



User Guide for Cisco Secure Access Control Server

Release 4.2

February 2008

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-14386-01

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.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0801R)



CONTENTS

Preface XXVII

Audience XXVII

Organization XXVII

Conventions XXVIII

Product Documentation XXIX

Related Documentation XXXI

Obtaining Documentation and Submitting a Service Request XXXI

Open Source License Acknowledgements XXXI

OpenSSL/Open SSL Project XXXI

CHAPTER 1

Overview 1-1

Introduction to ACS 1-1

Network Admission Control (NAC) 1-2

Identity-Based Networking Services (IBNS) 1-2

ACS Features, Functions and Concepts 1-3

ACS as the AAA Server 1-3

AAA Protocols—TACACS+ and RADIUS 1-3

TACACS+ 1-4

RADIUS 1-4

Platforms 1-5

Additional Features in This Release 1-5

Authentication 1-7

Authentication Considerations 1-7

Authentication and User Databases 1-7

Authentication Protocol-Database Compatibility 1-8

Passwords 1-8

EAP Support 1-10

Other Authentication-Related Features 1-12

Authorization 1-12

Max Sessions 1-13

Dynamic Usage Quotas 1-13

Shared Profile Components 1-14

Support for Cisco Device-Management Applications 1-14

Other Authorization-Related Features 1-14

Accounting	1-15
Other Accounting-Related Features	1-16
Managing and Administrating ACS	1-16
Web Interface Security	1-16
Cisco Security Agent Integration (ACS SE Only)	1-17
Cisco Security Agent Service Management	1-17
Cisco Security Agent Logging	1-17
Cisco Security Agent Restrictions	1-18
Cisco Security Agent Policies	1-18
HTTP Port Allocation for Administrative Sessions	1-19
Web Interface Layout	1-19
Uniform Resource Locator for the Web Interface	1-21
Online Help and Online Documentation	1-21
Using Online Help	1-21
Using the Online User Guide	1-22
ACS Specifications	1-22
System Performance Specifications	1-22
ACS Windows Services	1-23
Online Documentation Reference	1-23
Related Documentation	1-24
TACACS+ Documents	1-24
Network Admission Control (NAC) documentation	1-24
Requests for Comments (RFCs)	1-24
Technology White Papers	1-25
Question and Answer Pages	1-25
Tutorials	1-25
Software Download	1-25

CHAPTER 2

Using the Web Interface 2-1

Administrative Sessions	2-1
Administrative Sessions and HTTP Proxy	2-2
Administrative Sessions Through Firewalls	2-2
Administrative Sessions Through a NAT Gateway	2-2
Accessing the Web Interface	2-3
Logging Off the Web Interface	2-4
Configuring User Access	2-4
User-to-Group Relationship	2-4
Network Access Profiles (NAPs)	2-5
Per-User or Per-Group Features	2-5

Customizing User Data	2-5
Displaying Advanced Options	2-6
Displaying TACACS+ Configuration Options	2-6
Displaying RADIUS Configuration Options	2-7
Specifying Display of RADIUS (IETF) Options	2-9
Specifying Display of RADIUS (<vendor>) Options	2-9
Interface Configuration Reference	2-10
Configure User Defined Fields	2-10
TACACS+ Services	2-11
Advanced Configuration Options (for TACACS+)	2-11
RADIUS Protocols	2-12
Advanced Options (for Interface Configuration)	2-14

CHAPTER 3

Network Configuration	3-1
About Network Configuration	3-1
About ACS in Distributed Systems	3-2
AAA Servers in Distributed Systems	3-2
Default Distributed System Settings	3-3
Proxy in Distributed Systems	3-3
The Proxy Feature	3-3
An Example	3-4
Proxy Distribution Table	3-4
Fallback on Failed Connection	3-4
Character String	3-5
Stripping	3-5
Remote Use of Accounting Packets	3-5
Other Features Enabled by System Distribution	3-6
Network Device Searches	3-6
Network Device Search Criteria	3-6
Searching for Network Devices	3-7
Configuring AAA Clients	3-8
AAA Client Configuration Options	3-8
Adding AAA Clients	3-12
Editing AAA Clients	3-13
Configuring a Default AAA Client	3-14
Deleting AAA Clients	3-14
Configuring AAA Servers	3-15
AAA Server Configuration Options	3-15

Adding AAA Servers	3-17
Editing AAA Servers	3-17
Deleting AAA Servers	3-18
Configuring Remote Agents (ACS SE Only)	3-19
About Remote Agents	3-19
Remote Agent Configuration Options	3-19
Adding a Remote Agent	3-21
Editing a Remote Agent Configuration	3-22
Deleting a Remote Agent Configuration	3-23
Configuring Network Device Groups	3-23
Adding a Network Device Group	3-24
Assigning an Unassigned AAA Client or AAA Server to an NDG	3-25
Reassigning AAA Clients or AAA Servers to an NDG	3-26
Editing a Network Device Group	3-26
Deleting a Network Device Group	3-27
Configuring Proxy Distribution Tables	3-28
About the Proxy Distribution Table	3-28
Adding a New Proxy Distribution Table Entry	3-28
Sorting the Character String Match Order of Distribution Entries	3-29
Editing a Proxy Distribution Table Entry	3-30
Deleting a Proxy Distribution Table Entry	3-30

CHAPTER 4

Shared Profile Components 4-1

About Shared Profile Components	4-1
802.1X Example Setup	4-1
Network Access Filters	4-2
About Network Access Filters	4-2
Adding a Network Access Filter	4-3
Editing a Network Access Filter	4-5
Deleting a Network Access Filter	4-6
RADIUS Authorization Components	4-6
About RADIUS Authorization Components	4-7
Understanding RACs and NAPs	4-7
Vendors	4-7
Attribute Types	4-8
Before You Begin Using RADIUS Authorization Components	4-8
Enabling Use of RAC	4-9
Adding RADIUS Authorization Components	4-10
Cloning a RADIUS Authorization Component	4-10

Editing a RADIUS Authorization Component	4-11
Deleting a RADIUS Authorization Component	4-11
Downloadable IP ACLs	4-13
About Downloadable IP ACLs	4-13
Adding a Downloadable IP ACL	4-15
Editing a Downloadable IP ACL	4-16
Deleting a Downloadable IP ACL	4-17
Network Access Restrictions	4-18
About Network Access Restrictions	4-18
About IP-Based NAR Filters	4-19
About Non-IP-based NAR Filters	4-20
Adding a Shared NAR	4-21
Editing a Shared NAR	4-23
Deleting a Shared NAR	4-24
Command Authorization Sets	4-25
About Command Authorization Sets	4-25
Command Authorization Sets Description	4-26
Command Authorization Sets Assignment	4-27
Case Sensitivity and Command Authorization	4-27
Arguments and Command Authorization	4-28
About Pattern Matching	4-28
Adding a Command Authorization Set	4-29
Editing a Command Authorization Set	4-30
Deleting a Command Authorization Set	4-31

CHAPTER 5

User Group Management 5-1

About User Group Setup Features and Functions	5-2
Default Group	5-2
Group TACACS+ Settings	5-2
Group RADIUS Settings	5-3
Basic User Group Settings	5-3
Group Disablement	5-3
Enabling VoIP Support for a User Group	5-4
Setting Default Time-of-Day Access for a User Group	5-5
Setting Callback Options for a User Group	5-5
Setting Network Access Restrictions for a User Group	5-6
Setting Max Sessions for a User Group	5-9
Setting Usage Quotas for a User Group	5-10
Configuration-Specific User Group Settings	5-12

Setting Enable Privilege Options for a User Group	5-13
Setting Token Card Settings for a User Group	5-14
Enabling Password Aging for the ACS Internal Database	5-15
Varieties of Password Aging Supported by ACS	5-15
Password Aging Feature Settings	5-16
Enabling Password Aging for Users in Windows Databases	5-19
Setting IP Address Assignment Method for a User Group	5-21
Assigning a Downloadable IP ACL to a Group	5-22
Configuring TACACS+ Settings for a User Group	5-22
Configuring a Shell Command Authorization Set for a User Group	5-23
Configuring a PIX Command Authorization Set for a User Group	5-25
Configuring Device Management Command Authorization for a User Group	5-26
Configuring IETF RADIUS Settings for a User Group	5-27
Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group	5-28
Advanced Configuration Options	5-29
Configuring Cisco Airespace RADIUS Settings for a User Group	5-29
Configuring Cisco Aironet RADIUS Settings for a User Group	5-30
Configuring Ascend RADIUS Settings for a User Group	5-31
Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group	5-32
Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group	5-33
Configuring Microsoft RADIUS Settings for a User Group	5-34
Configuring Nortel RADIUS Settings for a User Group	5-36
Configuring Juniper RADIUS Settings for a User Group	5-37
Configuring 3COMUSR RADIUS Settings for a User Group	5-37
Configuring BBSM RADIUS Settings for a User Group	5-38
Configuring Custom RADIUS VSA Settings for a User Group	5-39
Group Setting Management	5-40
Listing Users in a User Group	5-40
Resetting Usage Quota Counters for a User Group	5-40
Renaming a User Group	5-41
Saving Changes to User Group Settings	5-41

CHAPTER 6

User Management 6-1

About User Setup Features and Functions	6-1
About User Databases	6-2
Basic User Setup Options	6-2
Adding a Basic User Account	6-3
Setting Supplementary User Information	6-4
Setting a Separate CHAP/MS-CHAP/ARAP Password	6-5

Assigning a User to a Group	6-5
Setting the User Callback Option	6-6
Assigning a User to a Client IP Address	6-7
Setting Network Access Restrictions for a User	6-8
Setting Max Sessions Options for a User	6-11
Options for Setting User Usage Quotas	6-12
Setting Options for User Account Disablement	6-13
Assigning a Time Bound Alternate Group	6-14
Assigning a Downloadable IP ACL to a User	6-14
Advanced User Authentication Settings	6-15
TACACS+ Settings (User)	6-15
Configuring TACACS+ Settings for a User	6-16
Configuring a Shell Command Authorization Set for a User	6-17
Configuring a PIX Command Authorization Set for a User	6-19
Configuring Device-Management Command Authorization for a User	6-20
Configuring the Unknown Service Setting for a User	6-21
Advanced TACACS+ Settings for a User	6-21
Setting Enable Privilege Options for a User	6-22
Setting TACACS+ Enable Password Options for a User	6-23
Setting TACACS+ Outbound Password for a User	6-24
RADIUS Attributes	6-24
Setting IETF RADIUS Parameters for a User	6-25
Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User	6-26
Setting Cisco Airespace RADIUS Parameters for a User	6-27
Setting Cisco Aironet RADIUS Parameters for a User	6-27
Setting Ascend RADIUS Parameters for a User	6-29
Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User	6-29
Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User	6-30
Setting Microsoft RADIUS Parameters for a User	6-31
Setting Nortel RADIUS Parameters for a User	6-33
Setting Juniper RADIUS Parameters for a User	6-33
Setting 3COMUSR RADIUS Parameters for a User	6-34
Setting BBSM RADIUS Parameters for a User	6-35
Setting Custom RADIUS Attributes for a User	6-36
User Management	6-37
Listing All Users	6-37
Finding a User	6-37
Disabling a User Account	6-38
Deleting a User Account	6-39
Resetting User Session Quota Counters	6-39

Resetting a User Account after Login Failure	6-40
Removing Dynamic Users	6-41
Saving User Settings	6-41

CHAPTER 7

System Configuration: Basic 7-1

Service Control	7-1
Determining the Status of ACS Services	7-2
Stopping, Starting, or Restarting Services	7-2
Setting Service Log File Parameters	7-2
Logging	7-3
Date and Time Format Control	7-3
Setting the Date and Time Formats	7-3
Local Password Management	7-4
Changing a User Password from a Device Using TACACS+	7-5
Configuring Local Password Management	7-6
Configuring Intervals for Generating a New Password (ACS for Windows Only)	7-7
ACS Backup	7-8
About ACS Backup	7-8
Backup File Locations (ACS for Windows Only)	7-9
Directory Management (ACS for Windows Only)	7-9
Components Backed Up	7-9
Reports of ACS Backups	7-10
Backup Options	7-10
Performing a Manual ACS Backup	7-11
Scheduling ACS Backups	7-12
Disabling Scheduled ACS Backups	7-14
ACS System Restore	7-14
About ACS System Restore	7-14
Filenames and Locations	7-15
Components Restored	7-16
Reports of ACS Restorations	7-16
Restoring ACS from a Backup File	7-16
ACS Active Service Management	7-18
System Monitoring	7-18
System Monitoring Options	7-18
Setting Up System Monitoring	7-19
Event Logging	7-20
Setting Up Event Logging	7-20
VoIP Accounting Configuration	7-21

Configuring VoIP Accounting	7-21
Appliance Configuration (ACS SE Only)	7-22
Enabling or Disabling CSAgent	7-22
Configuring SNMP Support	7-23
Setting System Time and Date	7-23
Setting the ACS Host and Domain Names	7-24
Support Page	7-25
Running Support	7-25
Monitoring System Information	7-26
Viewing or Downloading Diagnostic Logs (ACS SE Only)	7-27
Appliance Upgrade Mechanism (ACS SE Only)	7-27
About Appliance Upgrades and Patches	7-28
Distribution Server Requirements	7-29
Upgrading an Appliance	7-29
Transferring an Upgrade Package to an Appliance	7-30
Applying an Upgrade to an Appliance	7-33

CHAPTER 8

System Configuration: Advanced	8-1
ACS Internal Database Replication	8-1
About ACS Internal Database Replication	8-2
Replication Process	8-3
Replication Frequency	8-5
Important Implementation Considerations	8-5
Database Replication Versus Database Backup	8-6
Database Replication Logging	8-7
Replication Options	8-7
Replication Components Options	8-7
Outbound Replication Options	8-9
Inbound Replication Options	8-10
Implementing Primary and Secondary Replication Setups on ACSs	8-10
Configuring a Secondary ACS	8-11
Replicating Immediately	8-13
Scheduling Replication	8-14
Disabling ACS Database Replication	8-16
Configuring Automatic Change Password Replication	8-16
Database Replication Event Errors	8-17
RDBMS Synchronization	8-17
About RDBMS Synchronization	8-17
Invoking RDBMS Synchronization	8-19

Configuring RDBMS for the ACS SE	8-19
Configuring for RDBMS Synchronization for ACS for Windows	8-19
RDBMS Synchronization Functionality	8-20
User Related Actions for RDBMS Synchronization	8-20
User Groups Related Actions for RDBMS Synchronization	8-21
Creating, Updating and Deleting dACLs for User and User Groups	8-21
Network Configuration	8-22
Creating, Reading, Updating and Deleting Actions for AAA clients	8-22
Creating, Reading, Updating, and Deleting dACL Attributes	8-23
Custom RADIUS Vendors and VSAs	8-27
RDBMS Synchronization Components	8-27
About CSDBSync	8-27
About the accountActions Table (ACS for Windows)	8-28
About the accountActions File (ACS SE)	8-29
ACS Database Recovery Using the accountActions Table	8-30
Reports and Event (Error) Handling	8-30
Preparing to Use RDBMS Synchronization	8-30
Configuring a System DSN for RDBMS Synchronization (ACS for Windows)	8-32
RDBMS Synchronization Options	8-33
RDBMS Setup Options	8-33
RDBMS Synchronization Setup For the accountActions File for Windows	8-33
FTP Setup Options for RDBMS Synchronization for SE	8-34
Scriptable Interface for RDBM Synchronization	8-34
Synchronization Scheduling Options	8-34
Synchronization Partners Options	8-34
Performing RDBMS Synchronization	8-35
Scheduling RDBMS Synchronization	8-36
Disabling Scheduled RDBMS Synchronizations	8-37
RDBMS Synchronization Failure Codes	8-38
IP Pools Server	8-39
About IP Pools Server	8-39
Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges	8-40
Refreshing the AAA Server IP Pools Table	8-41
Adding a New IP Pool	8-41
Editing an IP Pool Definition	8-42
Resetting an IP Pool	8-42
Deleting an IP Pool	8-43
IP Pools Address Recovery	8-44
Enabling IP Pool Address Recovery	8-44

NAC Attribute Management (ACS SE Only)	8-44
Posture Validation Attribute Definition File	8-44
Adding Attributes	8-47
Deleting Attributes	8-48
Exporting (Dumping) Attributes	8-50
Default Posture Validation Attribute Definition File	8-51

CHAPTER 9

System Configuration: Authentication and Certificates 9-1

About Certification and EAP Protocols	9-1
Digital Certificates	9-1
EAP-TLS Authentication	9-2
About the EAP-TLS Protocol	9-2
EAP-TLS and ACS	9-3
EAP-TLS Limitations	9-4
Enabling EAP-TLS Authentication	9-4
EAP-TLS and ACS in a NAC/NAP Environment	9-5
PEAP Authentication	9-6
About the PEAP Protocol	9-6
PEAP and ACS	9-7
PEAP and the Unknown User Policy	9-8
Enabling PEAP Authentication	9-8
EAP-FAST Authentication	9-9
About EAP-FAST	9-9
About Master Keys	9-11
About PACs	9-12
Provisioning Modes	9-13
Types of PACs	9-13
EAP-FAST for Anonymous TLS Renegotiation	9-16
PAC Free EAP-FAST	9-16
EAP-FAST PKI Authorization Bypass	9-16
Master Key and PAC TTLs	9-17
Replication and EAP-FAST	9-17
Enabling EAP-FAST	9-19
Stateless Session Server Resume	9-20
Global Authentication Setup	9-21
Configuring Authentication Options	9-21
ACS Certificate Setup	9-22
Installing an ACS Server Certificate	9-22
Adding a Certificate Authority Certificate	9-26

Editing the Certificate Trust List	9-28
Deleting a Certificate from the Certificate Trust List	9-29
Managing Certificate Revocation Lists	9-29
About Certificate Revocation Lists	9-29
Certificate Revocation List Configuration Options	9-30
Editing a Certificate Revocation List Issuer	9-31
Generating a Certificate Signing Request	9-32
Using Self-Signed Certificates	9-33
About Self-Signed Certificates	9-33
Self-Signed Certificate Configuration Options	9-34
Generating a Self-Signed Certificate	9-35
Updating or Replacing an ACS Certificate	9-36
EAP-FAST PAC Files Generation (ACS SE)	9-37
PAC File Generation Options	9-37
Generating PAC Files	9-39
Advanced System Configuration Pages Reference	9-40
Global Authentication Setup Page	9-41
EAP-FAST Configuration Page	9-44

CHAPTER 10

Logs and Reports 10-1

About ACS Logs and Reports	10-1
AAA-Related Logs	10-1
ACS Audit Logs	10-5
ACS Logging Formats and Targets	10-5
CSV Logger	10-6
Syslog Logger	10-7
ODBC Logger (ACS for Windows only)	10-9
Remote Logging for ACS for Windows	10-10
Remote Logging for ACS SE with ACS Remote Agents	10-10
Dynamic Administration Reports	10-11
Entitlement Reports	10-11
Service Logs	10-12
Adding Session IDs to the CSAuth Diagnostic Log	10-13
Description of Error Codes in the CSAuth Diagnostic Log	10-13
Configuring ACS Logs	10-22
Configuring Critical Loggers	10-23
Configuring a CSV Log	10-24
Configuring Syslog Logging	10-24
Configuring an ODBC Log (ACS for Windows only)	10-25

