protocol support.

Table B-5 EAP Authentication Protocol and User Database Compatibility

Identity Store	EAP-MD5	EAP-TLS[1]	PEAP EAP-MSCHAPv2	EAP-FAST MSCHAPv2	PEAP-GTC	EAP-FAST-GTC
ACS	Yes	No	Yes	Yes	Yes	Yes
Windows AD	No	Yes	Yes	Yes	Yes	Yes
LDAP	No	Yes	No	No	Yes	Yes
RSA Identity Store	No	No	No	No	Yes	Yes
RADIUS Identity Store	No	No	No	No	Yes	Yes

1. In EAP-TLS authentication, the user is authenticated by cryptographic validation of the certificate. Additionally, ACS 5.1 optionally allows a binary comparison of the user's certificate sent by the end-user client against the certificate located in the user's record in the LDAP identity store.

GLOSSARY

A

AAA — Authentication, authorization, and accounting (AAA) is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security. A system in IP-based networking to control what computer resources users have access to and to keep track of the activity of users over a network.

AAA client IP address — An IP address of the AAA client, used to configure the AAA client in Access Control Server (ACS) to interact with the network device. To represent multiple network devices, specify multiple IP addresses. Separate each IP address by pressing **Enter**.

AAA server — A server program that handles user requests for access to computer resources and, for an enterprise, provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information. The current standard by which devices or applications communicate with an AAA server is the Remote Authentication Dial-In User Service (RADIUS).

access — The capability to get to what you need. Data access is being able to get to (usually having permission to use) particular data on a computer.

Access Control — Ensures that resources are only granted to those users who are entitled to them.

Access Control List (ACL) — A mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource.

Access Control System (ACS) — A AAA server that performs authentication, authorization, and accounting to manage devices in a network.

Access Control Service — A security service that provides protection of system resources against unauthorized access. The two basic mechanisms for implementing this service are ACLs and tickets.

AP — access point. The Hub of a wireless network. Wireless clients connect to the access point, and traffic between two clients must travel through the access point.

access policies — The policies that limit access to the ACS web interface by IP address, TCP port range, and secure socket layer (SSL).

AR — access registrar . A RADIUS-compliant, access policy server designed to support the delivery of dial, ISDN, and new services including DSL, cable with telco-return, wireless and Voice over IP

ADR — accessibility design requirements. Provides detail on how to design accessible products, web sites, and documentations

accounts The capability of ACS to record user sessions in a log file.

ACS System Administrators Administrators with different access privileges defined under the System Configuration section of the ACS web interface. They administer and manage ACS deployments in your network.

ARP address resolution protocol. A protocol for mapping an Internet Protocol address to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

AES advanced encryption standard. A Federal Information Processing Standard (FIPS) Publication that will specify a cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. This standard specifies Rijndael as a FIPS-approved symmetric encryption algorithm that may be used by U.S. Government organizations (and others) to protect sensitive information.

anonymous (LDAP) An LDAP session is described as anonymous if no user DN or secret is supplied when initiating the session (sending the bind).

anti-virus A software program designed to identify and remove a known or potential computer virus

API application program interface. The specific methodology by which a programmer writing an application program may make requests of the operating system or another application.

applet Java programs; an application program that uses the client's web browser to provide a user interface.

ARP Address Resolution Protocol. A protocol used to obtain the physical addresses (such as MAC addresses) of hardware units in a network environment. A host obtains such a physical address by broadcasting an ARP request, which contains the IP address of the target hardware unit. If the request finds a unit with that IP address, the unit replies with its physical hardware address.

ARPANET Advanced Research Projects Agency Network. A pioneer packet-switched network that was built in the early 1970s under contract to the US Government, led to the development of today's Internet, and was decommissioned in June 1990.

Asymmetrical Key Exchange Asymmetric or public key cryptography is based on the concept of a key pair. Each half of the pair (one key) can encrypt information so that only the other half (the other key) can decrypt it. One part of the key pair, the private key, is known only by the designated owner; the other part, the public key, is published widely but is still associated with the owner.

attribute (LDAP) The data in an entry is contained in attribute-value pairs. Each attribute has a name (and sometimes a short form of the name) and belongs to an objectClass. The attributes characteristics are fully described by an ASN.1 definition. One or more objectClasses may be included in a Schema. Depending on the ASN.1 definition of the attribute there can be more that one attribute-value pair of the same named attribute in an entry. One (or more) attribute(s), the naming attribute or RDN will always uniquely identify an entry.

auditing The information gathering and analysis of assets to ensure such things as policy compliance and security from vulnerabilities.

authenticated (LDAP) A session is described as authenticated if a user DN and secret is supplied when initiating the session (sending the bind).

authentication The process of confirming the correctness of the claimed identity.

authenticity The validity and conformance of the original information.

authorization The approval, permission, or empowerment for someone or something to do something.

authorization profile The basic "permissions container" for a RADIUS-based network access service. The authorization profile is where you define all permissions to be granted for a network access request. VLANs, ACLs, URL redirects, session timeout or reauthorization timers, or any other RADIUS attributes to be returned in a response are defined in the authorization profile.

B

basic authentication The simplest web-based authentication scheme that works by sending the username and password with each request.

BIND Berkeley Internet Name Domain. An implementation of DNS. DNS is used for domain name to IP address resolution.

bind (LDAP) When connection is made to an LDAP server the first operation of the sequence is called a bind. The bind operation sends the dn of the entry that will be used for authentication and the password to be used. In the case of an anonymous bind both values will be NULL.

block cipher Encrypts one block of data at a time.

bridge A product that connects a local area network (LAN) to another local area network that uses the same protocol (for example, Ethernet or token ring).

broadcast To simultaneously send the same message to multiple recipients. One host to all hosts on network.

broadcast address An address used to broadcast a datagram to all hosts on a given network using UDP or ICMP protocol.

browser A client computer program that can retrieve and display information from servers on the World Wide Web.

C

CA Signature A digital code that vouches for the authenticity of a digital certificate. The CA signature is provided by the certificate authority (CA) that issued the certificate.

cache A special high-speed storage mechanism. It can be either a reserved section of main memory or an independent high-speed storage device. Two types of caching are commonly used in personal computers: memory caching and disk caching.