Configuring and Enabling Remote Logging (ACS for Windows only)	10-26
Configuring the Remote Logging Server	10-26
Configuring ACS to Send Data to a Remote Logger	10-27
Configuring Logging to Remote Agents (ACS SE only)	10-27
Configuring ACS SE to Send Data to the Remote Agent	10-28
Configuring Remote Agent Logs on the Configuration Provider	10-28
Configuring Service Logs	10-29
Providing Service Logs for Customer Support	10-29
Viewing and Downloading Reports	10-30
Viewing and Downloading CSV Reports	10-31
CSV Log File Names	10-31
Viewing a CSV Report	10-31
Downloading a CSV Report	10-33
Viewing Dynamic Administration Reports	10-34
Viewing the Logged-in Users Report	10-34
Viewing the Disabled Accounts Report	10-35
Viewing the Appliance Status Report	10-35
Viewing and Downloading Entitlement Reports	10-36
Update Packets in Accounting Logs	10-37
Logging Configuration Pages Reference	10-37
Logging Configuration Page	10-37
Critical Loggers Configuration Page	10-38
Remote Logging Setup Page	10-39
Remote Agents Reports Configuration Page (ACS SE only)	10-39
CSV <i>log</i> File Configuration Page	10-40
Syslog <i>log</i> Configuration Page	10-41
ODBC <i>log</i> Configuration Page (ACS for Windows only)	10-42
Service Control Page Reference	10-43
Reports Page Reference	10-44
Audit Log Attributes	10-46

CHAPTER 11

Administrators and Administrative Policy 11-1

Administrator Accounts	11-1
About Administrator Accounts	11-1
Privileges	11-2
Administration Control Privilege	11-2
The Influence of Policy	11-3
Group Access Privileges	11-3
Password Expirations and Account Lockouts	11-3

Support for Regulatory Compliance	11-4
Logging In	11-5
Adding, Editing, and Deleting Accounts	11-6
Adding or Editing Accounts	11-6
Deleting an Account	11-7
Configuring Policy Options	11-8
Configuring Access Policy	11-8
Configuring Session Policy	11-8
Configuring Password Policy	11-9
Administration Control Pages Reference	11-10
Administration Control Page	11-10
Add Administrator and Edit Administrator Pages	11-11
Administrator Password Policy Page	11-16
Access Policy Setup Page	11-18
Session Policy Setup Page	11-20

CHAPTER 12

User Databases 12-1

ACS Internal Database	12-1
About the ACS Internal Database	12-2
User Import and Creation	12-2
About External User Databases	12-3
Authenticating with External User Databases	12-4
External User Database Authentication Process	12-4
Windows User Database	12-5
Windows User Database Support	12-5
Authentication with Windows User Databases	12-6
Trust Relationships	12-6
Windows Dial-Up Networking Clients	12-6
Windows Dial-Up Networking Clients with a Domain Field	12-7
Windows Dial-Up Networking Clients without a Domain Field	12-7
Usernames and Windows Authentication	12-7
Username Formats and Windows Authentication	12-7
Nondomain-Qualified Usernames	12-8
Domain-Qualified Usernames	12-9
UPN Usernames	12-9
EAP and Windows Authentication	12-10
Machine Authentication	12-10
Machine Access Restrictions	12-12
Microsoft Windows and Machine Authentication	12-13

Enabling Machine Authentication	12-15
User-Changeable Passwords with Windows User Databases	12-16
Preparing Users for Authenticating with Windows	12-17
Selecting Remote Agents for Windows Authentication (Solution Engine Only)	12-17
Windows User Database Configuration Options	12-18
Configuring a Windows External User Database	12-21
Machine Authentication Support in a Multi-Forest Environment	12-22
Generic LDAP	12-23
ACS Authentication Process with a Generic LDAP User Database	12-23
Multiple LDAP Instances	12-24
LDAP Organizational Units and Groups	12-24
Domain Filtering	12-24
LDAP Failover	12-25
Successful Previous Authentication with the Primary LDAP Server	12-26
Unsuccessful Previous Authentication with the Primary LDAP Server	12-26
LDAP Admin Logon Connection Management	12-26
Distinguished Name Caching	12-26
LDAP Configuration Options	12-27
Configuring a Generic LDAP External User Database	12-31
ODBC Database (ACS for Windows Only)	12-35
What is Supported with ODBC User Databases	12-36
ACS Authentication Process with an ODBC External User Database	12-36
Preparing to Authenticate Users with an ODBC-Compliant Relational Database	12-37
Implementation of Stored Procedures for ODBC Authentication	12-38
Type Definitions	12-38
Microsoft SQL Server and Case-Sensitive Passwords	12-39
Sample Routine for Generating a PAP Authentication SQL Procedure	12-39
Sample Routine for Generating an SQL CHAP Authentication Procedure	12-40
Sample Routine for Generating an EAP-TLS Authentication Procedure	12-40
PAP Authentication Procedure Input	12-40
PAP Procedure Output	12-41
CHAP/MS-CHAP/ARAP Authentication Procedure Input	12-41
CHAP/MS-CHAP/ARAP Procedure Output	12-42
EAP-TLS Authentication Procedure Input	12-42
EAP-TLS Procedure Output	12-43
Result Codes	12-43
Configuring a System Data Source Name for an ODBC External User Database	12-44
Configuring an ODBC External User Database	12-44
Downloading a Certificate Database (Solution Engine Only)	12-47

LEAP Proxy RADIUS Server Database (Both Platforms)	12-48
Configuring a LEAP Proxy RADIUS Server External User Database	12-49
Token Server User Databases	12-50
About Token Servers and ACS	12-50
Token Servers and ISDN	12-51
RADIUS-Enabled Token Servers	12-51
About RADIUS-Enabled Token Servers	12-51
Token Server RADIUS Authentication Request and Response Contents	12-51
Configuring a RADIUS Token Server External User Database	12-52
Using RSA Token-Card Client Software	12-54
RSA Authentication with LDAP Group Mapping	12-56
Deleting an External User Database Configuration	12-57

CHAPTER 13

Posture Validation 13-1

What is Posture Validation?	13-1
Posture Validation in Network Access Control	13-2
Posture Validation and Network Access Profiles	13-3
Posture Tokens	13-3
The Posture Validation Process	13-4
Policy Overview	13-5
About Posture Credentials and Attributes	13-5
Extended Attributes	13-6
Posture Validation Attribute Data Types	13-6
Internal Policies	13-7
About Internal Policies	13-7
About Rules, Rule Elements, and Attributes	13-8
External Policies	13-8
External Posture Validation Audit Servers	13-9
About External Audit Servers	13-9
How an External Audit Gets Triggered	13-10
Exemption List Support	13-10
Auditing Device Types	13-10
Policy Formation	13-11
User Groups and Device Types	13-11
Group Assignment	13-11
Group Mapping Rules	13-12
Layer 2 Audit for Network Access Control	13-12
Configuring NAC in ACS	13-13

Configuring ACS in a NAC/NAP Environment	13-15
Configuring Policies	13-15
Posture Validation Options	13-15
Setting Up Posture Validation Policies	13-16
Creating an Internal Policy	13-17
Editing a Policy	13-19
Cloning a Policy or Policy Rule	13-20
Renaming a Policy	13-20
Deleting a Policy or Rule	13-21
Deleting a Condition Component or Condition Set	13-21
Setting Up an External Policy Server	13-22
Editing an External Posture Validation Server	13-23
Deleting an External Posture Validation Server	13-23
Setting Up an External AAA Server	13-23
Editing an External Posture AAA Server	13-24
Deleting an External Posture AAA Server	13-25
Setting Up an External Audit Posture Validation Server	13-25
Adding an External Posture Validation Audit Server	13-25
Editing an External Posture Validation Audit Server	13-27
Deleting an External Posture Validation Server	13-27
Audit Processing with MAC Authentication Bypass	13-27
Workflow	13-28
Processing	13-28
Policy Configurations	13-28
Posture Validation Pages Reference	13-30
Posture Validation Components Setup Page	13-30
Internal Posture Validation Setup Pages	13-30
Posture Validation Policies Page	13-30
Posture Validation Policy Page	13-31
Posture Validation Rules for <policy_name> Page	13-31
Posture Validation Rule - <policy_name> Page	13-32
Add/Edit Condition Page	13-33
External Posture Validation Setup Pages	13-33
External Posture Validation Servers Page	13-33
Add/Edit External Posture Validation Server Page	13-34
External Posture Validation Audit Setup Pages	13-36
External Posture Validation Audit Server Page	13-36
External Posture Validation Audit Server Setup Page	13-36

Network Access Profiles	14-1
Overview of NAPs	14-1
Classification of Access Requests	14-2
NAFs	14-2
Protocol Types	14-2
Advanced Filtering	14-2
Profile-based Policies	14-3
Workflow for Configuring NAPs and Profile-based Policies	14-3
Processing Unmatched User Requests	14-3
Managing NAPs	14-4
Adding a Profile	14-4
Ordering Profiles	14-5
Editing a Profile	14-5
Cloning a Profile	14-6
Deleting a Profile	14-6
Using Profile Templates	14-7
Prerequisites for Using Profile Templates	14-7
Creating a Profile with a Profile Template	14-8
Profile Templates	14-8
NAC L3 IP	14-9
NAC L2 IP	14-11
NAC Layer 2 802.1x	14-14
Microsoft IEEE 802.1x	14-16
Wireless (NAC L2 802.1x)	14-17
Agentless Host for L2 (802.1x Fallback)	14-17
Agentless Host for L3	14-18
Agentless Host for L2 and L3	14-20
Configuring Policies for Profiles	14-22
Protocol Configuration for NAPs	14-23
Authentication Protocols	14-23
Agentless Request Processing	14-24
EAP Configuration for NAPs	14-25
EAP-FAST with Posture Validation	14-25
EAP Authentication with RADIUS Key Wrap	14-25
Configuring Protocols	14-26
Authentication Policy Configuration for NAPs	14-27
Credential Validation Databases	14-27
Group Filtering at NAP Level	14-27
Object Identifier Check for EAP-TLS Authentication	14-28

Configuring Authentication Policies	14-28
Posture-Validation Policy Configuration for NAPs	14-29
About Posture Validation Rules	14-29
Setting a Posture-Validation Policy	14-30
Deleting a Posture Validation Rule	14-31
Setting a Posture-Validation Policy to Process Statements of Health	14-32
Deleting a Statement of Health Posture Validation Rule	14-33
Configuring Posture Validation for Agentless Hosts	14-33
Authorization Policy Configuration for NAPs	14-34
About Authorization Rules	14-34
Configuring an Authorization Rule	14-36
Configuring a Default Authorization Rule	14-37
Ordering the Authorization Rules	14-37
Deleting an Authorization Rule	14-38
Troubleshooting Profiles	14-38
Policy Replication and Backup	14-38
Network Access Profiles Pages Reference	14-39
Network Access Profiles Page	14-39
Profile Setup Page	14-40
Create Profile from Template Page	14-43
Protocols Settings for profile_name Page	14-43
Authentication for profile_name Page	14-46
Posture Validation Page	14-48
Posture Validation Rule for profile_name Page	14-48
Select External Posture Validation Audit for profile_name Page	14-49
Authorization Rules for profile_name	14-50

CHAPTER 15

Unknown User Policy 15-1

Known, Unknown, and Discovered Users	15-2
Authentication and Unknown Users	15-3
About Unknown User Authentication	15-3
General Authentication of Unknown Users	15-3
Windows Authentication of Unknown Users	15-4
Domain-Qualified Unknown Windows Users	15-4
Windows Authentication with Domain Qualification	15-5
Multiple User Account Creation	15-5
Performance of Unknown User Authentication	15-6
Added Authentication Latency	15-6
Authentication Timeout Value on AAA clients	15-6

Authorization of Unknown Users	15-6
Unknown User Policy Options	15-6
Database Search Order	15-7
Configuring the Unknown User Policy	15-8
Disabling Unknown User Authentication	15-9

CHAPTER 16

User Group Mapping and Specification 16-1

About User Group Mapping and Specification	16-1
Group Mapping by External User Database	16-1
Creating an ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database	16-2
Group Mapping by Group Set Membership	16-3
Group Mapping Order	16-3
No Access Group for Group Set Mappings	16-4
Default Group Mapping for Windows	16-4
Creating an ACS Group Mapping for Windows or Generic LDAP Groups	16-4
Editing a Windows or Generic LDAP Group Set Mapping	16-6
Deleting a Windows or Generic LDAP Group Set Mapping	16-7
Deleting a Windows Domain Group Mapping Configuration	16-7
Changing Group Set Mapping Order	16-8
RADIUS-Based Group Specification	16-8

APPENDIX A

TACACS+ Attribute-Value Pairs A-1

Cisco IOS AV Pair Dictionary	A-1
TACACS+ AV Pairs	A-1
TACACS+ Accounting AV Pairs	A-3

APPENDIX B

RADIUS Attributes B-1

Before Using RADIUS Attributes	B-1
Cisco IOS Dictionary of RADIUS IETF	B-2
Cisco IOS/PIX 6.0 Dictionary of RADIUS VSAs	B-4
About the cisco-av-pair RADIUS Attribute	B-5
Cisco VPN 3000 Concentrator/ASA/PIX 7.x+ Dictionary of RADIUS VSAs	B-6
Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs	B-10
Cisco Building Broadband Service Manager Dictionary of RADIUS VSA	B-10
Cisco Airespace Dictionary of RADIUS VSA	B-10
IETF Dictionary of RADIUS IETF (AV Pairs)	B-11

Microsoft MPPE Dictionary of RADIUS VSAs	B-19
Ascend Dictionary of RADIUS AV Pairs	B-21
Nortel Dictionary of RADIUS VSAs	B-28
Juniper Dictionary of RADIUS VSAs	B-28
3COMUSR Dictionary of RADIUS VSAs	B-28

APPENDIX C

CSUtil Database Utility C-1

Location of CSUtil.exe and Related Files	C-2
CSUtil Command Syntax	C-2
Backing Up ACS with CSUtil.exe	C-3
Restoring ACS with CSUtil.exe	C-4
Initializing the ACS Internal Database	C-5
Creating an ACS Internal Database Dump File	C-6
Loading the ACS Internal Database from a Dump File	C-7
Cleaning up the ACS Internal Database	C-8
User and AAA Client Import Option	C-9
Importing User and AAA Client Information	C-9
User and AAA Client Import File Format	C-10
About User and AAA Client Import File Format	C-10
ONLINE or OFFLINE Statement	C-11
ADD Statements	C-11
UPDATE Statements	C-12
DELETE Statements	C-13
ADD_NAS Statements	C-14
DEL_NAS Statements	C-15
Import File Example	C-15
Exporting User List to a Text File	C-15
Exporting Group Information to a Text File	C-16
Decoding Error Numbers	C-17
User-Defined RADIUS Vendors and VSA Sets	C-17
About User-Defined RADIUS Vendors and VSA Sets	C-18
Adding a Custom RADIUS Vendor and VSA Set	C-18
Support for User-Defined Vendors Extended VSA ID	C-19
Using the CSUtil.ini file to Install User-Defined Vendor or VSA Data	C-19
Deleting a Custom RADIUS Vendor and VSA Set	C-20
Listing Custom RADIUS Vendors	C-21
Exporting Custom RADIUS Vendor and VSA Sets	C-21
RADIUS Vendor/VSA Import File	C-22

About the RADIUS Vendor/VSA Import File	C-22
Vendor and VSA Set Definition	C-23
Attribute Definition	C-23
Enumeration Definition	C-24
Example RADIUS Vendor/VSA Import File	C-25
PAC File Generation	C-26
PAC File Options and Examples	C-26
Generating PAC Files	C-28
Posture-Validation Attributes	C-29
Posture-Validation Attribute Definition File	C-29
Exporting Posture-Validation Attribute Definitions	C-32
Importing Posture-Validation Attribute Definitions	C-32
Importing External Audit Posture-Validation Servers	C-34
Deleting a Posture-Validation Attribute Definition	C-34
Deleting an Extended Posture-Validation Attribute Definition	C-35
Default Posture-Validation Attribute Definition File	C-36
Adding External Audit Device Type Attributes	C-40
Adding and Editing Devices Using the CSUtil Utility	C-41

APPENDIX D

VPDN Processing D-1

VPDN Process	D-1
--------------	-----

APPENDIX E

RDBMS Synchronization Import Definitions E-1

accountActions Specification	E-1
accountActions Format	E-2
accountActions Mandatory Fields	E-2
accountActions Processing Order	E-3
Supported Versions for ODBC Data Sources (ACS for Windows)	E-3
Action Codes	E-3
Action Codes for Setting and Deleting Values	E-4
Action Codes for Creating and Modifying User Accounts	E-5
Action Codes for Initializing and Modifying Access Filters	E-10
Action Codes for Modifying TACACS+ and RADIUS Group and User Settings	E-13
Action Codes for Modifying Network Configuration	E-18
ACS Attributes and Action Codes	E-23
User-Specific Attributes	E-24
User-Defined Attributes	E-25
Group-Specific Attributes	E-26

Using the RDBMS Synchronization Action Codes to Install User-Defined Vendor or VSA Data	E-27
Action Codes for dACL Attributes	E-27
Sample File Format for dACLs: DumpACL.txt	E-30
Sample File Format for Dump NAS: DumpNAS.txt	E-30
An Example of accountActions	E-30

APPENDIX F

Internal Architecture	F-1
Windows Services	F-1
Windows Registry (ACS for Windows Only)	F-2
SQL Registry	F-2
Solution Engine Services	F-3
Operating System Services the ACS SE Automatically Runs	F-3
Disabled Operating System Services in the ACS SE	F-4
Packet Filtering	F-6
CSAdmin	F-7
CSAgent (ACS SE Only)	F-8
CSAgent Policies	F-8
CSAuth	F-9
CSDBSync	F-9
CSLog	F-9
CSMon	F-10
Monitoring	F-10
Recording	F-11
Notification	F-11
Response	F-11
CSTacacs and CSRADIUS	F-12
Disabling NetBIOS	F-12

INDEX



Preface

Audience

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

Organization



Note

This release of the User Guide combines the Windows and Solution Engine platforms. Where necessary, the appropriate platform is clearly identified.