CSS cascading style sheet. A Web page derived from multiple sources with a defined order of precedence where the definitions of any style element conflict.

CA certificate authority. An authority in a network that issues and manages security credentials and public keys for message encryption and decryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

certificate-based authentication The use of Secure Sockets Layer (SSL) and certificates to authenticate and encrypt HTTP traffic.

certificate Digital representation of user or device attributes, including a public key, that is signed with an authoritative private key.

CGI common gateway interface. This mechanism is used by HTTP servers (web servers) to pass parameters to executable scripts in order to generate responses dynamically.

CHAP Challenge-Handshake Authentication Protocol. A protocol that uses a challenge/response authentication mechanism where the response varies every challenge to prevent replay attacks.

CHAP is an authentication technique where after a link is established, a server sends a challenge to the requestor. The requestor responds with a value obtained by using a one-way hash function. The server checks the response by comparing it its own calculation of the expected hash value. If the values match, the authentication is acknowledged otherwise the connection is usually terminated.

challenge-response A common authentication technique whereby an individual is prompted (the challenge) to provide some private information (the response). Most security systems that rely on smart cards are based on challenge-response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.

checksum A value that is computed by a function that is dependent on the contents of a data object and is stored or transmitted together with the object, for the purpose of detecting changes in the data.

cipher A cryptographic algorithm for Encryption and Decryption. The method used to transform a readable message (called plaintext or cleartext) into an unreadable, scrambled, or hidden message (called ciphertext).

ciphertext The encrypted form of the message being sent. Ciphertext is data that has been encrypted. It is the output of the encryption process and can be transformed back into a readable form (plaintext) with the appropriate decryption key.

client A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

client/server Describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfills the request. Although the client/server idea can be used by programs within a single computer, it is a more important idea in a network. In a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations.

collision Occurs when multiple systems transmit simultaneously on the same wire.

command sets Contains a set of permitted commands for TACACS+ based, per-command authorization.

community string A character string used to identify valid sources for Simple Network Management Protocol (SNMP) requests, and to limit the scope of accessible information. Ravlin units use a community string, such as a password, allowing only a limited set of management stations to access its MIB.

computer network A collection of host computers together with the sub-network or inter-network through which they can exchange data.

confidentiality The need to ensure that information is disclosed only to those who are authorized to view it.

configuration management	The process of establishing a known baseline condition and managing it.
cookie	Data exchanged between an HTTP server and a browser (a client of the server) to store state information on the client side and retrieve it later for server use. An HTTP server, when sending data to a client, may send along a cookie, which the client retains after the HTTP connection closes. A server can use this mechanism to maintain persistent client-side state information for HTTP-based applications, retrieving the state information in later connections.
corruption	A threat action that undesirably alters system operation by adversely modifying system functions or data.
CoS	Class of Service. A way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority.
countermeasure	Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected. Intrusion Prevention Systems (IPS) commonly employ countermeasures to prevent intruders form gaining further access to a computer network. Other counter measures are patches, access control lists and malware filters.
covert channels	The means by which information can be communicated between two parties in a covert fashion using normal system operations. For example by changing the amount of hard drive space that is available on a file server can be used to communicate information.
CRL	certificate revocation list. A list of certificates (more accurately: their serial numbers) which have been revoked, are no longer valid, and should not be relied upon by any system user.
CRUD	Create, read, update and delete. The basic management operations that are performed on managed data
cryptanalysis	The mathematical science that deals with analysis of a cryptographic system in order to gain knowledge needed to break or circumvent the protection that the system is designed to provide. In other words, convert the cipher text to plaintext without knowing the key.
cryptographic algorithm or hash	An algorithm that employs the science of Cryptography, including Encryption algorithms, Cryptographic Algorithm or Hash, Digital Signature Algorithm (DSA), and key agreement algorithms.
cryptography	Garbles a message in such a way that anyone who intercepts the message cannot understand it.
CSV	comma-separated value. This file format is a delimited data format that has fields separated by the comma character and records separated by new lines.
CTS	Cisco Trusted Security
CUE	Common User Experience
cut-through	A method of switching where only the header of a packet is read before it is forwarded to its destination.
CRC	Cyclic Redundancy Check. Sometimes called "cyclic redundancy code." A type of checksum algorithm that is not a cryptographic hash but is used to implement data integrity service where accidental changes to data are expected.

D

daemon A program which is often started at the time the system boots and runs continuously without intervention from any of the users on the system. The daemon program forwards the requests to other programs (or processes) as appropriate. The term daemon is a Unix term, though many other operating systems provide support for daemons, though they're sometimes called other names. Windows, for example, refers to daemons and System Agents and services.

DES Data Encryption Standard. A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.

datagram Request for Comment 1594 says, "a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network." The term has been generally replaced by the term packet. Datagrams or packets are the message units that the Internet Protocol deals with and that the Internet transports. A datagram or packet needs to be self-contained without reliance on earlier exchanges because there is no connection of fixed duration between the two communicating points as there is, for example, in most voice telephone conversations. (This kind of protocol is referred to as connectionless.)

decapsulation The process of stripping off one layer's headers and passing the rest of the packet up to the next higher layer on the protocol stack.

decryption The process of transforming an encrypted message into its original plaintext.

denial of service The prevention of authorized access to a system resource or the delaying of system operations and functions.

device administration Capability to control and audit the administration operations performed on network devices. The network device administrator role has full access to perform the administrative operations on network devices.

dictionaries A store to configure attributes of RADIUS and TACACS+ protocols, internal users, and internal hosts.

dictionary attack An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

Diffie-Hellman A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman. Diffie-Hellman does key establishment, not encryption. However, the key that it produces may be used for encryption, for further key management operations, or for any other cryptography.

Digest Authentication Allows a web client to compute MD5 hashes of the password to prove it has the password.

digital certificate An electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real.

digital envelope An encrypted message with the encrypted session key.

digital signature A hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

DSA digital signature algorithm. An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

(DSS Digital Signature Standard. The US Government standard that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography.

disassembly The process of taking a binary program and deriving the source code from it.

disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.

DIT directory information tree (also known as the naming context). The hierarchy of objects that make up the local directory structure. More than one DIT may be supported by an LDAP server. The Root DSE will provide this information.