This document contains the following chapters and appendixes:

- **Chapter 1, “Overview”**—An overview of ACS and its features, network diagrams, and system requirements.
- **Chapter 2, “Using the Web Interface”**—Concepts and procedures regarding how to use the Interface Configuration section of ACS to configure the HTML interface.
- **Chapter 3, “Network Configuration”**—Concepts and procedures for establishing ACS network configuration and building a distributed system.
- **Chapter 4, “Shared Profile Components”**—Concepts and procedures regarding ACS shared profile components: downloadable IP ACLs, network access filters, network access restrictions, and device command sets.
- **Chapter 5, “User Group Management”**—Concepts and procedures for establishing and maintaining ACS user groups.
- **Chapter 6, “User Management”**—Concepts and procedures for establishing and maintaining ACS user accounts.
- **Chapter 7, “System Configuration: Basic”**—Concepts and procedures regarding the basic features found in the System Configuration section of ACS.
- **Chapter 8, “System Configuration: Advanced”**—Concepts and procedures regarding RDBMS Synchronization, ACS Internal Database Replication, and IP pools, found in the System Configuration section of ACS.
- **Chapter 9, “System Configuration: Authentication and Certificates”**—Concepts and procedures regarding the Global Authentication and ACS Certificate Setup pages, found in the System Configuration section of ACS.

- **Chapter 10, “Logs and Reports”**—Concepts and procedures regarding ACS logging and reports.
- **Chapter 11, “Administrators and Administrative Policy”**—Concepts and procedures for establishing and maintaining ACS administrators.
- **Chapter 12, “User Databases”**—Concepts about user databases and procedures for configuring ACS to perform user authentication with external user databases.
- **Chapter 13, “Posture Validation”**—Concepts and procedures for implementing Posture Validation (also known as Network Admission Control or NAC) and configuring posture validation policies.
- **Chapter 14, “Network Access Profiles”**—Concepts and procedures for creating Network Access Profiles and implementing profile-based policies in ACS.
- **Chapter 15, “Unknown User Policy”**—Concepts and procedures about using the Unknown User Policy with posture validation and unknown user authentication.
- **Chapter 16, “User Group Mapping and Specification”**—Concepts and procedures regarding the assignment of groups for users authenticated by an external user database.
- **Appendix A, “TACACS+ Attribute-Value Pairs”**—A list of supported TACACS+ AV pairs and accounting AV pairs.
- **Appendix B, “RADIUS Attributes”**—A list of supported RADIUS AV pairs and accounting AV pairs.
- **Appendix C, “CSUtil Database Utility”**—Instructions for using CSUtil.exe, a command line utility you can use to work with the ACS internal database, to import AAA clients and users, to define RADIUS vendors and attributes, and to generate (Protected Access Credentials) PAC files for EAP-FAST clients.
- **Appendix D, “VPDN Processing”**—An introduction to Virtual Private Dial-up Networks (VPDN), including stripping and tunneling, with instructions for enabling VPDN on ACS.
- **Appendix E, “RDBMS Synchronization Import Definitions”**—A list of import definitions, for use with the RDBMS Synchronization feature.
- **Appendix F, “Internal Architecture”**—A description of ACS architectural components.

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	boldface font
Variables for which you supply values and new or important terminology	<i>italic font</i>
Displayed session and system information, paths and file names	screen font
Information you enter	boldface screen font
Variables you enter	<i>italic screen font</i>
Menu items and button names	boldface font
Indicates menu items to select, in the order you select them.	Option > Network Preferences

**Tip**

Identifies information to help you get the most benefit from your product.

**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.

**Caution**

Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

**Warning**

Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.

Product Documentation

**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 I-1 describes the product documentation that is available.

Table I-1 **Product Documentation**

Document Title	Available Formats
<i>Documentation Guide for Cisco Secure ACS Release 4.2</i>	<ul style="list-style-type: none"> Shipped with product. PDF on the product CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html
<i>Release Notes for Cisco Secure ACS Release 4.2</i>	<ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html
<i>Configuration Guide for Cisco Secure ACS Release 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs42_config_guide.html

Table I-1 Product Documentation (continued)

Document Title	Available Formats
<i>Installation Guide for Cisco Secure ACS for Windows Release 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html
<i>Installation Guide for Cisco Secure ACS Solution Engine Release 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/SE42.html
<i>User Guide for Cisco Secure Access Control Server 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html <p>You can also access the user guide by clicking Online Documentation in the ACS navigation bar. The user guide PDF is available on this page by clicking View PDF.</p>
<i>Regulatory Compliance and Safety Information for the Cisco Secure ACS Solution Engine Release 4.2</i>	<ul style="list-style-type: none"> Shipped with product. PDF on the product CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/RCSI_42.html
<i>Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/remote_agent/rmag42.html
<i>Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.2</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html
<i>Installation and User Guide for Cisco Secure ACS User-Changeable Passwords</i>	<ul style="list-style-type: none"> PDF on the ACS Recovery CD-ROM. On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/user_passwords/ucp42.html

Table I-1 **Product Documentation (continued)**

Document Title	Available Formats
<i>Cisco Secure Access Control Server Troubleshooting Guide</i>	<ul style="list-style-type: none"> On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACS_Troubleshooting.html
Online Documentation	In the ACS HTML interface, click Online Documentation.
Online Help	In the ACS HTML interface, online help appears in the right-hand frame when you are configuring a feature.

Related Documentation



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.

A set of white papers about ACS are available on Cisco.com at:

<http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml>

For information on Network Admission Control, various NAC components, and ACS see:

<http://www.cisco.com/go/NAC>

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.

Open Source License Acknowledgements

The following acknowledgements 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:

© 1998-1999 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 (ey@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

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

This package is an SSL implementation written by Eric Young (ey@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].



TABLES

Table I-1	Product Documentation	I-XXIX
Table 1-1	TACACS+ and RADIUS Protocol Comparison	1-3
Table 1-2	Non-EAP Authentication Protocol and User Database Compatibility	1-8
Table 1-3	EAP Authentication Protocol and User Database Compatibility	1-8
Table 1-4	The PAP, CHAP, and ARAP Protocols	1-9
Table 1-5	EAP Protocol Support	1-10
Table 1-6	Online Documentation	1-23
Table 2-1	RADIUS Listings in Interface	2-7
Table 2-2	Interface Configuration Page	2-10
Table 2-3	Configure User Defined Fields	2-10
Table 2-4	TACACS+ Services	2-11
Table 2-5	Displayable TACACS+ Advanced Options	2-12
Table 2-6	Displayable RADIUS Settings	2-13
Table 2-7	Advanced Options (for Interface Configuration)	2-14
Table 4-1	802.1X Example SPC Scenario	4-2
Table 4-2	RAC Display Fields	4-12
Table 4-3	RAC Configuration Fields	4-12
Table 4-4	Add or Edit RAC Attributes Fields	4-13
Table 4-5	NAR Permit or Deny Conditions	4-18
Table 4-6	Attributes for IP-Based NAR Filters	4-19
Table 4-7	Attributes for IP-Based Restrictions	4-20
Table 4-8	Attributes for DNIS/CLI-Based Restrictions	4-21
Table 8-1	Replication Component Descriptions	8-8
Table 8-2	Outbound Replication Options	8-9
Table 8-3	Account Action Codes to Create, Read, Update, Delete for AAA Clients	8-23
Table 8-4	Account Action Codes for Creating, Reading, Updating, or Deleting a dACL	8-25
Table 8-5	List of Fatal Errors	8-38
Table 9-1	Master Key versus PAC States	9-17
Table 9-2	EAP-FAST Components and Replication	9-18
Table 9-3	Certificate Subject Fields	9-32

Table 10-1	AAA-Related Log Descriptions	10-2
Table 10-2	Audit Log Descriptions	10-5
Table 10-3	Default CSV Log File Locations	10-6
Table 10-4	Dynamic Administration Report Descriptions	10-11
Table 10-5	Entitlement Report Descriptions	10-12
Table 10-6	Descriptive Request Text and Request Code	10-14
Table 10-7	Descriptive Status Text and Request Code	10-17
Table 10-8	Regular Expression Syntax Definitions	10-32
Table 10-9	Logging Configuration Page	10-38
Table 10-10	Critical Loggers Configuration Page	10-38
Table 10-11	Remote Logging Setup Page	10-39
Table 10-12	Logging Configuration Page	10-39
Table 10-13	CSV log File Configuration Page	10-40
Table 10-14	Syslog log File Configuration Page	10-41
Table 10-15	ODBC log Configuration Page	10-42
Table 10-16	Services Log File Configuration Page	10-43
Table 10-17	Reports Page	10-44
Table 10-18	Audit Log Attributes	10-46
Table 11-1	Group Access Options	11-3
Table 11-2	Administration Control (Privileged Administrator)	11-10
Table 11-3	Add Administrator and Edit Administrator Pages	11-11
Table 11-4	Administrator Password Policy	11-17
Table 11-5	Access Policy Options	11-18
Table 11-6	Session Policy	11-20
Table 12-1	PAP Stored Procedure Input	12-40
Table 12-2	PAP Stored Procedure Results	12-41
Table 12-3	CHAP Stored Procedure Input	12-41
Table 12-4	CHAP/MS-CHAP/ARAP Stored Procedure Results	12-42
Table 12-5	EAP-TLS Stored Procedure Input	12-42
Table 12-6	EAP-TLS Stored Procedure Results	12-43
Table 12-7	Result Codes	12-43
Table 13-1	ACS Posture Tokens	13-3
Table 13-2	Audit Policy Requirements	13-9
Table 13-3	Posture Validation Options	13-16
Table 13-4	Agentless Host Authentication and Authorization Support	13-28

Table 13-5	Posture Validation Components Setup Page	13-30
Table 13-6	Posture Validation Policies Page	13-31
Table 13-7	Posture Validation Policy Page	13-31
Table 13-8	Posture Validation Rules for <policy_name> Page	13-32
Table 13-9	Posture Validation Rule - <policy_name> Page	13-32
Table 13-10	Add/Edit Condition Page	13-33
Table 13-11	External Posture Validation Servers Page	13-34
Table 13-12	Add/Edit External Posture Validation Server Page	13-34
Table 13-13	External Posture Validation Audit Server Setup Options	13-37
Table 14-1	NAC Layer 3 IP Profile Sample	14-9
Table 14-2	Authorization Rules for NAC Layer 3 IP Profile Template	14-10
Table 14-3	Posture Validation for NAC Layer 3 IP Sample	14-11
Table 14-4	Shared Profile Components for NAC Layer 3 IP Sample	14-11
Table 14-5	NAC Layer 2 IP Profile Sample	14-13
Table 14-6	Authorization Rules for NAC Layer 2 IP Profile Template	14-13
Table 14-7	Posture Validation for NAC Layer 2 IP Sample	14-14
Table 14-8	NAC L2 802.1x Profile Sample	14-14
Table 14-9	Authorization Rules for NAC Layer 2 801.x Profile Sample	14-15
Table 14-10	Posture Validation for NAC Layer 2 802.1x Profile Sample	14-16
Table 14-11	Shared Profile Components for NAC Layer 2 802.1x Profile Template	14-16
Table 14-12	Microsoft IEEE 802.1x Profile Sample	14-17
Table 14-13	Authorization Rules for Microsoft IEEE 802.1x Profile Sample	14-17
Table 14-14	Agentless Host for L2 (802.1x Fallback) Sample Profile	14-18
Table 14-15	Authorization Rules for Agentless Host for L2 (802.1x Fallback) Sample Profile	14-18
Table 14-16	Agentless Host for L3 Sample Profile Template	14-18
Table 14-17	Shared Profile Components for Agentless Host for L3 Sample	14-20
Table 14-18	Agentless Host for L2 and L3 Sample Profile Template	14-20
Table 14-19	Shared Profile Components for Agentless Host for L3 and L3 Sample	14-22
Table 14-20	Network Access Profiles Page	14-40
Table 14-21	Profile Setup Page	14-41
Table 14-22	Create Profile from Template Page	14-43
Table 14-23	Protocols and EAP Configuration Page	14-43
Table 14-24	Authentication Settings Page	14-46
Table 14-25	Posture Validation Page for profile_name Page	14-48
Table 14-26	Posture Validation Rule for profile_name Page	14-48

Table 14-27	Authorization Rules for profile_name	14-50
Table B-1	Cisco IOS Software RADIUS AV Pairs	B-3
Table B-2	Cisco IOS/PIX 6.0 RADIUS VSAs	B-4
Table B-3	Cisco VPN 3000 Concentrator /ASA/PIX 7.x+ RADIUS VSAs	B-7
Table B-4	Cisco VPN 5000 Concentrator RADIUS VSAs	B-10
Table B-5	Cisco BBSM RADIUS VSA	B-10
Table B-6	Cisco Airespace RADIUS Attributes	B-11
Table B-7	RADIUS (IETF) Attributes	B-11
Table B-8	Microsoft MPPE RADIUS VSAs	B-20
Table B-9	Ascend RADIUS Attributes	B-22
Table B-10	Nortel RADIUS VSAs	B-28
Table B-11	Juniper RADIUS VSAs	B-28
Table B-12	3COMUSR RADIUS VSAs	B-29
Table C-1	CSUtil Options	C-2
Table C-2	ONLINE/OFFLINE Statement Tokens	C-11
Table C-3	ADD Statement Tokens	C-12
Table C-4	UPDATE Statement Tokens	C-13
Table C-5	UPDATE Statement Tokens	C-13
Table C-6	ADD_NAS Statement Tokens	C-14
Table C-7	DEL_NAS Statement Tokens	C-15
Table C-9	RADIUS VSA Import File Section Types	C-23
Table C-10	Vendor and VSA Set Keys	C-23
Table C-11	Attribute Definition Keys	C-24
Table C-12	Enumerations Definition Keys	C-25
Table E-1	accountActions Fields	E-2
Table E-2	Action Codes for Setting and Deleting Values	E-5
Table E-3	User Creation and Modification Action Codes	E-5
Table E-4	Action Codes for Initializing and Modifying Access Filters	E-11
Table E-5	Action Codes for Modifying TACACS+ and RADIUS Group and User Settings	E-13
Table E-6	Action Codes for Modifying Network Configuration	E-19
Table E-7	User-Specific Attributes	E-24
Table E-8	User-Defined Attributes	E-25
Table E-9	Group-Specific Attributes	E-26
Table 10	RDBMS Account Action Codes and Definition for Vendor Configuration	E-27
Table E-11	Action Codes for Modifying dACL Attributes	E-28

<i>Table E-12</i>	Example accountActions Table	E-30
<i>Table F-1</i>	Operating Services that the ACS SE Automatically Runs	F-3
<i>Table F-2</i>	Operating System Services Not Run on the ACS SE	F-4
<i>Table F-3</i>	Input Traffic Open Ports for the Packet Filter	F-7



CHAPTER 1

Overview

This chapter contains an overview of the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

The following topics are presented:

- [Introduction to ACS, page 1-1](#)
- [ACS Features, Functions and Concepts, page 1-3](#)
- [Managing and Administrating ACS, page 1-16](#)
- [ACS Specifications, page 1-22](#)
- [Online Documentation Reference, page 1-23](#)
- [Related Documentation, page 1-24](#)

Introduction to ACS

ACS is a scalable, high-performance Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+) security server. As the centralized control point for managing enterprise network users, network administrators, and network infrastructure resources, ACS provides a comprehensive identity-based network-access control solution for Cisco intelligent information networks.

ACS extends network-access security by combining traditional authentication, authorization, and accounting (AAA) (pronounced "triple-A") with policy control. ACS enforces a uniform network-access security policy for network administrators and other network users.

ACS extends network-access security by combining AAA with policy control from a centralized identity-based networking framework. This combination gives enterprise networks greater flexibility, mobility, and security, resulting in user-productivity gains.

ACS supports a broad variety of Cisco and other network-access devices (NADs), also known as AAA clients, including:

- Wired and wireless LAN switches and access points
- Edge and core routers
- Dialup and broadband terminators
- Content and storage devices
- Voice over IP (VoIP)
- Firewalls

- Virtual private networks (VPNs)

Figure 1-1 on page 1-2 illustrates the role of ACS as a traditional network access control/AAA server.

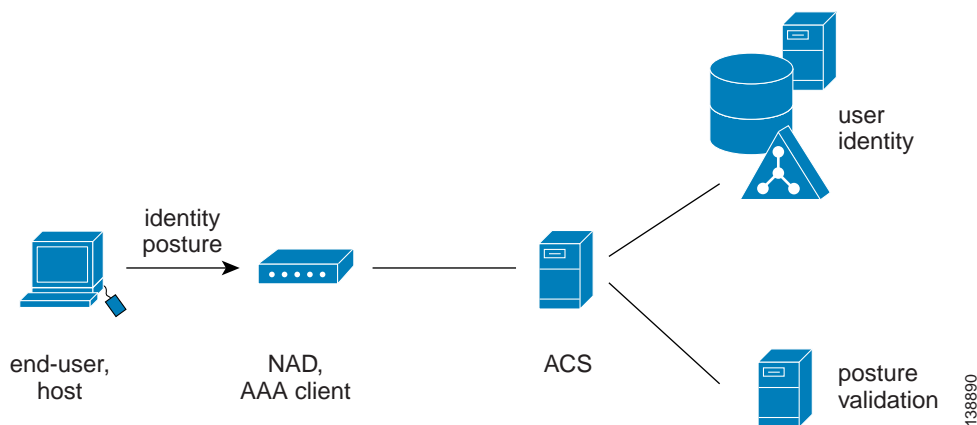
Figure 1-1 A Simple AAA Scenario



Network Admission Control (NAC)

ACS is a critical component of the Cisco Network Admission Control (NAC) framework. Cisco NAC is a Cisco Systems-sponsored industry initiative that uses the network infrastructure to enforce security-policy compliance on all machines seeking to access network computing resources, thereby limiting damage from viruses and worms. With NAC, network access to compliant and trusted PCs can be permitted, while the access of noncompliant devices can be restricted. See Figure 1-2.

Figure 1-2 ACS Extended to NAC



Identity-Based Networking Services (IBNS)

ACS is also an important component of the Cisco Identity-Based Networking Services (IBNS) architecture. Cisco IBNS is based on Extensible Authentication Protocol (EAP) and on port-security standards such as IEEE 802.1x (a standard for port-based network-access control) to extend security authentication, authorization, and accounting from the perimeter of the network to every connection point inside the LAN. New policy controls such as per-user quotas, virtual LAN (VLAN) assignments, and access-control lists (ACLs) can be deployed, due to the extended capabilities of Cisco switches and wireless access points to query ACS over the RADIUS protocol.

ACS Features, Functions and Concepts

ACS incorporates many technologies to render AAA services to network-access devices, and provides a central access-control function.

This section contains:

- [ACS as the AAA Server, page 1-3](#)
- [AAA Protocols—TACACS+ and RADIUS, page 1-3](#)
- [Additional Features in This Release, page 1-5](#)
- [Authentication, page 1-7](#)
- [Authorization, page 1-12](#)
- [Accounting, page 1-15](#)

ACS as the AAA Server

ACS functions as an AAA server for one or more NADs. The NADs are AAA clients of the ACS server. You must configure each client NAD to direct end-user host access requests to the ACS by using the TACACS+ or RADIUS protocols.

TACACS+ is traditionally used to provide authorization for network administrative operations on the network infrastructure itself; RADIUS is universally used to secure the access of end-users to network resources.