DN Distinguished Name. A DN is comprised of a series of RDNs that uniquely describe the naming attributes on the path UP the DIT from the required entry to the directory root. A DN is written LEFT to RIGHT and looks something like this:

domain A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

domain name Locates an organization or other entity on the Internet. For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a particular host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.

DNS Domain Name System. The way that Internet domain names are located and translated into IP addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

DSA Directory System Agent X.500 term for any DAP or LDAP enabled directory service e.g. an LDAP server.

DSE DSA Specific Entry An entry in a local directory server.

due diligence The requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

dumpsec A security tool that dumps a variety of information about a system's users, file system, registry, permissions, password policy, and services.

DLL Dynamic Link Library. A collection of small programs, any of which can be called when needed by a larger program that is running in the computer. The small program that lets the larger program communicate with a specific device such as a printer or scanner is often packaged as a DLL program (usually referred to as a DLL file).

E

eavesdropping Listening to a private conversation which may reveal information which can provide access to a facility or network.

Egress Filtering Filtering outbound traffic.

encapsulation The inclusion of one data structure within another structure so that the first data structure is hidden for the time being.

encryption Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.

entry (LDAP) The name given to a stored object in a LDAP enabled directory. Each entry has one parent entry (object) and zero or more child entries (objects). The data content of an entry consist of one or more attributes one (or more) of which is (are) used as the naming attribute (more correctly the RDN) to uniquely identify this object in the DIT.

equality (LDAP) Equality defines the comparison rule of an attribute when used in a search filter that contains no wildcards, and both the content and length must be exactly the same. When wildcards are used, this is called a substring and the SUBSTR rule is used.

external identity store External databases that ACS accesses to perform credential and authentication validations for internal and external users (as defined by you within a policy).

Ethernet The most widely-installed LAN technology. Specified in a standard, IEEE 802.3, an Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Devices are connected to the cable and compete for access using a CSMA/CD protocol.

event An observable occurrence in a system or network.

Exponential Backoff Algorithm Used to adjust TCP timeout values on the fly so that network devices don't continue to timeout sending data over saturated links.

exposure A threat action whereby sensitive data is directly released to an unauthorized entity.

extended ACLs A more powerful form of standard ACLs on Cisco routers. They can make filtering decisions based on IP addresses (source or destination), Ports (source or destination), protocols, and whether a session is established.

EAP Extensible Authentication Protocol. A protocol for wireless networks that expands on Authentication methods used by the PPP (Point-to-Point Protocol), a protocol often used when connecting a computer to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and Public Key Encryption authentication.

EAP-MD5 Extensible Authentication Protocol-Message Digest 5. An EAP security algorithm developed by RSA Security that uses a 128-bit generated number string, or hash, to verify the authenticity of a data communication.

EAP-TLS Extensible Authentication Protocol-Translation Layer Security. A high-security version of EAP that requires authentication from both the client and the server. If one of them fails to offer the appropriate authenticator, the connection is terminated. Used to create a secured connection for 802.1X by preinstalling a digital certificate on the client computer. EAP-TLS is the protocol that serves for mutual authentication and integrity-protected cipher suite negotiation and key exchange between a client and server. Both the client and the server use X.509 certificates to verify their identities to each other.

F

false rejects When an authentication system fails to recognize a valid user.

FTP File Transfer Protocol . A TCP/IP protocol specifying the transfer of text or binary files across the network.

filter Used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

filtering router An inter-network router that selectively prevents the passage of data packets according to a security policy. A filtering router may be used as a firewall or part of a firewall. A router usually receives a packet from a network and decides where to forward it on a second network. A filtering router does the same, but first decides whether the packet should be forwarded at all, according to some security policy. The policy is implemented by rules (packet filters) loaded into the router.

firewall A TCP/IP Fragmentation Attack that is possible because IP allows packets to be broken down into fragments for more efficient transport across various media. The TCP packet (and its header) are carried in the IP packet. In this attack the second fragment contains incorrect offset. When packet is reconstructed, the port number will be overwritten.

fragmentation The process of storing a data file in several "chunks" or fragments rather than in a single contiguous sequence of bits in one place on the storage medium.

frames Data that is transmitted between network points as a unit complete with addressing and necessary protocol control information. A frame is usually transmitted serial bit by bit and contains a header field and a trailer field that "frame" the data. (Some control frames contain no data.)

full duplex A type of duplex communications channel which carries data in both directions at once. Refers to the transmission of data in two directions simultaneously. Communications in which both sender and receiver can send at the same time.

fully-qualified domain name A server name with a hostname followed by the full domain name.

G

gateway A network point that acts as an entrance to another network.

global system options Configuring TACACS+, EAP-TTLS, PEAP, and EAP-FAST runtime characteristics and generating EAP-FAST PAC.

H

hash functions Used to generate a one way "check sum" for a larger text, which is not trivially reversed. The result of this hash function can be used to validate if a larger file has been altered, without having to compare the larger files to each other. Frequently used hash functions are MD5 and SHA1.

header The extra information in a packet that is needed for the protocol stack to process the packet.

host Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

Host-Based ID Host-based intrusion detection systems use information from the operating system audit records to watch all operations occurring on the host that the intrusion detection software has been installed upon. These operations are then compared with a pre-defined security policy. This analysis of the audit trail imposes potentially significant overhead requirements on the system because of the increased amount of processing power which must be utilized by the intrusion detection system. Depending on the size of the audit trail and the processing ability of the system, the review of audit data could result in the loss of a real-time analysis capability.

HTTPS Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL. HTTPS is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. When used in the first part of a URL (the part that precedes the colon and specifies an access scheme or protocol), this term specifies the use of HTTP enhanced by a security mechanism, which is usually SSL.HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP and an additional encryption/authentication layer between HTTP and TCP.

hub A network device that operates by repeating data that it receives on one port to all the other ports. As a result, data transmitted by one host is retransmitted to all other hosts on the hub. The central device in a star network, whether wired or wireless. Wireless access points act as hubs in wireless networks.

hybrid attack Builds on the dictionary attack method by adding numerals and symbols to dictionary words.

hybrid encryption An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

(HTML Hypertext Markup Language. The set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page.

(HTTP Hypertext Transfer Protocol. The protocol in the Internet Protocol (IP) family used to transport hypertext documents across an internet.