Basically, 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 its internal database or one of the configured external identity directories. ACS ultimately responds to the NAD with an access denied or an access-accept message with a set of authorization attributes. When ACS is used in the context of the NAC architecture, additional machine data, known as *posture*, is validated as well, before the user is granted access to the network.

AAA Protocols—TACACS+ and RADIUS

ACS can use the TACACS+ and RADIUS AAA protocols.

[Table 1-1](#) compares the two protocols.

Table 1-1 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
Ports Used	49	Authentication and Authorization: 1645 and 1812 Accounting: 1646 and 1813
Encryption	Full packet 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

TACACS+

ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.78. For more information, refer to the Cisco IOS software documentation at <http://www.cisco.com>.

RADIUS

ACS conforms to the RADIUS protocol as defined in the draft of April 1997 and in the following Requests for Comments (RFCs):

- RFC 2138, Remote Authentication Dial In User Service
- RFC 2139, RADIUS Accounting
- RFC 2284
- RFC 2865
- RFC 2866
- RFC 2867
- RFC 2868
- RFC 2869

The ports used for authentication and accounting have changed in RADIUS RFC documents. To support the older and newer RFCs, ACS accepts authentication requests on port 1645 and port 1812. For accounting, ACS accepts accounting packets on port 1646 and 1813.

In addition to support for standard Internet Engineering Task Force (IETF) RADIUS attributes, ACS includes support for RADIUS vendor-specific attributes (VSAs). We have predefined the following RADIUS VSAs in ACS:

- Cisco Airespace
- Cisco Aironet
- Cisco Building Broadband Service Manager (BBSM)
- RADIUS (3COMUSR)
- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX 7.x+
- Cisco VPN 5000
- RADIUS IETF
- RADIUS Ascend
- RADIUS Juniper
- RADIUS Nortel
- RADIUS iPass

ACS also supports up to 10 RADIUS VSAs that you define. After you define a new RADIUS VSA, you can use it as you would one of the RADIUS VSAs that come predefined in ACS. In the Network Configuration section of the ACS web interface, you can configure AAA clients to use a user-defined RADIUS VSA as the AAA protocol. In Interface Configuration, you can enable user-level and group-level attributes for user-defined RADIUS VSAs. In User Setup and Group Setup, you can configure the values for enabled attributes of a user-defined RADIUS VSA.

For more information about creating user-defined RADIUS VSAs, see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#).

Platforms

ACS is available on two platforms, ACS for Windows and ACS for the Solution Engine. ACS for Windows is a software platform. The ACS Solution Engine is a hardware and software platform that requires a network appliance and is hereafter referred to as ACS SE.

The platforms are nearly identical. However, only Windows supports Open Database Connectivity (ODBC) databases, and the **CSUtil.exe** database utility. This guide identifies information exclusively belonging to one platform as “ACS for Windows only” or “ACS SE only.” All other text belongs to both platforms.

Additional Features in This Release

This release of ACS provides the following features that protect networked business systems:

- **Transition to the Windows 2003 Operating System for the ACS SE**
- **Turning ICMP ping on/off (ACS SE)**—On the ACS SE, you can turn the ICMP ping response on or off. In some cases, another network device must receive a valid ICMP ping response before sending an authentication request.
- **Native RSA (ACS SE)**—Support of RSA proprietary interface on the ACS SE has been added.
- **Programmatic interface enhancements for RDBMS Synchronization**—RDBMS synchronization has added capabilities for dACLs. You can create, update, and delete user-level and group-level downloadable ACLs through RDBMS synchronization.
- **Enabling SSH client remote invocation for RDBMS Synchronization for the ACS SE**—A command line interface has been added to change the ACS configuration through remote systems. A SSH server has been added as a service in the ACS SE, so that you can connect from any SSH client to the ACS SE and use the CSDBSync command to perform database synchronization options.
- **Enabling CLI RDBMS Synchronization invocation for ACS for Windows.**
- **NetBIOS disabling**—In ACS for Windows you can now disable NetBIOS on the server on which it is running.
- **Logging enhancements**—Enhance CSV generated log messages. Passed and failed authentication reports now include Response Time, Session-ID and Framed-IP-Address attributes.
- **Upgrade features**—ACS now has a new mechanism that allows you to restore ACS 4.1 backup information to ACS 4.2. Previous ACS configuration is preserved. This feature eliminates the problem of upgrading existing ACS 4.1 configuration to ACS 4.2.
- **Group filtering at NAP level when using LDAP**—When using LDAP to query an external user database, you can perform group filtering at the Network Access Profile level. Depending on the user's external database group membership, ACS can reject or accept access to the network based on the group filtering settings.
- **RSA authentication with LDAP group mapping**—ACS can authenticate with RSA and at the same time perform group mapping with LDAP. Administrators can now use this option to control authorization based on a user's LDAP group membership.
- **EAP_FAST options:**

- **EAP-FAST enhancement for anonymous TLS renegotiation**—ACS allows an anonymous TLS handshake between the end-user client and ACS. EAP-MSCHAP is used as the only inner method in Phase 0 of EAP-FAST.
- **EAP-FAST enhancement for an invalid PAC**—ACS provides an option to run EAP-FAST without issuing or accepting any tunnel or machine PACs, when it receives an invalid PAC. All requests for PACs are ignored. ACS responds with a Success-TLV even though no valid PAC is present. All the relevant PAC options are disabled when you hose this option.
- **EAP-TLS - PAC less and no Active Directory processing EAP-TLS**—ACS supports EAP-FAST tunnel establishment without PACs, or client certificate lookup.
- **Option of disabling caching of dynamic users**—Administrators may determine whether they want disable the creation of dynamic users while using an external database for authentication. Minimal performance disruption occurs when disabling caching of dynamic users
- **Active Directory multi forest support**—ACS supports authentication in a multi-forest environment. Active Directory authentication succeeds as long as an appropriate trust relationship exists between the primary ACS forest and the requested domain's forest.
- **Time configuration**—You can set the ACS SE to the local or GMT time zone. Log viewing and syslog can receive local or GMT time zone stamps.
- **Temporary Elevated User Privileges**—ACS supports granting administrator privileges temporarily to another user.
- **Object Identifier (OID) Check for EAP-TLS Authentication**—ACS checks the OID against the Enhanced Key Usage (EKU) field in the user's certificate.
- **Layer 2 Audit for Network Access Control**—ACS supports auditing agentless hosts connected to a Layer 2 Network Access Device (NAD).
- **ACS for Windows now includes the CSSupport utility.**
- **UTF-8 Support**—ACS supports the use of UTF-8 (the 8-bit Universal Coded Character Set (UCS)/Unicode Transformation Format) for the username and password only when authenticating with Active Directory.
- **Adding devices through CSUtil**—ACS now supports using the CSUtil *import.txt* file for adding and editing authentication, authorization, and accounting (AAA) devices.
- **ACS now supports 3COMUSR VSAs.**
- **User-defined vendors extended VSA ID**— You can use CSUtil or RDBMS synchronization to install dictionary components for vendors that require extended VSA ID length.
- **Customizing a Workstation Name for Windows Authentication**—ACS now supports multiple ACS deployments by using a single Active Directory tree.
- **Configuring the ACS RADIUS Server to reject or discard requests to an external ODBC Database**
- **Improved Diagnostic Logs** —Diagnostic log files contain the line number of the source code that generated the error.The CSAuth diagnostic log now includes Session IDs.
- **Improved EAP Code Debug Messages**—All EAP debug messages are now reported to the CSAuth diagnostic log.
- **RADIUS Key Wrap is now extended to all EAP protocols.**

Authentication

Authentication determines user identity and verifies the information. Traditional authentication uses a name and a fixed password. More secure methods use technologies such as Challenge Authentication Handshake Protocol (CHAP) and One-time Passwords (OTPs). 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.

This section contains:

- [Authentication Considerations, page 1-7](#)
- [Authentication and User Databases, page 1-7](#)
- [Authentication Protocol-Database Compatibility, page 1-8](#)
- [Passwords, page 1-8](#)
- [Other Authentication-Related Features, page 1-12](#)

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 capturing 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, such as:

- 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 User Database
- Generic Lightweight Directory Access Protocol (LDAP)
- LEAP Proxy Remote Access Dial-In User Service (RADIUS) servers
- Token servers
- Open Database Connectivity (ODBC)-compliant relational databases (ACS for Windows)

Authentication Protocol-Database Compatibility

The various password protocols that ACS supports for authentication are supported unevenly by the various databases that ACS supports. For more information about the password protocols that ACS supports, see [Passwords, page 1-8](#).

[Table 1-2](#) specifies non-EAP authentication protocol support.

Table 1-2 Non-EAP Authentication Protocol and User Database Compatibility

Database	ASCII/PAP	CHAP	ARAP	MS-CHAP v.1	MS-CHAP v.2
ACS	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes
Windows AD	Yes	No	No	Yes	Yes
LDAP	Yes	No	No	No	No
ODBC (ACS for Windows only)	Yes	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes
All Token Servers	Yes	No	No	No	No

[Table 1-3](#) specifies EAP authentication protocol support.

Table 1-3 EAP Authentication Protocol and User Database Compatibility

Database	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTC)	PEAP (EAP-MS CHAPv2)	PEAP (EAP-TLS)	EAP-FAST Phase Zero	EAP-FAST Phase Two
ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes	No	Yes	Yes
Windows AD	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
LDAP	No	No	Yes	Yes	No	Yes	No	Yes
ODBC (ACS for Windows only)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes	No	Yes	Yes
All Token Servers	No	No	No	Yes	No	No	No	No

Passwords

ACS supports many common password protocols:

- ASCII/Password Authentication Protocol (ASCII/PAP)
- CHAP
- MS-CHAP
- Lightweight and Efficient Application Protocol (LEAP)

- AppleTalk Remote Access Protocol (ARAP)
- EAP-MD5
- EAP-TLS
- PEAP(EAP-GTC)
- PEAP(EAP-MSCHAPv2)
- PEAP(EAP-TLS)
- EAP-FAST

Passwords can be processed by using these password-authentication protocols based on the version and type of security-control protocol used (for example, RADIUS or TACACS+), and the configuration of the AAA client and end-user client. The following sections outline the different conditions and functions of password handling.

In the case of token servers, ACS acts as a client to the token server by using its proprietary API or its RADIUS interface, depending on the token server. For more information, see [About Token Servers and ACS, page 12-50](#).

Different levels of security can be concurrently used with ACS for different requirements. The basic user-to-network security level is PAP. Although PAP provides unencrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows database. With this configuration, users need to log in only once. CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client. You can use CHAP with the ACS internal database. ARAP support is included to support Apple clients.

Comparing PAP, CHAP, and ARAP

PAP, CHAP, and ARAP are authentication protocols that encrypt passwords. However, each protocol provides a different level of security. [Table 1-4](#) describes the security associated with each protocol.

Table 1-4 *The PAP, CHAP, and ARAP Protocols*

Protocol	Security
PAP	Uses clear-text passwords (that is, unencrypted passwords) and is the least sophisticated authentication protocol. If you are using the Windows user database to authenticate users, you must use PAP password encryption or Microsoft-Challenge Authentication Handshake Protocol (MS-CHAP).
CHAP	Uses a challenge-response mechanism with one-way encryption on the response. You use CHAP to enable 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.
ARAP	Uses a two-way challenge-response mechanism. The AAA client challenges the end-user client to authenticate itself, and the end-user client challenges the AAA client to authenticate itself.

MS-CHAP

ACS supports MS-CHAP for user authentication. Differences between MS-CHAP and standard CHAP are:

- The MS-CHAP Response packet is in a format compatible with Microsoft Windows and LAN Manager 2.x. The MS-CHAP format does not require the authenticator to store a clear-text or reversibly encrypted password.
- MS-CHAP provides an authentication-retry mechanism that the authenticator controls.
- MS-CHAP provides additional failure codes in the Failure packet Message field.

For more information on MS-CHAP, refer to RFC 2433 [Microsoft PPP CHAP Extensions](#) for RADIUS Attributes for MS-CHAP Support.

EAP Support

The EAP, based on IETF 802.1x, is an end-to-end framework that allows the creation of authentication types without changing AAA client configurations. For more information about EAP, see RFC 2284, [PPP Extensible Authentication Protocol \(EAP\)](#).

ACS supports several EAP protocols. [Table 1-5](#) describes each supported protocol.

Table 1-5 *EAP Protocol Support*

EAP Protocol	Description
EAP-MD5	An EAP protocol that does not support mutual authentication.
EAP-TLS	EAP incorporating Transport Layer Security. For more information, see EAP-TLS Deployment Guide for Wireless LAN Networks and EAP-TLS Authentication, page 9-2 .
LEAP	An EAP protocol that Cisco Aironet wireless equipment uses; it supports mutual authentication.
PEAP	Protected EAP, which is implemented with EAP-Generic Token Card (GTC), EAP-TLS and EAP-MS-CHAPv2 protocols. For more information, see PEAP Authentication, page 9-6 .
EAP-FAST	A faster means of encrypting EAP authentication, supports EAP-GTC authentication. For more information, see EAP-FAST Authentication, page 9-9 .

The architecture of ACS is extensible with regard to EAP; additional varieties of EAP will be supported as those protocols mature.

Basic Password Configurations

Several basic password configurations are available:



Note

These configurations are all classed as inbound authentication.

- **Single password for ASCII/PAP/CHAP/MS-CHAP/ARAP**—The most convenient method for the administrator when setting up accounts and the user when obtaining authentication. However, because the CHAP password is the same as the PAP password, and the PAP password is transmitted in clear text during an ASCII/PAP login, the CHAP password could be compromised.
- **Separate passwords for ASCII/PAP and CHAP/MS-CHAP/ARAP**—For a higher level of security, users can have two separate passwords. If the ASCII/PAP password is compromised, the CHAP/ARAP password can remain secure.

- **External user database authentication**—For authentication by an external user database, the user does not need a password stored in the ACS internal database. Instead, ACS records which external user database it should query to authenticate the user.

Advanced Password Configurations

ACS supports the following advanced password configurations:

- **Inbound passwords**—Passwords used by most ACS users. The TACACS+ and RADIUS protocols support these passwords. The passwords are held in the ACS internal database and are not usually provided to an external source if an outbound password has been configured.
- **Outbound passwords**—The TACACS+ protocol supports outbound passwords that can be used, for example, when another AAA client and end-user client authenticate a AAA client. Passwords from the ACS internal database are then sent to the second AAA client and end-user client.
- **Token caching**—When token caching is enabled, ISDN users can connect (for a limited time) to a second B Channel by using the same OTP that was entered during original authentication. For greater security, the B-Channel authentication request from the AAA client should include the OTP in the username value (for example, *Fredpassword*) while the password value contains an ASCII/PAP/ARAP password. The TACACS+ and RADIUS servers then verify that the token is still cached and validate the incoming password against the single ASCII/PAP/ARAP or separate CHAP/ARAP password, depending on the configuration that the user employs.

You use the TACACS+ SENDAUTH feature to allow AAA clients to authenticate themselves to other AAA clients or an end-user clients via outbound authentication. The outbound authentication can be PAP, CHAP, or ARAP. With outbound authentication, the ACS password is given out. By default, ASCII/PAP or CHAP/ARAP password is used, depending on how this has been configured; however, we recommend that you configure the separate SENDAUTH password for the user so that ACS inbound passwords are never compromised.

If you want to use outbound passwords and maintain the highest level of security, we recommend that you configure users in the ACS internal user database with an outbound password that is different from the inbound password.

Password Aging

With ACS you can choose whether and how to employ password aging. Control for password aging may reside in the ACS internal database, or in an external Windows user database. Each password-aging mechanism differs as to requirements and setting configurations.

You use the password aging feature the ACS internal database controls to force users to change their passwords under any of the following conditions:

- Date exceeds: value (a date).
- After a specified number of logins.
- The first time a new user logs in.

For information on the requirements and configuration of the password aging feature that the ACS internal database controls, see [Enabling Password Aging for the ACS Internal Database, page 5-15](#).

You use the Windows-based password aging feature to control the following password aging parameters:

- Maximum password age in days.
- Minimum password age in days.

The methods and functionality of Windows password aging differ according to the Windows operating system release. For information on the requirements and configuration of the Windows-based password aging feature, see [Enabling Password Aging for Users in Windows Databases, page 5-19](#), and refer to your Windows system documentation.

User-Changeable Passwords

With ACS, you can install a separate program so that users can change their passwords by using a web-based utility. For more information about installing user-changeable passwords, see the *Installation and User Guide for Cisco Secure ACS User-Changeable Passwords* on <http://www.cisco.com>.

Other Authentication-Related Features

In addition to the authentication-related features discussed in this section, ACS provides additional features:

- Authentication of unknown users with external user databases. (See [About Unknown User Authentication, page 15-3](#).)
- Authentication of computers running Microsoft Windows. (See [Machine Authentication, page 12-10](#).)
- Support for the Microsoft Windows Callback feature. (See [Setting the User Callback Option, page 6-6](#).)
- Ability to configure user accounts, including passwords, by using an external data source. (See [About RDBMS Synchronization, page 8-17](#).)
- Ability for external users to authenticate via an enable password. (See [Setting TACACS+ Enable Password Options for a User, page 6-23](#).)
- Proxy of authentication requests to other AAA servers. (See [Proxy in Distributed Systems, page 3-3](#).)
- Configurable character string stripping from proxied authentication requests. (See [Stripping, page 3-5](#).)
- Self-signed server certificates. (See [Using Self-Signed Certificates, page 9-33](#).)
- Certificate revocation list checking during EAP-TLS authentication. (See [Managing Certificate Revocation Lists, page 9-29](#).)

Authorization

Authorization determines what a user is allowed to do. ACS can send user profile policies to AAA clients to determine which network services the user can access. You can configure authorization to give different users and groups different levels of service. For example, standard dial-up users might not have the same access privileges as premium customers and users. You can also differentiate by levels of security, access times, and services.

You can use the ACS access restrictions feature to permit or deny logins based on time-of-day and day-of-week. For example, you could create a group for temporary accounts that you can disable on specified dates. A service provider could then offer a 30-day free trial. You could use the same authorization to create a temporary account for a consultant with login permission that is limited to Monday through Friday, 9 A.M. to 5 P.M.

You can also apply the following restrictions to users:

- a single service
- a combination of services, such as PPP, ARAP, Serial Line Internet Protocol (SLIP), or EXEC
- Layer 2 and Layer 3 protocols, such as IP and IPX
- access lists

On a per-user or per-group basis, access lists can restrict the following user access:

- parts of the network where critical information is stored
- certain services, such as File Transfer Protocol (FTP) or Simple Network Management Protocol (SNMP)

One fast-growing service that providers offer and corporations adopt is a service authorization for Virtual Private Dial-Up Networks (VPDNs). ACS can provide information to the network device for a specific user to configure a secure tunnel through a public network, such as the Internet. The information can be for the access server (such as the home gateway for that user) or for the home gateway router to validate the user at the customer premises. In either case, ACS can be used for each end of the VPDN.

This section contains:

- [Max Sessions, page 1-13](#)
- [Dynamic Usage Quotas, page 1-13](#)
- [Shared Profile Components, page 1-14](#)
- [Support for Cisco Device-Management Applications, page 1-14](#)
- [Other Authorization-Related Features, page 1-14](#)

Max Sessions

Max Sessions is a useful feature for organizations that need to limit the number of concurrent sessions that are available to a user or a group:

- **User Max Sessions**—For example, an Internet service provider can limit each account holder to a single session.
- **Group Max Sessions**—For example, an enterprise administrator can allow the remote access infrastructure to be shared equally among several departments and limit the maximum number of concurrent sessions for all users in any one department.

In addition to enabling simple User and Group Max Sessions control, as an administrator you can use ACS to specify a Group Max Sessions value and a group-based User Max Sessions value; that is, a User Max Sessions value based on the group membership of the user. For example, an administrator can allocate a Group Max Sessions value of 50 to the group *Sales* and also limit each member of the *Sales* group to five sessions each. Therefore, no single member of a group account would be able to use more than five sessions at any one time, but the group could still have up to 50 active sessions.

For more information about the Max Sessions feature, see [Setting Max Sessions for a User Group, page 5-9](#) and [Setting Max Sessions Options for a User, page 6-11](#).

Dynamic Usage Quotas

You can use ACS to define network usage quotas for users. Using quotas, you can limit the network access of each user in a group or of individual users. You define quotas by duration of sessions or the total number of sessions. Quotas can be absolute; or based on daily, weekly, or monthly periods. To grant access to users who have exceeded their quotas, you can reset session quota counters as needed.

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off and the accounting stop packet is received from the AAA client. If the AAA client through which the user is accessing your network fails, the session information is not updated. In the case of multiple sessions, such as with ISDN, the quota would not be updated until all sessions terminate, which means that a second channel will be accepted; even if the first channel has exhausted the quota that is allocated to the user.

For more information about usage quotas, see [Setting Usage Quotas for a User Group, page 5-10](#) and [Options for Setting User Usage Quotas, page 6-12](#).

Shared Profile Components

ACS provides a means for specifying authorization profile components that you can apply to multiple user groups and users. For example, you may have multiple user groups that have identical network-access restrictions. Rather than configuring the network-access restrictions several times, once per group, you can configure a network-access restriction set in the Shared Profile Components section of the web interface, and then configure each group to use the network-access restriction set that you created.

For information about the types of shared-profile components that ACS supports, see [About Shared Profile Components, page 4-1](#).

Support for Cisco Device-Management Applications

ACS supports Cisco device-management applications, such as 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-authorization set types for each management application that is configured to use ACS for authorization.

ACS uses TACACS+ to communicate with management applications. For a management application to communicate with ACS, you must configure the management application in ACS 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.

Additionally, the administrator that the management application uses must have the Create New Device Command Set Type privilege enabled. When a management application initially communicates with ACS, it dictates to ACS the creation of a device command set type, which appears in the Shared Profile Components section of the web interface. It also dictates a custom service for TACACS+ to authorize. The custom service appears on the TACACS+ (Cisco IOS) page in the Interface Configuration section of the web interface. For information about enabling TACACS+ services, see [Displaying TACACS+ Configuration Options, page 2-6](#). For information about device command-authorization sets for management applications, see [Command Authorization Sets, page 4-25](#).

After the management application has dictated the custom TACACS+ service and device command-authorization set type to ACS, you can configure command-authorization sets for each role that the management application supports and apply those sets to user groups that contain network administrators or to individual users who are network administrators.

Other Authorization-Related Features

In addition to the authorization-related features discussed in this section, ACS provides these additional features:

- Group administration of users. (See [Chapter 5, “User Group Management.”](#))
- Ability to map a user from an external user database to a specific ACS group. (See [Chapter 16, “User Group Mapping and Specification.”](#))
- Ability to disable an account after a number of failed attempts, specified by the administrator. (See [Setting Options for User Account Disablement, page 6-13.](#))
- Ability to disable an account on a specific date. (See [Setting Options for User Account Disablement, page 6-13.](#))
- Ability to disable groups of users. (See [Group Disablement, page 5-3.](#))
- Ability to restrict time-of-day and day-of-week access. (See [Setting Default Time-of-Day Access for a User Group, page 5-5.](#))
- Network access restrictions (NARs) based on remote address caller line identification (CLID) and dialed number identification service (DNIS.) (See [Setting Network Access Restrictions for a User Group, page 5-6.](#))
- Downloadable ACLs for users or groups, enabling centralized, modular ACL management. (See [Downloadable IP ACLs, page 4-13.](#))
- Network access filters, which apply different downloadable ACLs and NARs based on a user’s point of entry into your network. (See [Network Access Filters, page 4-2.](#))
- Ability to enable or disable users based on the Network Access Profile configuration. (See [Authorization Policy Configuration for NAPs, page 14-34.](#))
- IP pools for IP address assignment of end-user client hosts. (See [Setting IP Address Assignment Method for a User Group, page 5-21.](#))
- Per-user and per-group TACACS+ or RADIUS attributes. (See [Displaying Advanced Options, page 2-6.](#))
- Support for VoIP, including configurable logging of accounting data. (See [Enabling VoIP Support for a User Group, page 5-4.](#))

Accounting

AAA clients use the accounting functions that the RADIUS and TACACS+ protocols provide to communicate relevant data for each user session to the AAA server for recording. You can import the accounting logs into popular database and spreadsheet applications for billing, security audits, and report generation. You can also use a third-party reporting tool to manage accounting data.

ACS writes accounting records to one or more of the following, depending on your configuration:

- a comma-separated value (CSV) log file
- Syslog file
- ODBC database (ACS for Windows only)

The types of accounting logs that you can generate include:

- **TACACS+ Accounting**—Lists when sessions start and stop; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **RADIUS Accounting**—Lists when sessions stop and start; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **VoIP Accounting**—Lists VoIP session stop and start times, AAA client messages with usernames, caller line identification (CLID) information, and VoIP session duration.

For more information about ACS logging capabilities, see [Chapter 10, “Logs and Reports.”](#)

Other Accounting-Related Features

In addition to the accounting-related features in this section, ACS provides these additional features:

- Centralized logging for:
 - ACS Windows, allow several ACS installations to forward their accounting data to a remote ACS.
 - The ACS SE, which uses the remote agent for centralized logging.

For more information, see [Remote Logging for ACS for Windows, page 10-10](#).

- Configurable supplementary user ID fields for capturing additional information in logs. (See [Customizing User Data, page 2-5](#).)
- Configurable logs, allowing you to capture as much information as needed. (See [AAA-Related Logs, page 10-1](#).)

Managing and Administrating ACS

ACS provides a flexible administration scheme to configure, maintain, and protect its AAA functionality. You can perform nearly all ACS administration tasks through the ACS web interface. You use the web interface to easily modify the ACS configuration from any connection on your LAN or WAN, and view it by using a web browser. For a list of supported browsers, see the latest version of the *Release Notes for Cisco Secure ACS Release 4.2* on

http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_note09186a00805efcbc.html.

The web interface not only makes viewing and editing user and group information possible, you use it to restart services, add remote administrators, change AAA client information, back up the system, view reports from anywhere on the network, and more.

This section describes the ACS web interface and provides information about the following topics:

- [Web Interface Security, page 1-16](#)
- [Cisco Security Agent Integration \(ACS SE Only\), page 1-17](#)
- [HTTP Port Allocation for Administrative Sessions, page 1-19](#)
- [Web Interface Layout, page 1-19](#)
- [Uniform Resource Locator for the Web Interface, page 1-21](#)
- [Online Help and Online Documentation, page 1-21](#)

Web Interface Security

Accessing the web interface requires a valid administrator name and password. The ACS Login page encrypts the administrator credentials before sending them to ACS.

Administrative sessions time out after a configurable length of idle time. Regardless, we recommend that you log out of the web interface after each session. For information about configuring the idle timeout feature, see [Configuring Access Policy, page 11-8](#) and [Access Policy Setup Page, page 11-18](#).

You can enable a secure socket layer (SSL) for administrative sessions. This method ensures that all communication between the web browser and ACS is encrypted. Your browser must support SSL. You can enable this feature on the Access Policy Setup page in the Administration Control section. For more information about enabling the SSL for web interface security, see [Configuring Access Policy, page 11-8](#) and [Access Policy Setup Page, page 11-18](#).

Cisco Security Agent Integration (ACS SE Only)

CSA protects the ACS SE. Whether you have applied a CSA update to ACS or you are using an appliance base image that incorporates the CSA, the CSA helps to protect ACS from viruses, worms, and attacks. On the ACS SE, the CSA operates in standalone mode, which Cisco has configured to permit ACS to operate normally while providing protection.



Note

The first appliance base image version that incorporates the CSA is 3.3.1.3. You can determine the base image version of an appliance by using the **show** console command or the Appliance Upgrade Status page in the System Configuration section of the web interface.

This section contains:

- [Cisco Security Agent Service Management, page 1-17](#)
- [Cisco Security Agent Logging, page 1-17](#)
- [Cisco Security Agent Restrictions, page 1-18](#)
- [Cisco Security Agent Policies, page 1-18](#)

Cisco Security Agent Service Management

The CSA runs on the appliance as an additional service, named **CSAgent**.

From the appliance console, you can use the **start**, **stop**, and **restart** commands to manage **CSAgent**. For more information about these commands, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

From the HTML interface, you can use the Appliance Configuration page in the System Configuration section of the web interface to enable or disable **CSAgent**. For more information, see [Appliance Configuration \(ACS SE Only\), page 7-22](#).

Cisco Security Agent Logging

The CSA writes two logs to the appliance hard drive, *CSALog* and *CSASecurityLog*. The size of each log is limited to 1 MB. When a CSA log exceeds 1 MB, the CSA begins a new log file. ACS retains the three most recent files for each CSA log.

From the appliance console, you can use the **exportlogs** command to retrieve the CSA logs. For more information about the **exportlogs** command or using the console, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

From the web interface, you can view the CSA logs by clicking the links on the View Diagnostic Logs page in the System Configuration section.

Cisco Security Agent Restrictions

The protection that the CSA provides to the appliance imposes the following restrictions when **CSAgent** is enabled:

- **Upgrade and Patch Restriction**—You cannot apply upgrades or patches by using the Appliance Upgrade Status page in the System Configuration section or the **upgrade** command at the appliance console. To upgrade ACS or apply patches, you must first disable **CSAgent**.
- **ping Restriction**—The CSA does not allow the ACS SE to respond to **ping** requests that it receives from other computers. The CSA does not affect the use of the **ping** command at the appliance console. If you disable **CSAgent** to permit the ACS SE to respond to **ping** requests, no CSA protection is in place for as long as **CSAgent** is disabled.

For information about disabling CSAgent, see [Cisco Security Agent Service Management, page 1-17](#).

Cisco Security Agent Policies

The CSA is configured with the following policies:

- **Application Control**—The CSA permits execution of only those applications required for ACS to operate correctly. Because of this protection, you must disable the CSA before applying an upgrade or patch.
- **File Access Control**—The CSA permits file system access for only those applications required for ACS to correctly operate.
- **IP and Transport Control**—The CSA provides the following protections:
 - Discards invalid IP headers.
 - Discards invalid transport headers.
 - Detects TCP/UDP port scans.
 - Cloaks the appliance to prevent port scans.
 - Prevents TCP blind session spoofing.
 - Prevents TCP SYN floods.
 - Blocks ICMP covert channels.
 - Blocks dangerous ICMP messages, including **ping**.
 - Prevents IP source routing.
 - Prevents trace routing.
- **E-mail Worm Protection**—The CSA guards the appliance against e-mail worms.
- **Registry Access Control**—The CSA permits registry access to only those applications requiring access for proper operation of the appliance.
- **Kernel Protection**—The CSA does not allow kernel modules to be loaded after system startup is complete.
- **Trojan and Malicious Application Protection**—The CSA provides the following protections. Applications cannot:
 - Write code to space owned by other applications.
 - Download and execute ActiveX controls.
 - Automatically execute downloaded programs.

- Directly access operating system password information.
- Write into memory owned by other processes.
- Monitor keystrokes while accessing the network.

HTTP Port Allocation for Administrative Sessions

You use the HTTP port allocation feature to configure the range of TCP ports that ACS uses for administrative HTTP sessions. Narrowing this range with the HTTP port allocation feature reduces the risk of unauthorized access to your network through a port that is open for administrative sessions.

We do not recommend that you administer ACS through a firewall. Doing so requires that you configure the firewall to permit HTTP traffic over the range of HTTP administrative session ports that ACS uses. While narrowing this range reduces the risk of unauthorized access, a greater risk of attack remains if you allow administration of ACS from outside a firewall. A firewall that is configured to permit HTTP traffic over the ACS administrative port range must also permit HTTP traffic through port 2002, because a web browser must address this port to initiate an administrative session.



Note

A broad HTTP port range could create a security risk. To prevent accidental discovery of an active administrative port by unauthorized users, keep the HTTP port range as narrow as possible. ACS tracks the IP address that is associated with each administrative session. An unauthorized user would have to impersonate, or “spoof,” the IP address of the legitimate remote host to make use of the active administrative session HTTP port.

For information about configuring the HTTP port allocation feature, see [Configuring Access Policy, page 11-8](#) and [Access Policy Setup Page, page 11-18](#).

Web Interface Layout

The web interface has three vertical partitions, known as frames:

- **Navigation Bar**—The gray frame on the left side of the browser window, the navigation bar contains the task buttons. Each button changes the configuration area to a unique section of the ACS application, such as the User Setup section or the Interface Configuration section. This frame does not change; it always contains the following buttons:
 - **User Setup**—Add and edit user profiles. For more information about the User Setup section, see [Chapter 6, “User Management.”](#)
 - **Group Setup**—Configure network services and protocols for groups of users. For more information about the Group Setup section, see [Chapter 5, “User Group Management.”](#)
 - **Shared Profile Components**—Add and edit network-access restriction and command-authorization sets, to be applied to users and groups. For more information about the Shared Profile Components section, see [Chapter 4, “Shared Profile Components.”](#)
 - **Network Configuration**—Add and edit network-access devices and configure distributed systems. For more information about the Network Configuration section, see [Chapter 3, “Network Configuration.”](#)
 - **System Configuration**—Configure system-level features. Four chapters address this large section of the web interface. For information about fundamental features such as backup scheduling and service controls, see [Chapter 7, “System Configuration: Basic.”](#) For information about advanced features such as database replication, see [Chapter 8, “System Configuration:](#)

[Advanced.](#) For information about configuring authentication protocols and certificate-related features, see [Chapter 9, “System Configuration: Authentication and Certificates.”](#) For information about configuring logs and reports, see [Chapter 10, “Logs and Reports.”](#)

- **Interface Configuration**—Display or hide product features and options to configure. For more information about the Interface Configuration section, [Chapter 2, “Using the Web Interface.”](#)
- **Administration Control**—Define and configure access policies. For more information about the Administration Control section, [Chapter 11, “Administrators and Administrative Policy.”](#)
- **External User Databases**—Configure databases, the Unknown User Policy, and user group mapping. For information about configuring databases, see [Chapter 12, “User Databases.”](#) For information about the Unknown User Policy, see [Chapter 15, “Unknown User Policy.”](#) For information about user group mapping, see [Chapter 16, “User Group Mapping and Specification.”](#)
- **Posture Validation**—Control the degree of access that is permitted from computers that access your network through AAA clients that are configured to enforce NAC. For more information on posture validation, see [Chapter 13, “Posture Validation.”](#)
- **Network Access Profiles**—Set up the conditions that allow a user to connect to the network and identify the way requests to access the network are applied. For more information on setting up Network Access Profiles and Profile-based Policies, see [Chapter 14, “Network Access Profiles.”](#)
- **Reports and Activity**—Display accounting and logging information. For information about viewing reports, see [Chapter 10, “Logs and Reports.”](#)
- **Online Documentation**—View the user guide. For information about using the online documentation, see [Online Help and Online Documentation, page 1-21.](#)
- **Configuration Area**—The frame in the middle of the browser window, the configuration area displays web pages that belong to one of the sections represented by the buttons in the navigation bar. The configuration area is where you add, edit, or delete information. For example, you configure user information in this frame on the User Setup Edit page.



Note Most pages have a Submit button at the bottom. Click **Submit** to confirm your changes. If you do not click Submit, the changes are not saved.

- **Display Area**—The pane on the right side of the browser window, the display area shows one of the following options:
 - **Online Help**—Displays basic help about the page that currently appears in the configuration area. This help does not offer in-depth information, rather it gives some basic information about what can be accomplished in the middle frame. For more information about online help, see [Using Online Help, page 1-21.](#)
 - **Reports or Lists**—Displays lists or reports, including accounting reports. For example, in User Setup you can show all usernames that start with a specific letter. The list of usernames beginning with a specified letter appears in this section. The usernames are hyperlinks to the specific user configuration, so you click the name to edit that user.
 - **System Messages**—Displays messages after you click Submit if you have typed in incorrect or incomplete data. For example, if the information that you entered in the Password box does not match the information in the Confirm Password box in the User Setup section, ACS displays an error message here. The incorrect information remains in the configuration area so that you can retype the information correctly and resubmit it.

Uniform Resource Locator for the Web Interface

You can access the ACS web interface by using one of the following uniform resource locators (URLs):

- `http://IP address:2002`
- `http://hostname:2002`

where *IP address* is the dotted decimal IP address and *hostname* is the hostname of the server that is running ACS. If you use the hostname, DNS must be functioning properly on your network or the hostname must be listed in the local hosts file of the computer that is running the browser.

If ACS is configured to use SSL to protect administrative sessions, you must specify the HTTPS protocol in the URLs:

- `https://IP address:2002`
- `https://hostname:2002`

If SSL is enabled and you do not specify HTTPS, ACS redirects the initial request to HTTPS for you. Using SSL to access the login page protects administrator credentials. For more information about enabling SSL to protect administrative sessions, see [Configuring Access Policy, page 11-8](#) and [Access Policy Setup Page, page 11-18](#).

From the computer that is running ACS, you can also use the following URLs:

- `http://127.0.0.1:2002`
- `http://localhost:2002`

If SSL is enabled, you can specify the HTTP protocol in the URLs:

- `https://127.0.0.1:2002`
- `https://localhost:2002`

Online Help and Online Documentation

We provide two sources of information in the web interface:

- **Online Help**—Contains basic information about the page shown in the configuration area.
- **Online Documentation**—Contains the entire user guide.

Using Online Help

Each page in the Web interface includes a corresponding online help page. Each online help page contains a list of topics that correspond to the current web page.

The two help icons that appear on pages in ACS are:

- **Question Mark**—Many subsections of the pages in the configuration area contain an icon with a question mark (?). To jump to the applicable topic in an online help page, click the question mark (?) icon.
- **Back to Help**—Wherever you find a online help page with a Section Information icon, the corresponding page in the configuration area contains a Back to Help icon. If you have accessed the online documentation by clicking a Section Information icon and want to view the online help page again, click the Back to Help icon.