I

I18N Internationalization and localization are means of adapting software for non-native environments, especially other nations and cultures. Internationalization is the adaptation of products for potential use virtually everywhere, while localization is the addition of special features for use in a specific locale.

identity Whom someone or what something is, for example, the name by which something is known.

identity groups A logical entity that is associated with all types of users and hosts.

incremental backup A scheduled job that allows users to take smaller, periodic backups of the Monitoring & Report Viewer database.

integrity The need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

internal identity store A database that contains the internal user attributes and credential information used to authenticate internal users and hosts.

IETF Internet Engineering Task Force . The body that defines standard Internet operating protocols such as TCP/IP. The IETF is supervised by the Internet Society Internet Architecture Board (IAB). IETF members are drawn from the Internet Society's individual and organization membership.

(IP Internet Protocol. The method or protocol by which data is sent from one computer to another on the Internet.

IPsec Internet Protocol Security. A developing standard for security at the network or packet processing layer of network communication.

Interrupt A signal that informs the OS that something has occurred.

intrusion detection A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Internet Protocol. The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP address A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP flood A denial of service attack that sends a host more echo request ("ping") packets than the protocol implementation can handle.

IP forwarding An Operating System option that allows a host to act as a router. A system that has more than 1 network interface card must have IP forwarding turned on in order for the system to be able to act as a router.

IP poofing The technique of supplying a false IP address.

ISO International Organization for Standardization, a voluntary, non-treaty, non-government organization, established in 1947, with voting members that are designated standards bodies of participating nations and non-voting observer organizations.

ISP Internet Service Provider. A business or organization that provides to consumers access to the Internet and related services. In the past, most ISPs were run by the phone companies.

J

JRE Java Runtime Environment. A software bundle that allows a computer system to run a Java application.

K

Kerberos A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.

key In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.

L

Layer 2 Forwarding Protocol (L2F) An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user.

Layer 2 Tunneling Protocol (L2TP) An extension of the Point-to-Point Tunneling Protocol used by an Internet service provider to enable the operation of a virtual private network over the Internet.

LDAP client LDAP Client describes a piece of software that provides access to an LDAP sever. Most standard web browsers provide limited LDAP client capabilities using LDAP URLs. LDAP browsers and web interfaces are both very common examples of LDAP clients. List of Open Source Clients.

Lightweight Directory Access Protocol (LDAP) LDAP is a networking protocol for querying and modifying directory services running over TCP/IP The LDAP protocol is used to locate organizations, individuals, and other resources such as files and devices in a network, on the public Internet or on a corporate Intranet.

Local Operations (secondary servers only) The operations performed to register or deregister a secondary server, or to replicate a secondary server and a request for a local mode from the Join a Distributed System page.

Log Configuration A system that uses logging categories and maintenance parameters that enable you to configure and store the logs generated for accounting messages, AAA audit and diagnostics messages, system diagnostics messages, and administrative audit messages.

M

MAC Address — A physical address; a numeric value that uniquely identifies that network device from every other device on the planet.

matchingRule (LDAP) — The method by which an attribute is compared in a search operation. A matchingRule is an ASN.1 definition that usually contains an OID a name (for example, caseIgnoreMatch [OID = 2.5.13.2]), and the data type it operates on (for example, DirectoryString).

MD5 — A one way cryptographic hash function.

MIB (Management Information Base) — A MIB is a formal description of a set of network objects that can be managed using SNMP (Simple Network Management Protocol).

monitoring and reports — In the ACS web interface, a drawer that contains the monitoring, reporting, and troubleshooting options.

MPPE Microsoft Point-to-Point Encryption — A protocol for encrypting data across PPP (Point-to-Point Protocol) and Virtual Private Network links.

N

name space (LDAP) — Term used to describe all DNs that lie in (or are contained within or bounded by) a given directory information tree (DIT). If the DIT root is dc=example,dc=com, then cn=people,dc=example,dc=com is said to lie in the name space but ou=people,dc=example,dc=net does not; it lies in the dc=example,dc=net name space.

naming attribute (LDAP) — A unique identifier for each entry in the directory information tree (DIT). Also known as the Relative Distinguished Name (RDN).

naming context (LDAP) — A a unique name space starting from (and including) the root Distinguished Name (DN). Also known as namingContext or directory information tree (DIT).

NAS (Network Access Server) — A single point of access to a remote resource. The NAS is meant to act as a gateway to guard access to a protected resource. This can be anything from a telephone network, to printers, to the Internet.

network device groups — A logical grouping of network devices by location and type.

network resources — A drawer that defines all network devices in the device repository that access the ACS network, including Network Device Groups (NDGs), network devices, AAA clients,, and external policy servers.

P

PAP (Password Authentication Protocol.) — PAP is a simple authentication protocol used to authenticate a user to a remote access server or Internet service provider(ISP).

PI (Programmatic Interface) The ACS PI is a programmatic interface that provides external applications the ability to communicate with ACS to configure and operate ACS; this includes performing the following operations on ACS objects: create, update, delete and read.

policy condition Rule-based single conditions that are based on policies, which are sets of rules used to evaluate an access request and return a decision.

policy element Global, shared object that defines policy conditions (for example, time and date, or custom conditions based on user-selected attributes) and permissions (for example, authorization profiles). Policy elements are referenced when you create policy rules.

port setting You can configure ACS to authenticate using different LDAP servers, or different databases on the same LDAP server, by creating more than one LDAP instance with different IP addresses or port settings.

PPP (Point-to-Point Protocol) PPP is a protocol for communication between two computers using a serial interface, typically a personal computer connected by phone line to a server. For example, your Internet server provider may provide you with a PPP connection so that the provider's server can respond to your requests, pass them on to the Internet, and forward your requested Internet responses back to you. PPP uses the Internet Protocol (IP) and is designed to handle others. It is sometimes considered a member of the TCP/IP suite of protocols. Relative to the Open Systems Interconnection (OSI) reference model, PPP provides layer 2 (data-link layer) service. Essentially, it packages your computer's TCP/IP packets and forwards them to the server where they can actually be put on the Internet.

protocol A protocol is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols at each layer in the telecommunication exchange that both ends of the exchange must recognize and observe. Protocols are often described in an industry or international standard.