Using the Online User Guide

The user guide provides information about the configuration, operation, and concepts of ACS. The information in the online documentation version of the user guide is as current as the release date of the ACS version that you are using. For the latest documentation about ACS, click <http://www.cisco.com>.

To access online documentation:

-
- Step 1** In the ACS web interface, click **Online Documentation**. For information on using the online documentation, see [Online Documentation Reference, page 1-23](#).
-

ACS Specifications



Note

For the hardware, operating system, third-party software, and network requirements, see the *Installation Guide for Cisco Secure ACS for Windows Release 4.2* or *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

This section contains:

- [System Performance Specifications, page 1-22](#)
- [ACS Windows Services, page 1-23](#)

System Performance Specifications

The performance capabilities of ACS are depend mostly on the Windows server it is installed on, your network topology and network management, the selection of user databases, and other factors. For example, ACS can perform many more authentications per second if it is using its internal user database and running on a computer that is using the fastest processor and network interface card available than if it is using external user databases and running on a computer that complies with the minimum system requirements. (See the *Installation Guide for Cisco Secure ACS for Windows Release 4.2* or *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.)

The following items are general answers to common system-performance questions. The performance of ACS in your network depends on your specific environment and AAA requirements.

- **Maximum users supported by the ACS internal database**—There is no theoretical limit to the number of users the ACS internal database can support. We have successfully tested ACS with databases in excess of 100,000 users. The practical limit for a single ACS authenticating against all its databases, internal and external, is 300,000 to 500,000 users. This number increases significantly if the authentication load is spread across a number of replicated ACS instances.
- **Transactions per second**—Authentication and authorization transactions per second depend on many factors, most of which are external to ACS. For example, high network latency in communication with an external user database lowers the number of transactions per second that ACS can achieve.
- **Maximum number of AAA clients supported**—ACS has been tested to support AAA services for approximately 50,000 AAA client configurations. This limitation is primarily a limitation of the ACS memory.

If your network comprises tens of thousands of AAA clients, we recommend using multiple ACSs and assigning a manageable number of AAA clients to each ACS. For example, if you have 80,000 AAA clients, you could use four ACS servers and divide the AAA client load among them so that no single ACS manages more than 40,000 AAA client configurations. Then you can have overlapping AAA client support for backup AAA servers and not exceed the 50,000 AAA client limit. If you use replication to propagate configuration data among ACSs, limit replication of AAA client data to ACSs that serve the same set of AAA clients.

ACS Windows Services

ACS operates as a set of Microsoft Windows services. When you install ACS, the installation adds these Windows services to the server. These services provide the core of ACS functionality.

The ACS services on the computer running ACS include:

- **CSAdmin**—Provides the web interface for administration of ACS.
- **CSAuth**—Provides authentication services.
- **CSDBSync**—Provides synchronization of the ACS internal database with an external RDBMS application.
- **CSLog**—Provides logging services, for accounting and system activity.
- **CSMon**—Provides monitoring, recording, and notification of ACS performance, and behavior.
- **CSTacacs**—Provides communication between TACACS+ AAA clients and the CSAuth service.
- **CSRADIUS**—Provides communication between RADIUS AAA clients and the CSAuth service.

For a full description of each service, see [Appendix F, “Internal Architecture.”](#)

You can start and stop each module individually from within the serial console and Microsoft Windows Service Control Panel or as a group from within the serial console or the ACS web interface. For information about stopping and starting ACS services by using the serial console, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*. For information about stopping and starting ACS services by using the web interface, see [Service Control, page 7-1](#). For information on service logs and gathering data for troubleshooting, see [Service Logs, page 10-12](#).

Network administrators who offer increased levels of security services and corporations that want to lessen the chance of intruder access resulting from password capturing can use an OTP. ACS supports several types of OTP solutions, including PAP for Point-to-Point Protocol (PPP) remote-node login. Token cards are considered one of the strongest OTP authentication mechanisms.

Online Documentation Reference

[Table 1-6](#) describes the options in the online documentation interface.

Table 1-6 *Online Documentation*

Option	Description
Home	Opens the top Online Documentation page (the first page of Chapter 1 in the user guide).
Search	Opens the Search page. Type the search string. Choose Any Words to return a list of topics that contain any word in the search string. Choose All Words to return a list of topics that contain all words in the search string. Click Using Search for information on searching.

Table 1-6 Online Documentation (continued)

Option	Description
Using Help	Opens the Using Help page, which contains tips on using the ACS online documentation.
Glossary	Opens the Cisco online glossary of internetworking terms and acronyms.
View PDF	Opens the user guide in PDF format.
Contents	Contains the complete list of topics from the user guide. Click the appropriate topic to display the corresponding Online Documentation page.
Index	Contains the complete index from the user guide. Click the letters to jump to particular sections of the index. Click the appropriate index entry to display the corresponding Online Documentation page.

Related Documentation



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.

The following sections list various categories of documents on ACS and related topics.

TACACS+ Documents

For a general description of the Cisco TACACS+ protocol, see:

http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

Network Admission Control (NAC) documentation

For general information about NAC and links to additional web pages about NAC, see:

<http://www.cisco.com/go/NAC>

For information on technical documentation for NAC, see:

http://www.cisco.com/en/US/netsol/ns617/networking_solutions_documentation_roadmap09186a008066499c.html

Requests for Comments (RFCs)

The following RFCs describe several of the security protocols used by ACS:

- RFC 2865: *Remote Authentication Dial In User Service (RADIUS)*
<http://www.rfc-archive.org/getrfc.php?rfc=2865>
- RFC 3748: *PPP Extensible Authentication Protocol (EAP)*
<http://www.rfc-archive.org/getrfc.php?rfc=3748>
- RFC 4346: *The Transport Layer Security (TLS) Protocol Version 1.1*
<http://www.rfc-archive.org/getrfc.php?rfc=4346>

- RFC PPP EAP TLS Authentication Protocol
<http://www.rfc-archive.org/getrfc.php?rfc=2716>

Technology White Papers

Cisco.com and Cisco Connection Online (CCO) contain a number of White Papers that present basic network security concepts and information about planning and configuring ACS installations:

A list of white papers specifically related to ACS available at:

http://www.cisco.com/en/US/partner/products/sw/secursw/ps2086/prod_white_papers_list.html

Additional white papers on related topics are available:

- *Network Security Policy: Best Practices White Paper* at:
http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a008014f945.shtml
- *Delivering End-to-End Security in Policy-Based Networks*
http://www.cisco.com/warp/public/cc/pd/nemnsw/cap/tech/deesp_wp.htm
- *Cisco IOS Security Configuration Guide*
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/secur_c/scdoverv.htm
- *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks*
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a008009256b.shtml

Question and Answer Pages

For answers to common questions about Cisco EAP-FAST, see the Cisco EAP-FAST Q&A page:

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

Tutorials

The ACS Primer is a training course on ACS 4.0:

http://www.cisco.com/application/pdf/en/us/guest/products/ps2086/c1161/cdccont_0900aecd8040daa7.pdf

Software Download

To download Cisco software that is mentioned in this manual, such as Cisco Authentication Agent, go to the Cisco Software Center at:

<http://www.cisco.com/public/sw-center/>



CHAPTER 2

Using the Web Interface

Ease of use is the overriding design principle of the web interface in the Cisco Secure Access Control Server Release 4.2, henceforth referred to as ACS. ACS presents intricate concepts of network security from the perspective of an administrator. You can use the Interface Configuration section of ACS to configure the ACS web interface. You can tailor the interface to simplify screens by hiding the features that you do not use and adding fields for your specific configuration.



Note

We recommend that you return to this section to review and confirm your initial settings. While it is logical to begin your ACS configuration efforts with configuring the interface, sometimes a section of the web interface that you initially believed should be hidden from view may later require configuration from within this section.



Tip

If a section of the ACS web interface appears to be missing or broken, return to the Interface Configuration section and confirm that the particular section has been activated.

This chapter contains:

- [Administrative Sessions, page 2-1](#)
- [Configuring User Access, page 2-4](#)
- [Customizing User Data, page 2-5](#)
- [Displaying Advanced Options, page 2-6](#)
- [Displaying TACACS+ Configuration Options, page 2-6](#)
- [Displaying RADIUS Configuration Options, page 2-7](#)
- [Interface Configuration Reference, page 2-10](#)

Administrative Sessions

We recommend that administrative sessions take place without the use of an HTTP proxy server, without a firewall between the browser and ACS, and without a NAT gateway between the browser and ACS. Because these limitations are not always practical, this section discusses how various network environmental issues affect administrative sessions.

This section contains:

- [Administrative Sessions and HTTP Proxy, page 2-2](#)

- [Administrative Sessions Through Firewalls, page 2-2](#)
- [Administrative Sessions Through a NAT Gateway, page 2-2](#)
- [Accessing the Web Interface, page 2-3](#)
- [Logging Off the Web Interface, page 2-4](#)

Administrative Sessions and HTTP Proxy

ACS does not support HTTP proxy for administrative sessions. If the browser used for an administrative session is configured to use a proxy server, ACS sees the administrative session originating from the IP address of the proxy server rather than from the actual address of the computer. Administrative session tracking assumes each browser resides on a computer with a unique IP.

Also, IP filtering of proxied administrative sessions has to be based on the IP address of the proxy server rather than the IP address of the computer. This conflicts with administrative session communication that does use the actual IP address of the computer. For more information about IP filtering of administrative sessions, see [Configuring Access Policy, page 11-8](#) and [Access Policy Setup Page, page 11-18](#).

For these reasons, we do not recommend performing administrative sessions using a web browser that is configured to use a proxy server. Administrative sessions using a proxy-enabled web browser is not tested. If your web browser is configured to use a proxy server, disable HTTP proxying when attempting ACS administrative sessions.

Administrative Sessions Through Firewalls

In the case of firewalls that do not perform network address translation (NAT), administrative sessions conducted across the firewall can require additional configuration of ACS and the firewall. This is because ACS assigns a random HTTP port at the beginning of an administrative session.

To allow administrative sessions from browsers outside a firewall that protects ACS, the firewall must permit HTTP traffic across the range of ports that ACS is configured to use. You can control the HTTP port range using the HTTP port allocation feature. For more information about the HTTP port allocation feature, see [HTTP Port Allocation for Administrative Sessions, page 1-19](#).

While administering ACS through a firewall that is not performing NAT is possible, we do not recommend that you administer ACS through a firewall. For more information, see [HTTP Port Allocation for Administrative Sessions, page 1-19](#).

Administrative Sessions Through a NAT Gateway

We do not recommend conducting administrative sessions across a network device performing NAT. If the administrator runs a browser on a computer behind a NAT gateway, ACS receives the HTTP requests from the public IP address of the NAT device, which conflicts with the computer private IP address, included in the content of the HTTP requests. ACS does not permit this.

If ACS is behind a NAT gateway and the URL used to access the web interface specifies ACS by its hostname, administrative sessions operate correctly, provided that DNS is functioning correctly on your network or that computers used to access the web interface have a hosts file entry for ACS.

If the URL used to access the web interface specifies ACS by its IP address, you could configure the gateway to forward all connections to port 2002 to ACS, using the same port. Additionally, all the ports allowed using the HTTP port allocation feature would have to be similarly mapped. We have not tested such a configuration and do not recommend implementing it.

Accessing the Web Interface

Remote administrative sessions always require that you log in using a valid administrator name and password, as configured in the Administration Control section. If the Allow automatic local login check box is cleared on the Sessions Policy Setup page in the Administration Control section, ACS requires a valid administrator name and password for administrative sessions accessed from a browser on the computer running ACS.

Before You Begin

Determine whether a supported web browser is installed on the computer you want to use to access the web interface. If not, install a supported web browser or use a computer that already has a supported web browser installed. For a list of supported browsers, see the *Release Notes for Cisco Secure ACS Release 4.2*. The latest revision to the Release Notes is posted on

http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_note09186a00805efcbc.html.

Because the web interface uses Java in a few places, the computer running the browser used to access the web interface must have a Java Virtual Machine available for the use of the browser.

To access the web interface:

-
- Step 1** Open a web browser. For a list of supported web browsers, see the Release Notes for the version of ACS you are accessing. The most recent revision to the Release Notes is posted on http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_release_note09186a00805efcbc.html.
- Step 2** In the Address or Location bar in the web browser, type the applicable URL. You can access the ACS web interface by using one of the following uniform resource locators (URLs):
- `http://IP address:2002`
 - `http://hostname:2002`



Note *IP address* is the dotted decimal IP address and *hostname* is the hostname of the server that is running ACS. If you use the hostname, DNS must be functioning properly on your network or the hostname must be listed in the local hosts file of the computer that is running the browser.

If ACS is configured to use SSL to protect administrative sessions, you must specify the HTTPS protocol in the URLs:

- `https://IP address:2002`
- `https://hostname:2002`



Note If SSL is enabled and you do not specify HTTPS, ACS redirects the initial request to HTTPS for you. Using SSL to access the login page protects administrator credentials. For more information about enabling SSL to protect administrative sessions, see [Configuring Access Policy, page 11-8](#) and [Access Policy Setup Page, page 11-18](#).

From the computer that is running ACS, you can also use the following URLs:

- `http://127.0.0.1:2002`
- `http://localhost:2002`

If SSL is enabled, you can specify the HTTPS protocol in the URLs:

- `https://127.0.0.1:2002`
- `https://localhost:2002`

Step 3 If the ACS login page appears:

- a. In the Username box, type a valid ACS administrator name.
- b. In the Password box, type the password for the administrator name you specified.
- c. Click **Login**.

The initial page appears, listing build and copyright information.

Logging Off the Web Interface

When you are finished using the web interface, we recommend that you log off. While ACS can timeout unused administrative sessions, logging off prevents unauthorized access by someone using the browser after you or by unauthorized persons using the HTTP port left open to support the administrative session.

To log off the ACS web interface, click the Logoff button (**X**) in the upper-right corner of the screen.



Note

The Logoff button (**X**) appears in the upper-right corner of the browser window, except on the initial page, where it appears in the upper-left corner of the configuration area.

Configuring User Access

Configuration of user access is a critical configuration activity.

This section introduces configuration for user access and contains:

[User-to-Group Relationship, page 2-4](#)

[Network Access Profiles \(NAPs\), page 2-5](#)

[Per-User or Per-Group Features, page 2-5](#)

User-to-Group Relationship

You can configure a user to belong to one group at a time. Then, as long as there are no conflicting attributes, the user inherits the group settings.



Note

If a user profile has an attribute configured differently from the same attribute in the group profile, the user setting always overrides the group setting.

If a user has a unique configuration requirement, you can make that user a part of a group and set unique requirements on the User Setup page; or you can assign that user to his or her own group. For complete information, see [Chapter 5, “User Group Management”](#) and [Chapter 6, “User Management.”](#)

Network Access Profiles (NAPs)

You no longer need to rely on user and group settings alone. With NAPs you can set up authorization rules that allow you to set user groups, RACs, and DACLs as part of a profile. For complete information, see [Chapter 14, “Network Access Profiles.”](#) For more details on authorization rules, see [Authorization Policy Configuration for NAPs, page 14-34.](#)

Per-User or Per-Group Features

You can configure most features at both the group and user levels, with the following exceptions:

- **User level only**—Static IP address, password, and expiration.
- **Group level only**—Password aging and time-of-day/day-of-week restrictions.

Customizing User Data

The Configure User Defined Fields page enables you to add (or edit) up to five fields for recording information on each user. The fields you define in this section subsequently appear in the Supplementary User Information section at the top of the User Setup page. For example, you could add the user's company name, telephone number, department, billing code, and so on. You can also include these fields in the accounting logs. For more information about the accounting logs, see [About ACS Logs and Reports, page 10-1](#). For information on the data fields that compose the user data options, see [User-Defined Attributes, page E-25](#).

To configure or edit user data fields:

-
- Step 1** Click **Interface Configuration**, and then click **User Data Configuration**.
- Step 2** The [Configure User Defined Fields, page 2-10](#) page appears. Use this page to enable and define or edit the fields that will appear in the Supplementary User Information section at the top of the User Setup page.
- Step 3** Click **Submit** or **Cancel**.



Tip

You can edit the title of a field by changing the text in the **Field Title** box and then clicking **Submit**.

Displaying Advanced Options

You use the Advanced Options page to determine which advanced options ACS displays. You can simplify the pages that appear in other areas of the ACS web interface by hiding advanced options that you do not use.

To set advanced options for the ACS web interface:

- Step 1 Click **Interface Configuration**, and then click **Advanced Options** to open the Advanced Options page.
- Step 2 Click each option that you want enabled in the ACS web interface. See [Advanced Options \(for Interface Configuration\)](#).



Caution

Disabling an advanced option in the Interface Configuration section does not affect anything except the display of that option in the web interface. Settings made while an advanced option was visible remain in effect when that advanced option is no longer visible. Furthermore, the interface displays any advanced option that has nondefault settings, even if you have configured that advanced option to be hidden. If you later disable the option or delete its settings, ACS hides the advanced option. The only exception is the Network Device Groups option. Regardless of whether Network Device Groups are in use, they are hidden when you clear the appropriate check box on the Advanced Options page.

- Step 3 Click **Submit**.

ACS alters the contents of various sections of the web interface according to your selections.

Displaying TACACS+ Configuration Options

The TACACS+ (Cisco) page details the configuration of the ACS web interface for TACACS+ settings. You use the interface settings to display or hide TACACS+ administrative and accounting options. You can simplify the web interface by hiding the features that you do not use.



Note

The TACACS+ or RADIUS security protocols appear as links on the Interface Configuration page when you have configured one or more AAA client(s) that support a particular protocol. For example, RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) appears when you have configured a AAA client in the Network Configuration sections that includes RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) in the client's Authenticate Using list.



Note

The ACS web interface displays any protocol option that is enabled or has nondefault values, even if you have configured that protocol option to be hidden. If you later disable the option or delete its value and the protocol option is configured to be hidden, ACS hides the protocol option. This behavior prevents ACS from hiding active settings.

You use this procedure to display or hide TACACS+ administrative and accounting options. It is unlikely that you will use every service and protocol available for TACACS+. Displaying each would make setting up a user or group cumbersome. To simplify setup, you can use the TACACS+ (Cisco IOS) Edit page to customize the services and protocols that appear.

To configure the user interface for TACACS+ options:

- Step 1** Click **Interface Configuration**, and then click **TACACS+ (Cisco IOS)** to display the TACACS+ (Cisco) page.
- Step 2** Use the [TACACS+ Services](#) area to define each TACACS+ service that you want to be visible on the applicable setup page.
- Step 3** Use the Advanced Configuration Options area to enable display of the advanced option. See [Advanced Configuration Options \(for TACACS+\)](#).
- Step 4** Click **Submit**.

The selections made in this procedure determine what TACACS+ options ACS displays in other sections of the web interface.

Displaying RADIUS Configuration Options

It is unlikely that you want to install every attribute available for every protocol. Displaying each would make setting up a user or group cumbersome. To simplify setup, use the options in this section to customize the attributes that are visible. For a list of supported RADIUS AV pairs and accounting AV pairs, see [Appendix B, “RADIUS Attributes.”](#)

Depending on which AAA client or clients you have configured, the Interface Configuration page displays different choices of RADIUS protocol configuration settings. The Interface Configuration page displays RADIUS Internet Engineering Task Force (IETF) settings whenever any RADIUS AAA client is configured. The Interface Configuration page also displays additional settings for each vendor-specific RADIUS type. The settings that appear for various types of AAA client depend on what settings that type of device can employ. These combinations are detailed in [Table 2-1](#).

Table 2-1 *RADIUS Listings in Interface*

Configure this Type of AAA Client	The Interface Configuration Page Lists the Types of Settings Shown											
	RADIUS IETF	RADIUS Cisco Airespace	RADIUS Cisco Aironet	RADIUS BBSM	RADIUS Cisco IOS/PIX 6.0	RADIUS Microsoft	RADIUS Ascend	RADIUS Cisco VPN 3000/ASA/PIX 7.x+	RADIUS Cisco VPN 5000	RADIUS Juniper	RADIUS Nortel	RADIUS 3COMUSR
RADIUS IETF/ RADIUS iPass	Yes	No	No	No	No	No	No	No	No	No	No	No
RADIUS Cisco Airespace)	Yes	Yes	No	No	No	No	No	No	No	No	No	No

Table 2-1 RADIUS Listings in Interface (continued)

Configure this Type of AAA Client	The Interface Configuration Page Lists the Types of Settings Shown											
RADIUS Cisco Aironet	Yes	No	Yes	No	Yes	No	No	No	No	No	No	No
RADIUS BBSM	Yes	No	No	Yes	No	No	No	No	No	No	No	No
RADIUS Cisco IOS/PIX 6.0	Yes	No	No	No	Yes	Yes	Yes	No	No	No	No	No
RADIUS Ascend	Yes	No	No	No	No	Yes	Yes	No	No	No	No	No
RADIUS (Cisco VPN3000/ASA/PIX 7.x+	Yes	No	No	No	Yes	Yes	No	Yes	No	No	No	No
RADIUS Cisco VPN 5000	Yes	No	No	No	No	No	No	No	Yes	No	No	No
RADIUS Juniper	Yes	No	No	No	No	No	No	No	No	Yes	No	No
RADIUS Nortel	Yes	No	No	No	No	No	No	No	No	No	Yes	No
RADIUS 3COMUSR												Yes

**Tip**

You must configure your network devices before you can select, on the Interface Configuration page, a type of setting for further configuration.

From the Interface Configuration page, when you select a type of RADIUS setting to configure, the web interface displays the corresponding list of available RADIUS attributes and associated check boxes. If you have selected the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options, a User check box appears alongside the Group check box for each attribute. Otherwise, only the Group check box for each attribute appears. By checking check boxes in a list of attributes, you determine whether the corresponding (IETF) RADIUS attribute or vendor-specific attribute (VSA) is configurable from the User Setup and Group Setup sections.

While ACS ships with these prepackaged VSAs, you can also define and configure custom attributes for any VSA set that is not already contained in ACS. If you have configured a custom VSA and a corresponding AAA client, from the Interface Configuration section you can select the custom VSA and then set the options for how particular attributes appear as configurable options on the User Setup or Group Setup page. For information about creating user-defined RADIUS VSAs, see [Creating, Reading, Updating and Deleting Actions for AAA clients](#), page 8-22.

Specifying Display of RADIUS (IETF) Options

This procedure enables you to hide or display any of the standard IETF RADIUS attributes for configuration from other portions of the ACS web interface.



Note If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is selected, a User check box appears alongside the Group check box for each attribute.

To set protocol configuration options for IETF RADIUS attributes:

- Step 1** Click **Interface Configuration**, and then click **RADIUS (IETF)** to display the RADIUS (IETF) page.
- Step 2** For each IETF RADIUS attribute that you want to appear as a configurable option on the User Setup or Group Setup page, check the corresponding check box. See [RADIUS Protocols](#).



Note Your RADIUS network devices must support each checked RADIUS attribute.

- Step 3** To specify how many values to display for tagged attributes on the User Setup and Group Setup pages, select the **Tags to Display Per Attribute** option, and then select a value from the corresponding list. Examples of tagged attributes are [064] Tunnel-Type and [069] Tunnel-Password.
- Step 4** Click **Submit**.

Each IETF RADIUS attribute that you checked appears as a configurable option on the User Setup or Group Setup page, as applicable.

Specifying Display of RADIUS (<vendor>) Options

You use this procedure to hide or display various RADIUS VSAs for configuration from the User Setup and Group Setup portions of the ACS web interface.

To set protocol configuration options for a set of RADIUS VSAs:

- Step 1** Click **Interface Configuration**.
- Step 2** Click one of the RADIUS VSA set types, for example, RADIUS (Ascend).
- Step 3** The page listing the selected set of available RADIUS VSAs appears. See [RADIUS Protocols](#).



Note If the Per-user TACACS+/RADIUS Attributes check box in Interface Configuration: Advanced Options is checked, a User check box appears beside the Group check box for each attribute.

- Step 4** For each RADIUS VSA that you want to appear as a configurable option on the User Setup or Group Setup page, check the corresponding check box.



Note Your RADIUS network devices must support each checked RADIUS attribute.

- Step 5** Click **Submit** at the bottom of the page.

According to your selections, the RADIUS VSAs appear on the User Setup or Group Setup pages, or both, as a configurable option.

Interface Configuration Reference

Click the Interface Configuration button in the navigation bar to open the top page of the Interface Configuration section of the Web interface.

[Table 2-2](#) describes the options on the Interface Configuration page.

Table 2-2 *Interface Configuration Page*

Option	Description
Select	
User Data Configuration	Opens the Configure User Defined Fields page, which you can use to configure additional fields that will appear on the User Setup page.
<protocol>	Opens a page that contains the associated TACACS+ or RADIUS service and attribute options. Note The TACACS+ or RADIUS security protocols appear as links on the Interface Configuration page when you have configured one or more AAA client(s) that support a particular protocol. For example, RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) appears when you have configured a AAA client in the Network Configuration sections that includes RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) in the client's Authenticate Using list.
Advanced Options	Opens the Advanced Options page, which you can use to choose additional options that will appear in the user interface.

The Interface Configuration Reference includes:

- [Configure User Defined Fields](#)
- [TACACS+ Services](#)
- [Advanced Configuration Options \(for TACACS+\)](#)
- [RADIUS Protocols](#)
- [Advanced Options \(for Interface Configuration\)](#)

Configure User Defined Fields

[Table 2-3](#) describes the options on the Configure User Defined Fields page.

Table 2-3 *Configure User Defined Fields*

Option	Description
Display	When checked, enables display of the field on the User Setup page and certain System Configuration: Logging pages.
Field ID	Lists the ID number for each field.

Table 2-3 *Configure User Defined Fields (continued)*

Option	Description
Field Name	Type a new field name or edit an existing field name. The range is 1 to 126 characters, any alpha-numeric characters are allowed. Note Be sure to check the Display field.
Submit	Submits the changes and then returns to the Interface Configuration page.
Cancel	Clears new changes and then returns to the Interface Configuration page.

TACACS+ Services

Table 2-4 describes the TACACS+ Services area.

Table 2-4 *TACACS+ Services*

Option	Description
TACACS+ Services	Contains a list of the most commonly used TACACS+ services and protocols. Check each TACACS+ service that you want to appear as a configurable option on the Group Setup page or the User Setup page. Note The default interface setting defines a single column of check boxes, at the group level only, for selecting TACACS+ Services Settings and New Service Settings. To view two columns of check boxes that you check to configure settings at the Group level or the User level, you must have checked the Per-user TACACS+/RADIUS Attributes option on the Advanced Options page of the Interface Configuration section. Note Customized settings at the user level take precedence over settings at the group level.
New Services	Use this area to add services and protocols that are particular to your network configuration. Be sure to check the appropriate check box. Note If you have configured ACS to interact with device-management applications for other Cisco products, such as Management Center for Firewalls, ACS might display new TACACS+ services as dictated by these device-management applications. To ensure the proper functioning of ACS, of device-management applications with which ACS interacts, and of the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types. Note The ACS web interface displays any protocol option that is enabled or has nondefault values, even if you have configured that protocol option to be hidden. If you later disable the option or delete its value and the protocol option is configured to be hidden, ACS hides the protocol option. This behavior prevents ACS from hiding active settings.

Advanced Configuration Options (for TACACS+)

Table 2-5 describes the TACACS+ advanced configuration options.

Table 2-5 Displayable TACACS+ Advanced Options

Option	Description
Advanced TACACS+ Features	This option displays or hides the Advanced TACACS+ Options section on the User Setup page. These options include Privilege Level Authentication and Outbound Password Configuration for SENDPASS and SENDAUTH clients, such as routers.
Display a Time-of-Day access grid for every TACACS+ service where you can override the default Time-of-Day settings	<p>If this option is checked, a grid appears on the User Setup page that you use to override the TACACS+ scheduling attributes on the Group Setup page.</p> <p>You can control the use of each TACACS+ service by the time of day and day of week. For example, you can restrict Exec (Telnet) access to business hours but permit PPP-IP access at any time.</p> <p>The default setting is to control time-of-day access for all services as part of authentication. However, you can override the default and display a time-of-day access grid for every service. This setting keeps user and group setup easy to manage, while making this feature available for the most sophisticated environments. This feature applies only to TACACS+ because TACACS+ can separate the authentication and authorization processes. RADIUS time-of-day access applies to all services. If TACACS+ and RADIUS are used simultaneously, the default time-of-day access applies to both. The default provides a common method by which to control access regardless of the access-control protocol.</p>
Display a window for each service selected in which you can enter customized TACACS+ attributes	<p>If you check this option, an area appears on the User Setup and Group Setup pages in which you enter custom TACACS+ attributes.</p> <p>ACS can also display a custom command field for each service. You use this text field to make specialized configurations to be downloaded for a particular service for users in a particular group.</p> <p>You can use this feature to send many TACACS+ commands to the access device for the service, provided that the device supports the command, and that the command syntax is correct. This feature is disabled by default, but you can enable it the same way you enable attributes and time-of-day access.</p>
Display enable Default (Undefined) Service Configuration	<p>If this check box is checked, the 'TACACS+ Unknown Services' check box appears in the User Setup and Group Setup pages that allow you to permit unknown TACACS+ services, such as the Cisco Discovery Protocol (CDP).</p> <p>Note Only advanced system administrators should use this option.</p>

RADIUS Protocols

Table 2-6 describes the RADIUS (IETF and non-IETF) protocols that you can display.

Table 2-6 *Displayable RADIUS Settings*

RADIUS Settings	Description
RADIUS (IETF)	
RADIUS (IETF) Settings	<p>This page lists attributes available for (IETF) RADIUS.</p> <p>These standard (IETF) RADIUS attributes are available for any network device configuration when using RADIUS. If you want to use IETF attribute number 26 (for VSAs), select Interface Configuration and then RADIUS for the vendors whose network devices you use. Attributes for (IETF) RADIUS and the VSA for each RADIUS network device vendor supported by ACS appear in User Setup or Group Setup.</p> <p>The RADIUS (IETF) attributes are shared with RADIUS VSAs. You must configure the first RADIUS attributes from RADIUS (IETF) for the RADIUS vendor.</p> <p>The Tags to Display Per Attribute option (located under Advanced Configuration Options) enables you to specify how many values to display for tagged attributes on the User Setup and Group Setup pages. Examples of tagged attributes include [064]Tunnel-Type and [069]Tunnel-Password.</p> <p>For detailed steps, see Specifying Display of RADIUS (IETF) Options, page 2-9.</p>
RADIUS (Non-IETF, in alphabetical order)	
RADIUS (Ascend) Settings	<p>From this section you enable the RADIUS VSAs for RADIUS (Ascend). This page appears if you have configured a RADIUS (Ascend) or a RADIUS (Cisco IOS/PIX 6.0) device. For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9.</p>
RADIUS (BBSM) Settings	<p>From this section you enable the RADIUS VSAs for RADIUS Building Broadband Service Manager (BBSM). For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9.</p>
RADIUS (Cisco Airespace) Settings	<p>From this section you enable the RADIUS VSAs for RADIUS (Cisco Airespace). This page appears if you have configured a RADIUS (Cisco Airespace) device. For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9.</p>
RADIUS (Cisco Aironet) Settings	<p>This section is now obsolete. You can now use the session-timeout in a dedicated WLAN RADIUS Authorization Component (RAC).</p> <p>We recommend that you do not use the RADIUS Cisco Aironet settings to enable a specific attribute for RADIUS (Cisco Aironet) unless it is an existing configuration.</p> <p>When ACS responds to an authentication request from a Cisco Aironet Access Point and the Cisco-Aironet-Session-Timeout attribute is configured in the RAC, ACS sends to the wireless device this value in the IETF Session-Timeout attribute. This setting enables you to provide different session-timeout values for wireless and wired end-user clients. For steps on adding a WLAN RAC session-timeout, see Adding RADIUS Authorization Components, page 4-10.</p>
RADIUS (Cisco IOS/PIX 6.0) Settings	<p>You use this section to enable the specific attributes for RADIUS (Cisco IOS/PIX 6.0). Selecting the first attribute listed under RADIUS (Cisco IOS/PIX 6.0), 026/009/001, displays an entry field under User Setup and/or Group Setup in which any TACACS+ commands can be entered to fully leverage TACACS+ in a RADIUS environment. For detailed steps, see Specifying Display of RADIUS (<vendor>) Options, page 2-9.</p>

Table 2-6 *Displayable RADIUS Settings (continued)*

RADIUS Settings	Description
RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) Settings	From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 3000/ASA/PIX 7.x+). For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9 .
RADIUS (Cisco VPN 5000) Settings	From this section you enable the RADIUS VSAs for RADIUS (Cisco VPN 5000). For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9 .
RADIUS (Juniper) Settings	From this section you enable the RADIUS VSAs for RADIUS (Juniper). For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9 .
RADIUS (Microsoft) Settings	From this section you enable the RADIUS VSAs for RADIUS (Microsoft). This page appears if you configure a RADIUS (Ascend), or a RADIUS (VPN 3000/ASA/PIX 7.x+), or a RADIUS (Cisco IOS/PIX 6.0) device. For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9 .
RADIUS (Nortel) Settings	From this section you enable the RADIUS VSAs for RADIUS (Nortel). For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9 .
RADIUS (3COMUSR) Settings	From this section you enable the RADIUS VSAs for RADIUS (3COMUSR). For detailed procedures, see Specifying Display of RADIUS (<vendor>) Options, page 2-9 .

Advanced Options (for Interface Configuration)

[Table 2-7](#) describes each advanced Interface Configuration option.

Table 2-7 *Advanced Options (for Interface Configuration)*

Option	Description
Per-User TACACS+/RADIUS Attributes	When selected, this option enables TACACS+/RADIUS attributes to be set at a per-user level, in addition to being set at the group level. After this option is enabled, you must edit the TACACS+ (Cisco IOS) or any RADIUS page in the Interface Configuration section to specify which attributes you want to appear in user accounts. After you do this, user accounts display the selected attributes and enable them to be configured. Attributes configured at the user level override those defined at the group level.
User-Level Shared Network Access Restrictions	When selected, this option enables the Shared Profile Component network-access restrictions (NARs) options on the User Setup page. You use these options to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the user level. For information on defining a NAR, or NAR set, within Shared Profile Components, see Adding a Shared NAR, page 4-21 .
User-Level Network Access Restrictions	When selected, this option enables the two sets of options for defining user-level, IP-based and CLI/DNIS-based NARs, on the User Setup page.
User-Level Downloadable ACLs	When selected, this option enables the Downloadable ACLs (access-control lists) section on the User Setup page.
Default Time-of-Day/Day-of-Week Specification	When selected, this option enables the default time-of-day/day-of-week access settings grid on the Group Setup page.

Table 2-7 *Advanced Options (for Interface Configuration) (continued)*

Option	Description
Group-Level Shared Network Access Restrictions	When selected, this option enables the Shared Profile Component NAR options on the Group Setup page. You use these options to apply previously configured, named, IP-based and CLID/DNIS-based NARs at the group level. For information on defining a NAR, or NAR set, within Shared Profile Components, see Adding a Shared NAR, page 4-21 .
Group-Level Network Access Restrictions	When selected, this option enables the two sets of options for defining group-level, IP-based and CLI/DNIS-based NARs on the Group Setup page.
Group-Level Downloadable ACLs	When selected, this option enables the Downloadable ACLs section on the Group Setup page.
Group-Level Password Aging	When selected, this option enables the Password Aging section on the Group Setup page. The Password Aging option enables you to force users to change their passwords.
Network Access Filtering	When selected, this option enables the Network Access Filtering (NAF) section on the Shared Profiles Components pages. The NAF option lets you set up groups of AAA client configurations (which may represent multiple network devices), network device groups (NDGs), or IP addresses of specific AAA client devices. You can use NAFs with downloadable IP ACLs and network-access restrictions to control access easily by device, which is important when creating your NAPs.
Max Sessions	When selected, this option enables the Max Sessions section on the User Setup and Group Setup pages. The Max Sessions option sets the maximum number of simultaneous connections for a group or a user.
Usage Quotas	When selected, this option enables the Usage Quotas sections on the User Setup and Group Setup pages. The Usage Quotas option sets one or more quotas for usage by a group or a user.
Distributed System Settings	When selected, this option displays the AAA server and proxy tables on the Network Interface page. If the tables have information other than the defaults in them, they always appear. Note You no longer need to select the Distributed System Settings flag to display remote logging configuration options and (ACS for Windows only) ODBC logging options.
ACS Internal Database Replication	When selected, this option enables the ACS database replication information on the System Configuration page.
RDBMS Synchronization	When selected, this option enables the Relational Database Management System (RDBMS) Synchronization option on the System Configuration page. If RDBMS Synchronization is configured, this option always appears.
IP Pools	When selected, this option enables the IP Pools Address Recovery and IP Pools Server options on the System Configuration page.
Network Device Groups	When selected, this option enables NDGs. When NDGs are enabled, the Network Configuration section and parts of the User Setup and Group Setup pages change to enable you to manage groups of network devices (AAA clients or AAA servers). This option is useful if you have many devices to administer.
Voice-over-IP (VoIP) Group Settings	When selected, this option enables the VoIP option on the Group Setup page.

Table 2-7 *Advanced Options (for Interface Configuration) (continued)*

Option	Description
Voice-over-IP (VoIP) Accounting Configuration	When selected, this option enables the VoIP Accounting Configuration option on the System Configuration page. You use this option to determine the logging format of RADIUS VoIP accounting packets.
Microsoft Network Access Protection Settings	When selected, this option enables the Microsoft Network Access Protection feature in the External Posture Validation Setup page. Use this option to enable Network Access Protection settings and configuration throughout ACS.
Submit	Submits the changes and then returns to the Interface Configuration page.
Cancel	Clears new changes and then returns to the Interface Configuration page.