Proxy An HTTP Proxy is a server that acts as a middleman in the communication between HTTP clients and servers.

Public Key In Cryptography a publicKey is a value provided by some designated authority as an Encryption Key that, combined with a private key derived from the public key, can be used to effectively encrypt messages andDigital Signatures.

The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).

Public Key Infrastructure (PKI) A PKI enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The Public Key infrastructure provides for a Digital Certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on.

R

RDN (LDAP) The Relative Distinguished Name (frequently but incorrectly written as Relatively Distinguished Name). The name given to an attribute(s) that is unique at its level in the hierarchy. RDNs may be single valued or multi-valued in which case two or more attributes are combined using '+' (plus) to create the RDN e.g. cn+uid. The term RDN is only meaningful when used as part of a DN to uniquely describe the attributes on the path UP the DIT from a selected entry (or search start location) to the directory root (or more correctly the Root DSE). More info.

referral (LDAP) An operation in which the LDAP server returns to an LDAP client the name (typically in the form of an LDAP URL) of another LDAP server that might be able to provide the information requested by the LDAP client.

Remote Authentication Dial-In User Service (RADIUS) RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

RFC (Request for Comments) A series of memoranda that encompass new research, innovations, and methodologies applicable to Internet technologies.

Role A set of typical administrator tasks, each with an associated set of permissions. An administrator can have more than one predefined role, and a role can apply to multiple administrators.

root (LDAP) The root entry (a.k.a base, suffix) is one of many terms used to describe the topmost entry in a DIT. The Root DSE is a a kind of super root.

Root DSE (LDAP) Conceptually the top most entry in a LDAP hierarchy - think of it as a super root and normally invisible i.e. not accessed in normal operations. Sometimes confused with root or base or suffix. DSE stands for DSA Specific Entry and DSA in turn stands for Directory System Agent (any directory enabled service providing DAP or LDAP access). Information about the rootDSE may be obtained in OpenLDAP by querying the OpenLDAProoDSE classobject and will provide information about protocol versions supported, services supported and the naming-context(s) or DIT(s) supported.

rootdn (LDAP) The rootdn is a confusingly named directive in the slapd.conf file which defines a superuser which can bypass normal directory access rules.

RPM (RedHat Package Manager) An RPM is a downloadable software package that is installable on Linux distributions that use RPM as their package management format.

S

SAN (Subject Alternative Name) Extension within certificate information.

Schema (LDAP) A package of attributes and object classes that are sometimes (nominally) related. The schema(s) in which the object classes and attributes that the application will use (reference) are packaged are identified to the LDAP server so that it can read and parse all that wonderful ASN.1 stuff. In OpenLDAP this done using the slapd.conf file.

search (LDAP) An operation that is carried out by defining a base directory name (DN), a scope, and a search filter.

Secure Sockets Layer(SSL) A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection. SSL is a cryptographic protocol which provides secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, and other data transfers. There are slight differences between SSL 3.0 and TLS 1.0, but the protocol remains substantially the same. The term "TLS" as used here applies to both protocols unless clarified by context.

Security Policy A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

server A system entity that provides a service in response to requests from other system entities called clients.

service provisioning Service provisioning refers to the "preparation beforehand" of IT systems' materials or supplies required to carry out a specific activity. This includes the provisioning of digital services such as user accounts and access privileges on systems, networks and applications, as well as the provisioning of non-digital or "physical" resources such as cell phones and credit cards.

service selection policy A set of rules that determines which access policy applies to an incoming request.

Session A session is a virtual connection between two hosts by which network traffic is passed.

session (LDAP) A session occurs between a LDAP client and a server when the client sends a bind command. A session may be either anonymous or authenticated.

session conditions Custom conditions, and date and time conditions.

Session Key In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

shell profiles The basic “permissions container” for a TACACS+ based device administration policy, in which you define permissions to be granted for a shell access request.

SLA (Service Level Agreement) A SLA is that part of a service contract in which a certain level of service is agreed upon. A SLA is a formal negotiated agreement between two parties. It is a contract that exists between customers and their service provider, or between service providers. It transcripts the common understanding about services, priorities, responsibilities, guarantee, etc. It then specifies the levels of availability, serviceability, performance, operation or other attributes of the service like billing.

SNMP (Simple Network Management Protocol) A TCP/IP network protocol that provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SOAP (Simple Object Access Protocol) A lightweight XML-based protocol for exchange of information in a decentralized, distributed environment. SOAP consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined datatypes, and a convention for representing remote procedure calls and responses.

SPML (Service Provisioning Markup Language) SPML is the open standard protocol for the integration and interoperation of service provisioning requests.

SSH(Secure Shell) A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

subtype (LDAP) LDAPv3 defines a number of subtypes at this time two have been defined binary (in RFC 2251) and lang (in RFC 2596). subtypes may be used when referencing an attribute and qualify e.g. cn;lang-en-us=smith would perform a search using US english. The subtype does not affect the encoding since UTF-8 (used for cn) allows for all language types. lang subtypes are case insensitive.

suffix (LDAP) Also known as root, base, is one of many terms used to describe the topmost entry in a DIT. The term is typically used because this entry is usually defined in the suffix parameter in a OpenLDAP's slapd.conf file. The Root DSE is a kind of super root. Suffix Naming.

system administration The role-based administrative functions performed by a group of administrators.

system configuration The role-based administrative functions performed by a group of administrators to configure system performance.

System Health Dashboard The Monitoring & Report Viewer Dashboard that provides information about the health status of associated ACS instances.

system operations A set of operations that you must perform to effectively deploy and manage the ACS servers in your network.

T

TACACS TACACS (Terminal Access Controller Access Control System) is an older Authentication protocol common to UNIX networks that allows a remote access server to forward a user's logon password to an authenticationServer to determine whether access can be allowed to a given system. TACACS is an Encryption protocol and therefore less secure than the later TACACS+ and Remote Authentication Dial-In User Service (RADIUS) protocols.

TACACS+ settings Used to configure TACACS+ runtime characteristics.

TCP/IP Transmission Control Protocol/Internet Protocol is the basic communication language or protocol of the Internet. TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

U

UDP User Datagram Protocol. A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP)

URL Uniform Resource Locator. The unique address for a file that is accessible on the Internet.

user and identity store A repository of users, user attributes, and user authentication options.

user authentication option An option to enable or disable TACACS+ password authentication.

user attribute configuration An administrative task consisting of configuring an internal user's identity attributes.

V

VPN Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.

VSA Vendor Specific Attribute. A proprietary property or characteristic not provided by the standard Remote Authentication Dial-In User Service (RADIUS) attribute set. VSAs are defined by vendors of remote access servers to customize RADIUS for their servers.

W

WCS Cisco Wireless Control System us a platform designed to help enterprises design, control and monitor Cisco wireless LANs. WCS is the industry leading platform for wireless LAN planning, configuration, and management.

Web server A Web server is a program that, using the client/server model and the World Wide Web's Hypertext Transfer Protocol (HTTP), serves the files that form Web pages to Web users (whose computers contain HTTP clients that forward their requests).

Web service A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. The web server interface is described in a machine-processable format, WSDL. Other systems interact with the Web service, typically using HTTP with an XML serialization in conjunction with other Web-related standards.

WSDL (Web Services Description Language) WSDL is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically.

X

X.509 A standard for public key infrastructure. X.509 specifies, amongst other things, standard formats for public key certificates and a certification path validation algorithm.

XML (eXtensible Markup Language) XML is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

INDEX

Symbols

! formatting symbol 13-33
% operator 13-58
& formatting symbol 13-32
& operator 13-58
* operator 13-57
+ operator 13-57
/ operator 13-57
<= operator 13-58
<> operator 13-58
< formatting symbol 13-33
< operator 13-58
= operator 13-58
>= operator 13-58
> formatting symbol 13-33
> operator 13-58
@ formatting symbol 13-32
– operator 13-57

A

ABS function 13-51
absolute values 13-51
accessing
    data 13-63
    Interactive Viewer 13-20
    table of contents entries 13-23
acs distributed deployment 17-1
ADD_DAY function 13-51
ADD_HOUR function 13-51
ADD_MINUTE function 13-51
ADD_MONTH function 13-51
ADD_QUARTER function 13-51
ADD_SECOND function 13-51
ADD_WEEK function 13-51
ADD_YEAR function 13-51
Add Group command 13-48
adding
    aggregate rows 13-61, 13-62
    data filters 13-65, 13-67, 13-68, 13-69
    data groups 13-47, 13-48
    formatting rules 13-35, 13-36
    page breaks 13-39
addition operator 13-57
administrator access setting 16-11
administrator password policy 16-9
administrator password reset 16-12
administrator roles 16-2
Advanced Filter dialog 13-69, 13-70
Advanced Sort command 13-45
aggregate functions 13-60, 13-61
aggregate rows
    creating 13-61, 13-62
    formatting data in 13-28 to 13-29
aggregate values 13-40
Aggregation dialog 13-61
alarms 12-1
    syslog targets 12-30
    system alarms 12-29
alarm schedules 12-5
aligning data 13-28
alignment options 13-28
AND operator 13-58, 13-70
Any Of condition 13-66
arguments 13-50

Arrange Columns dialog 13-40
ascending sort order 13-45
AVERAGE function 13-51
Average function 13-60
averages 13-51, 13-55, 13-57, 13-60, 13-61

B

background colors 13-37
Between condition 13-66, 13-70
BETWEEN function 13-51
Between operator 13-37
blank characters 13-56
Boolean values 13-52, 13-57, 13-66
Bottom N condition 13-66
Bottom Percent condition 13-66

C

calculated columns
  aggregating data and 13-60, 13-61, 13-62
  creating 13-49, 13-57
  placing values in 13-52
Calculation dialog 13-50, 13-58, 13-59
calculations 13-40
case conversions 13-33
case-insensitive searches 13-56
case-sensitive searches 13-52
category series 13-71
cautions
  description ii-xxiv
CEILING function 13-51
changing
  aggregate values 13-28
  chart subtypes 13-73
  column headers 13-23, 13-26
  conditional formats 13-36
  data filters 13-69
  default formats 13-27
  labels 13-26
  reports 13-20
character patterns 13-56, 13-67
character placeholder 13-32
charts
  overview 13-71
Chart Subtype command 13-73
Cisco CAT 6K 4-22
clearing data filters 13-69
closing Standard Viewer 13-20
collapsing data groups 13-48, 13-64, 13-65
colors 13-37
column headers 13-23
column names 13-68
Column Properties dialog 13-28
columns
  aligning data in 13-28
  changing order of 13-40
  counting rows in 13-60
  deleting 13-42
  determining first value in 13-52, 13-60
  determining last value in 13-53, 13-60
  determining type 13-30
  displaying data in 13-29
  formatting data in 13-35, 13-36
  grouping date and time values in 13-48
  resizing 13-24, 13-28
  sorting data in 13-45, 13-71
Column Width command 13-28
comma-separated values files. See CSV files
comparison filters 13-67
comparison operators 13-36, 13-67
comparisons 13-36, 13-52
concatenation operator 13-58
Conditional Formatting dialog 13-35, 13-36, 13-38
conditional formatting rules 13-35, 13-36
conditions
  filtering data and 13-65, 13-66, 13-69

formatting data and 13-35
context menus 13-20
conversions 13-33
COUNT_DISTINCT function 13-52
COUNT function 13-51
Count function 13-60
Count Value function 13-60
creating
aggregate rows 13-61, 13-62
calculated columns 13-49, 13-57
data filters 13-65, 13-67, 13-68, 13-69
data groups 13-47, 13-48
formatting rules 13-35, 13-36
crud operations 7-5
CSV files 13-23, 13-25
currency 13-31
Currency format option 13-30
currency formatting options 13-31
currency symbols 13-31
Custom format option 13-29, 13-30
customizing
formats 13-31, 13-32

D

data
accessing 13-63
aligning 13-28
displaying 13-29, 13-40, 13-63
hiding 13-42
plotting relationships for 13-71
data filters 13-65, 13-67, 13-68, 13-69
data points 13-71
data rows 13-63, 13-64
data sections 13-64, 13-65
data sets 13-40, 13-60, 13-63, 13-71
data sources 13-25, 13-30, 13-45, 13-63
data types 13-30
Date and Time Format dialog 13-34
date calculations 13-59
date data types 13-29
date expressions 13-58, 13-59
date formats 13-29, 13-34
Date or Time Column Format dialog 13-34
date values 13-34, 13-48, 13-52
DAY function 13-52
decimal values 13-31
default formats 13-27, 13-28
default network device 7-16
deleting
columns 13-42
conditional formats 13-38
data filters 13-69
filter conditions 13-70
page breaks 13-39
delimited text files 13-23, 13-25
descending sort order 13-45
designs
hiding data in 13-63
organizing data in 13-40
saving 13-25
DIFF_DAY function 13-52
DIFF_HOUR function 13-52
DIFF_MINUTE function 13-52
DIFF_MONTH function 13-52
DIFF_QUARTER function 13-52
DIFF_SECOND function 13-52
DIFF_WEEK function 13-52
DIFF_YEAR function 13-52
displaying
data 13-29, 13-40, 13-63
detail rows 13-64
reports 13-20
specific report pages 13-22, 13-23
table of contents 13-22
distinct values 13-52, 13-60
division 13-54, 13-57
division operator 13-57

downloads 18-42
duplicate values 13-63, 13-64

E

EAP-FAST
enabling B-25
identity protection B-19
logging B-19
master keys
definition B-20
PAC
automatic provisioning B-22
definition B-20
manual provisioning B-23
refresh B-25
phases B-18
EAP-FAST settings
configuring 18-3
EAP-TLS settings
configuring 18-2
equality 13-58, 13-70
equality operator 13-58
Equal to condition 13-66
Excel spreadsheets 13-23
expanding sections or groups 13-64
expanding table of contents entries 13-23
Export Data dialog 13-24
expressions
calculating data and 13-57, 13-58
filtering data and 13-65, 13-66, 13-67, 13-69, 13-70
external identity server
RSA SecurID 8-46
external identity servers
RADIUS identity stores 8-52
external identity stores 8-2
LDAP 8-18
Microsoft AD 8-38

F

false function 13-52
fields 13-26
filter conditions 13-65, 13-66, 13-69, 13-70
Filter dialog 13-68, 13-69
Filter drop-down list 13-71
filters 13-65, 13-67, 13-68, 13-69
FIND function 13-52
finding text values 13-52, 13-56
FIRST function 13-52
First function 13-60
Fixed format option 13-30
fixed numeric values 13-31
Font dialog box 13-37
fonts 13-37, 13-73
footers 13-60
Format Chart page 13-73
Format command 13-73
format patterns 13-31, 13-33
formats
changing 13-27, 13-36
customizing 13-31, 13-32
data types and 13-29
deleting conditional 13-38
exporting data and 13-23
previewing conditional 13-38
selecting 13-31
formatting
column headers 13-27
labels 13-26, 13-27
string data 13-32
formatting options 13-31, 13-32, 13-34
formatting rules 13-35, 13-36
formatting symbols 13-31, 13-32
functions 13-50, 13-60, 13-61

G

General Date format option 13-29
General Number format option 13-30
Go to page pick list 13-22
Greater Than condition 13-66
greater than operator 13-58
Greater Than or Equal to condition 13-66
greater than or equal to operator 13-58
Group Detail dialog 13-48
grouping
  filter conditions 13-70
grouping intervals 13-48
groups
  adding 13-47, 13-48
  aggregating data and 13-60
  collapsing 13-48, 13-64, 13-65
  counting rows for 13-51
  displaying data and 13-40, 13-63
  setting page breaks for 13-39
  sorting data and 13-46

H

headers 13-23, 13-60
hidden items 13-42
Hide Column command 13-43
Hide Detail command 13-65
Hide or Show Items dialog 13-42
hiding
  detail rows 13-64
  duplicate values 13-63, 13-64
  report items 13-42
HTML files 13-25

I

identity store sequences 8-65
If...Then...Else statement 13-53
IF function 13-53
import and export
  creating import files 5-20
  supported objects 5-18
information objects 13-29
IN function 13-53
Interactive Viewer 13-20
internal identity stores 8-1
ISBOTTOMN function 13-53
ISBOTTOMNPERCENT function 13-53
Is False condition 13-66
Is False operator 13-36
Is Not Null condition 13-66
Is Not Null operator 13-36
Is Null condition 13-66
ISNULL function 13-53
Is Null operator 13-36
ISTOPN function 13-53
ISTOPNPERCENT function 13-53
Is True condition 13-66
Is True operator 13-36

L

labels 13-26, 13-27
  formatting 13-27
LAST function 13-53
Last function 13-60
leading characters 13-56
LEFT function 13-54
LEN function 13-54
Less Than condition 13-66
less than operator 13-58
Less Than or Equal to condition 13-66
less than or equal to operator 13-58
licensing 18-35
Like condition 13-66
LIKE function 13-54
literal values 13-70

locales
creating charts and 13-73
customizing formats for 13-29, 13-31, 13-34
locating text values 13-52, 13-56
logical operators 13-57
Long Date format option 13-29
Long Time format option 13-29
lowercase characters 13-54
Lowercase format option 13-30
LOWER function 13-54

M

master key
definition B-20
matching character patterns 13-67
mathematical functions 13-50
mathematical operators 13-57
MAX function 13-54
Max function 13-60
MEDIAN function 13-54
Median function 13-60
median values 13-54, 13-60
Medium Date format option 13-29
Medium Time format option 13-29
membership filters 13-67
menus 13-20
migration
common scenarios 2-7
considerations 2-3
downloads 2-3
requirements 2-2
supported versions 2-2
MIN function 13-54
Min function 13-60
Mode function 13-60
MOD function 13-54
monitoring & report viewer
configuring remote database 15-16
data backup and purge 15-2
data upgrade status 15-11
restore 15-5
viewing process status 15-10
viewing scheduled jobs 15-10
monitoring and report viewer
dashboard 11-3
MONTH function 13-54, 13-55
Move to Group Header command 13-41
Move to Group Header dialog 13-41
MOVINGAVERAGE function 13-55
moving columns 13-40
moving through reports 13-22
multipage reports 13-64
multiplication 13-58
multiplication operator 13-57

N

naming
calculated columns 13-58
navigating through reports 13-22
navigational tools 13-22
negative numbers 13-31
non-null values 13-53, 13-55, 13-66
Not Between condition 13-66
Not Between operator 13-37
note, description of ii-xxiv
Not Equal to condition 13-66
not equal to operator 13-58
Not Like condition 13-66
NOTNULL function 13-55
NOT operator 13-58, 13-70
NOW function 13-55
null value filters 13-67
null values 13-53, 13-55, 13-66, 13-67
Number Column Format dialog 13-30, 13-31
Number column format dialog 13-32
number formats 13-30, 13-31

numeric data types 13-30
numeric expressions 13-58
numeric values 13-23, 13-31

O

opening
exported data files 13-25
Interactive Viewer 13-20
operators 13-36, 13-57
OR operator 13-58, 13-70

P

PAC
automatic provisioning B-22
definition B-20
manual provisioning B-23
refresh B-25
Page Break on Group dialog 13-39
page breaks 13-39
paging toolbar 13-22
pattern-matching filters 13-67
PDF files 13-25
PEAP
identity protection B-14
phases B-14
PEAP settings
configuring 18-3
percentage operator 13-58
percentages 13-31, 13-53, 13-55
Percent format option 13-30
PERCENTILE function 13-55
PERCENTRANK function 13-55
PERCENTSUM function 13-55
previewing conditional formats 13-38
primary sorting column 13-45
Print dialog 13-25
printing 13-25
printing options 13-25

Q

QUARTER function 13-55
QUARTILE function 13-55
Quartile function 13-60

R

RADIUS proxy 4-27
configuring proxy service 4-29
supported protocols 4-28
supported RADIUS attributes 4-29
range filters 13-67
range of values 13-36, 13-37, 13-66, 13-67
RANK function 13-55, 13-56
relationships 13-71
Reorder Columns command 13-40
report designs
hiding data in 13-63
organizing data in 13-40
saving 13-25
report items 13-42
reports 13-1
catalog 13-7
changing 13-20
displaying 13-20
dynamic change of authorization 13-2
favorites 13-3
navigating through 13-22
printing 13-25
setting page breaks for 13-39
shared 13-7
viewing specific pages in 13-22, 13-23
report sections 13-64, 13-65
report templates 13-27, 13-73

report viewers 13-20
resizing columns 13-24, 13-28
RIGHT function 13-56
ROUNDDOWN function 13-56
ROUND function 13-56
rounding 13-51, 13-56
ROUNDUP function 13-56
row-by-row comparisons 13-52
rows 13-63, 13-64
RUNNINGSUM function 13-56
running totals 13-56

S

Save As dialog 13-25
saving
  exported data 13-25
  report designs 13-25
Scientific format option 13-30
scientific numbers 13-31
SEARCH function 13-56
searching 13-52, 13-56, 13-68
sections 13-64, 13-65
Select data item dialog 13-68
Short Date format option 13-29
Short Time format option 13-29
Show Columns command 13-43
Show Columns dialog 13-43
Show Detail command 13-65
software
  updates 17-21
sorting multiple columns 13-45
sort order 13-45
spreadsheet reports 13-23
SQRT function 13-56
square roots 13-56
standard deviation 13-56, 13-60
Standard Deviation function 13-60
Standard Viewer 13-20
STDEV function 13-56
String Column Format dialog 13-33
String column format dialog 13-32
string conversions 13-33
string data types 13-30
string fields 13-67
string patterns 13-56
strings 13-32, 13-54, 13-66
substrings 13-54, 13-56, 13-66
subtraction operator 13-57
subtypes (charts) 13-73
SUM function 13-56
Sum function 13-60
summary values 13-56, 13-60

T

tables
  aggregating data and 13-60, 13-61, 13-62
  counting rows in 13-51, 13-60
TACACS+ settings
  configuring 18-1
templates 13-27, 13-73
testing
  character patterns 13-67
  for non-null values 13-55
  for null values 13-53, 13-67
  range of values 13-67
  sets of values 13-67
text
  aggregating values for 13-61
  changing label 13-26
  converting case 13-33
  searching for 13-52, 13-56
text files 13-23, 13-25
text formats 13-30
text patterns 13-67
text styles 13-37
themes 13-73

thousands separators 13-31
time data types 13-29
time formats 13-29, 13-34
timesaver, description of ii-xxiv
time stamps 13-55, 13-56
time values 13-34, 13-48
TODAY function 13-56
Top N condition 13-66
Top Percent condition 13-66
totals 13-36, 13-56, 13-60
trailing characters 13-56
TRIM function 13-56
TRIMLEFT function 13-56
TRIMRIGHT function 13-57
troubleshooting
  connectivity 14-1
  expert troubleshooter 14-2
  support bundles 14-1
true function 13-57
TrustSec 4-22

U

Unformatted format option 13-29, 13-30
uppercase characters 13-57
Uppercase format option 13-30
UPPER function 13-57

V

values
  averaging 13-51, 13-55, 13-57, 13-60, 13-61
  calculating 13-40
  comparing 13-36, 13-67
  counting number of distinct 13-52, 13-60
  determining rank 13-55
  displaying frequently occurring 13-60
  hiding duplicate 13-63, 13-64
  returning highest 13-54, 13-60
  returning last 13-53, 13-60
  returning lowest 13-54, 13-60, 13-66
  returning null 13-66
  returning specified 13-66
  rounding 13-51, 13-56
  searching for 13-68
  sorting highest or lowest 13-71
  testing for non-null 13-55
  testing for null 13-53, 13-67
  testing for specified 13-53
  testing range of 13-67
  testing sets of 13-67
value series 13-71
VAR function 13-57
variance 13-57, 13-61
Variance function 13-61
viewers 13-20
viewing
  data 13-29, 13-40, 13-63
  detail rows 13-64
  reports 13-20
  specific report pages 13-22, 13-23
  table of contents 13-22
viewing environments 13-20
vpn remote access 4-19
  configuring access service 4-21
  supported clients 4-21
  supported identity stores 4-20
  supported network access servers 4-20
  supported protocols 4-19

W

WEEKDAY function 13-57
WEEK function 13-57
WEIGHTEDAVERAGE function 13-57
Weighted average function 13-61
wildcard characters 13-56

X

x-axis values 13-71

Y

y-axis values 13-71
YEAR function 13-57