CHAPTER 3

Network Configuration

This chapter details concepts and procedures for configuring the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS. You use the configuration process to establish a distributed system, and set up interaction with authentication, authorization, and accounting (AAA) clients and servers. You can also configure remote agents for the ACS SE.

This chapter contains:

- [About Network Configuration, page 3-1](#)
- [About ACS in Distributed Systems, page 3-2](#)
- [Proxy in Distributed Systems, page 3-3](#)
- [Network Device Searches, page 3-6](#)
- [Configuring AAA Clients, page 3-8](#)
- [Configuring AAA Servers, page 3-15](#)
- [Configuring Remote Agents \(ACS SE Only\), page 3-19](#)
- [Configuring Network Device Groups, page 3-23](#)
- [Configuring Proxy Distribution Tables, page 3-28](#)

About Network Configuration

The appearance of the page that you see when you click Network Configuration differs according to the network-configuration selections that you made in the Interface Configuration section.

The tables that might appear in this section are:

- **AAA Clients**—This table lists each AAA client that is configured on the network, together with its IP address and associated protocol.

If you are using Network Device Groups (NDGs), this table does not appear on the initial page, but is accessed through the Network Device Group table. For more information about this interface configuration, see [Displaying Advanced Options, page 2-6](#).

- **AAA Servers**—This table lists each AAA server that is configured on the network together with its IP address and associated type. After installation, this table automatically lists the machine on which ACS is installed. In ACS SE, the name of the machine is listed as *self*.

If you are using Network Device Groups (NDGs), this table does not appear on the initial page, but is accessed through the Network Device Group table. For more information about this interface configuration, see [Displaying Advanced Options, page 2-6](#).

- **Remote Agents** (ACS SE)—This table lists each remote agent that is configured together with its IP address and available services. For more information about remote agents, see [About Remote Agents, page 3-19](#).

**Note**

The Remote Agents table does not appear unless you have enabled the Distributed System Settings feature in Interface Configuration. If you are using NDGs, this table does not appear on the initial page, but is accessed through the Network Device Groups table. For more information about this interface configuration, see [Displaying Advanced Options, page 2-6](#).

- **Network Device Groups**—This table lists the name of each NDG that has been configured, and the number of AAA clients and AAA servers that are assigned to each NDG. If you are using NDGs, the AAA Clients table and AAA Servers table do not appear on the opening page. To configure AAA clients or AAA servers, you must click the name of the NDG to which the device is assigned. If the newly configured device is not assigned to an NDG, it belongs to the (Not Assigned) group.

This table appears only when you have configured the interface to use NDGs. For more information about this interface configuration, see [Displaying Advanced Options, page 2-6](#).

- **Proxy Distribution Table**—You can use the Proxy Distribution Table to configure proxy capabilities including domain stripping. For more information, see [Configuring Proxy Distribution Tables, page 3-28](#).

This table appears only when you have configured the interface to enable Distributed Systems Settings. For more information about this interface configuration, see [Displaying Advanced Options, page 2-6](#).

About ACS in Distributed Systems

These topics describe how ACS can be used in a distributed system.

- [AAA Servers in Distributed Systems, page 3-2](#)
- [Default Distributed System Settings, page 3-3](#)

AAA Servers in Distributed Systems

AAA server is the generic term for an access-control server (ACS), and the two terms are often used interchangeably. Multiple AAA servers can be configured to communicate with one another as primary, backup, client, or peer systems. You can, therefore, use powerful features such as:

- Proxy
- Fallback on failed connection
- ACS internal database replication
- Remote and centralized logging

You can configure AAA servers to determine who can access the network and what services are authorized for each user. The AAA server stores a profile containing authentication and authorization information for each user. Authentication information validates user identity, and authorization information determines what network services a user can to use. A single AAA server can provide concurrent AAA services to many dial-up access servers, routers, and firewalls. Each network device can be configured to communicate with a AAA server. You can, therefore, centrally control dial-up access, and secure network devices from unauthorized access.

These types of access control have unique authentication and authorization requirements. With ACS, system administrators can use a variety of authentication methods that are used with different degrees of authorization privileges.

Completing the AAA functionality, ACS serves as a central repository for accounting information. Each user session that ACS grants can be fully accounted for, and its accounting information can be stored in the server. You can use this accounting information for billing, capacity planning, and security audits.

**Note**

If the fields mentioned in this section do not appear in the ACS web interface, you can enable them by choosing **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

Default Distributed System Settings

You use the AAA Servers table and the Proxy Distribution Table to establish distributed system settings. The parameters that are configured within these tables create the foundation so that you can configure multiple ACSs to work with one another. Each table contains an ACS entry for itself. In the AAA Servers table, the only AAA server that is initially listed is itself (in ACS SE, the server name is listed as *self*); the Proxy Distribution Table lists an initial entry of *(Default)*, which displays how the local ACS is configured to handle each authentication request locally.

You can configure additional AAA servers in the AAA Servers table. These devices can, therefore, become visible in the web interface so that they can be configured for other distributed features such as proxy, ACS internal database replication, remote logging, and RDBMS synchronization. For information about configuring additional AAA servers, see [Adding AAA Servers, page 3-17](#).

Proxy in Distributed Systems

Proxy is a powerful feature that enables you to use ACS for authentication in a network that uses more than one AAA server. This section contains:

- [The Proxy Feature, page 3-3](#)
- [Fallback on Failed Connection, page 3-4](#)
- [Remote Use of Accounting Packets, page 3-5](#)
- [Other Features Enabled by System Distribution, page 3-6](#)

The Proxy Feature

Using proxy, ACS automatically forwards an authentication request from AAA clients to AAA servers. After the request has been successfully authenticated, the authorization privileges that you configured for the user on the remote AAA server are passed back to the original ACS, where the AAA client applies the user profile information for that session.

Proxy provides a useful service to users, such as business travelers, who dial in to a network device other than the one they normally use and would otherwise be authenticated by a foreign AAA server. To configure proxy, you choose **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

An Example

This section presents a scenario of proxy that is used in an enterprise system. Mary is an employee with an office in the corporate headquarters in Los Angeles. Her username is *mary@la.corporate.com*. When Mary needs access to the network, she accesses the network locally and authenticates her username and password. Because Mary works in the Los Angeles office, her user profile, which defines her authentication and authorization privileges, resides on the local Los Angeles AAA server.

However, Mary occasionally travels to a division within the corporation in New York, where she still needs to access the corporate network to get her e-mail and other files. When Mary is in New York, she dials in to the New York office and logs in as *mary@la.corporate.com*. The New York ACS does not recognize her username, but the Proxy Distribution Table contains an entry, *@la.corporate.com*, to forward the authentication request to the Los Angeles ACS. Because the username and password information for Mary reside on that AAA server, when she authenticates correctly, the AAA client in the New York office applies the authorization parameters that are assigned to her.

Proxy Distribution Table

Whether, and where, an authentication request is to be forwarded is defined in the Proxy Distribution Table on the Network Configuration page. You can use multiple ACSs throughout your network. For information about configuring the Proxy Distribution Table, see [Configuring Proxy Distribution Tables, page 3-28](#).

ACS employs character strings that the administrator defines to determine whether an authentication request should be processed locally or forwarded, and where. When an end user dials in to the network device and ACS finds a match for the character string defined in the Proxy Distribution Table, ACS forwards the authentication request to the associated remote AAA server.



Note

When an ACS receives a TACACS+ authentication request forwarded by proxy, any requests for Network Access Restrictions for TACACS+ are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.



Note

When an ACS proxies to a second ACS, the second ACS responds to the first by using only IETF attributes, no VSAs, when it recognizes the first ACS as the AAA server. Alternatively, you can configure the second ACS to see an ACS as a AAA client; in this case, the second ACS responses include the RADIUS VSAs for whatever RADIUS vendor is specified in the AAA client definition table entry—in the same manner as any other AAA client.

Administrators with geographically dispersed networks can configure and manage the user profiles of employees within their immediate location or building. The administrator can, therefore, manage the policies of just their users and all authentication requests from other users within the company can be forwarded to their respective AAA server for authentication. Not every user profile must reside on every AAA server. Proxies save administration time and server space, and allows end users to receive the same privileges regardless of the access device through which they connect.

Fallback on Failed Connection

You can configure the order in which ACS checks remote AAA servers if a failure of the network connection to the primary AAA server occurs. If an authentication request cannot be sent to the first listed server, because of a network failure for example, the next listed server is checked. This checking

continues, in order, down the list, until the AAA servers handles the authentication request. (Failed connections are detected by failure of the nominated server to respond within a specified time period. That is, the request is timed out.) If ACS cannot connect to any server in the list, authentication fails.

Character String

ACS forwards authentication requests by using a configurable set of characters with a delimiter, such as periods (.), slashes (/), or hyphens (-). When configuring the ACS character string, you must specify whether the character string is the prefix or suffix. For example, you can use *domain.us* as a suffix character string in *username*domain.us*, where the asterisk (*) represents any delimiter. An example of a prefix character string is *domain.*username*, where the asterisk (*) would be used to detect the slash(/).

Stripping

Stripping allows ACS to remove, or strip, the matched character string from the username. When you enable stripping, ACS examines each authentication request for matching information. When ACS finds a match by character string in the Proxy Distribution Table, as described in the example under [Proxy in Distributed Systems, page 3-3](#), ACS strips off the character string if you have configured it to do so. For example, in the following proxy example, the character string that accompanies the username establishes the ability to forward the request to another AAA server. If the user must enter the user ID of *mary@corporate.com* to be forwarded correctly to the AAA server for authentication, ACS might find a match on the *@corporate.com* character string, and strip the *@corporate.com*, leaving a username of *mary*, which might be the username format that the destination AAA server requires to identify the correct entry in its database.



Note

Realm stripping does not work with Extensible Authentication Protocol (EAP)-based authentication protocols, such as Protected Extensible Authentication Protocol (PEAP) or Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST). For example, if you are using Protected Extensible Authentication Protocol Microsoft Challenge Authentication Handshake Protocol (PEAP MSCHAP), authentication will fail if a realm is stripped by proxy.

Remote Use of Accounting Packets

When proxy is employed, ACS can dispatch AAA accounting packets in one of three ways:

- Log them locally.
- Forward them to the destination AAA server.
- Log them locally and forward copies to the destination AAA server.

Sending accounting packets to the remote ACS offers several benefits.

- When ACS is configured to send accounting packets to the remote AAA server, the remote AAA server logs an entry in the accounting report for that session on the destination server. ACS also caches the user connection information and adds an entry in the List Logged on Users report. You can then view the information for users that are currently connected. Because the accounting information is sent to the remote AAA server, even if the connection fails, you can view the Failed Attempts report to troubleshoot the failed connection.

- Sending the accounting information to the remote AAA server also enables you to use the Max Sessions feature. The Max Sessions feature uses the Start and Stop records in the accounting packet. If the remote AAA server is an ACS and the Max Sessions feature is implemented, you can track the number of sessions that are allowed for each user or group.
- You can also choose to have Voice-over-IP (VoIP) accounting information logged remotely, appended to the RADIUS Accounting log, entered in a separate VoIP Accounting log, or both.

Other Features Enabled by System Distribution

Beyond basic proxy and fallback features, configuring an ACS to interact with distributed systems enables several other features that are beyond the scope of this chapter. These features include:

- **Replication**—For more information, see [ACS Internal Database Replication, page 8-1](#).
- **RDBMS synchronization**—For more information, see [RDBMS Synchronization, page 8-17](#).
- **Remote and centralized logging**—For more information, see [Remote Logging for ACS for Windows, page 10-10](#), and [Remote Logging for ACS SE with ACS Remote Agents, page 10-10](#).

Network Device Searches

You can search for any network device that is configured in the Network Configuration section of the ACS web interface.

This section contains:

- [Network Device Search Criteria, page 3-6](#)
- [Searching for Network Devices, page 3-7](#)

Network Device Search Criteria

You can specify search criteria for network device searches. ACS provides the following search criteria:

- **Name**—The name assigned to the network device in ACS. You can use an asterisk (*) as a wildcard character. For example, if you wanted to find all devices with names starting with the letter M, you would enter *M** or *m**. Name-based searches are case insensitive. If you do not want to search based on device name, you can leave the Name box blank or you can put only an asterisk (*) in the Name box.
- **IP Address**—The IP address specified for the network device in ACS. For each octet in the address, you have three options:
 - **Number**—You can specify a number, for example, 10.3.157.98.
 - **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen (-), for example, 10.3.157.10-50.
 - **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

ACS allows any octet or octets in the IP Address box to be a number, a numeric range, or an asterisk (*), for example 172.16-31.*.*.

- **Type**—The device type, as specified by the AAA protocol that it is configured to use, or the kind of AAA server it is. You can also search for Solution Engine remote agents. If you do not want to limit the search based on device type, choose **Any** from the Type list.
- **Device Group**—The NDG to which the device is assigned. This search criterion only appears if you have enabled Network Device Groups on the Advanced Options page in the Interface Configuration section. If you do not want to limit the search based on NDG membership, select **Any** from the Device Group list.

Searching for Network Devices

To search for a network device:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Click **Search**.

The Search for Network Devices page appears. In the configuration area, the controls for setting search criteria appear above the search results for the most recent search that was previously conducted for this session, if any.



Tip

When you leave the Search for Network Devices page, ACS retains your search criteria and results for the duration of the current administrative session. Until you log out of ACS, you can return to the Search for Network Devices page to view your most recent search criteria and results.

Step 3 Set the criteria for a device search. For information about search criteria, see [Network Device Search Criteria, page 3-6](#).



Tip

To reset the search criteria to default settings, click **Clear**.

Step 4 Click **Search**.

A table lists each network device configured in ACS that matches the search criteria you specified. If ACS did not find a matching network device, the message `No Search Results` appears.

The table listing that matches network devices includes the device name, IP address, and type. If you have enabled Network Device Groups on the Advanced Options page in the Interface Configuration Section, the table also includes the NDG of each matching network device.



Tip

You can sort the table rows by whichever column you want, in ascending or descending order. Click a column title once to sort the rows by the entries in that column in ascending order. Click the column a second time to sort the rows by the entries in that column in descending order.

Step 5 If you want to view the configuration settings for a network device found by the search, click the network device name in the Name column in the table of matching network devices.

ACS displays the applicable setup page. For information about the AAA Client Setup page, see [AAA Client Configuration Options, page 3-8](#). For information about the AAA Server Setup page, see [AAA Server Configuration Options, page 3-15](#).

- Step 6** If you want to download a file containing the search results in a comma-separated value format, click **Download**, and use your browser to save the file to a location and filename of your choice.
- Step 7** If you want to search again by using different criteria, repeat Step 3 and Step 4.
-

Configuring AAA Clients

This guide uses the term “AAA client” comprehensively to signify the device through which or to which service access is attempted. This is the RADIUS or TACACS+ client device, and may comprise Network Access Servers (NASs), PIX Firewalls, routers, or any other RADIUS or TACACS+ hardware or software client.

This section contains:

- [AAA Client Configuration Options, page 3-8](#)
- [Adding AAA Clients, page 3-12](#)
- [Editing AAA Clients, page 3-13](#)
- [Deleting AAA Clients, page 3-14](#)

AAA Client Configuration Options

AAA client configurations enable ACS to interact with the network devices that the configuration represents. A network device that does not have a corresponding configuration in ACS, or whose configuration in ACS is incorrect, does not receive AAA services from ACS.

The Add AAA Client and AAA Client Setup pages include:

- **AAA Client Hostname**—The name that you assign to the AAA client configuration. Each AAA client configuration can represent multiple network devices; thus, the AAA client hostname configured in ACS is not required to match the hostname configured on a network device. We recommend that you adopt a descriptive, consistent naming convention for AAA client hostnames. Maximum length for AAA client hostnames is 32 characters.



Note After you submit the AAA client hostname, you cannot change it. If you want to use a different name for AAA clients, delete the AAA client configuration and create a new AAA client configuration by using the new name.

- **AAA Client IP Address**—At a minimum, a single IP address of the AAA client or the keyword **dynamic**.

If you only use the keyword **dynamic**, with no IP addresses, the AAA client configuration can only be used for command authorization for Cisco multi device-management applications, such as Management Center for Firewalls. ACS only provides AAA services to devices based on IP address; so it ignores such requests from a device whose AAA client configuration only has the keyword **dynamic** in the Client IP Address box.

If you want the AAA client configuration in ACS to represent multiple network devices, you can specify multiple IP addresses. Separate each IP address by pressing **Enter**.

In each IP address that you specify, you have three options for each octet in the address:

- **Number**—You can specify a number, for example, 10.3.157.98.
- **Numeric Range**—You can specify the low and high numbers of the range in the octet, separated by a hyphen (-), for example, 10.3.157.10-50.
- **Wildcard**—You can use an asterisk (*) to match all numbers in that octet, for example, 10.3.157.*.

ACS allows any octet or octets in the IP Address box to be a number, a numeric range, or an asterisk (*), for example 172.16-31.*.*.

- **Shared Secret**—The shared secret key of the AAA client. Maximum length for the AAA client key is 64 characters.

For correct operation, the key must be identical on the AAA client and ACS. Keys are case sensitive. If the shared secret does not match, ACS discards all packets from the network device.

- **Network Device Group**—The name of the NDG to which this AAA client should belong. To make the AAA client independent of NDGs, use the Not Assigned selection.



Note This option does not appear if you have not configured ACS to use NDGs. To enable NDGs, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

- **RADIUS Key Wrap**—The shared secret keys for RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications. Each key must be unique, and must also be distinct from the RADIUS shared key. These shared keys are configurable for each AAA Client, as well as for each NDG. The NDG key configuration overrides the AAA Client configuration.
 - **Key Encryption Key (KEK)**—This is used for encryption of the Pairwise Master Key (PMK). In ASCII mode, enter a key length of exactly 16 characters; in hexadecimal mode, enter a key length of 32 characters.
 - **Message Authentication Code Key (MACK)**—This is used for the keyed hashed message authentication code (HMAC) calculation over the RADIUS message. In ASCII mode, enter a key length of exactly 20 characters; in hexadecimal mode, enter a key length of 40 characters.



Note If you leave a key field empty when key wrap is enabled, the key will contain only zeros.

- **Key Input Format**—Select whether to enter the keys as ASCII or hexadecimal strings (the default is ASCII).



Note You must enable the Key Wrap feature in the NAP Authentication Settings page to implement these shared keys in PEAP, EAP-FAST and EAP-TLS authentication.

- **Authenticate Using**—The AAA protocol to use for communications with the AAA client. The Authenticate Using list includes Cisco IOS TACACS+ and several vendor-specific implementations of RADIUS. If you have configured user-defined RADIUS vendors and VSAs, those vendor-specific RADIUS implementations appear on the list also. For information about creating user-defined RADIUS VSAs, see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#).

The Authenticate Using list always contains:

- **TACACS+ (Cisco IOS)**—The Cisco IOS TACACS+ protocol, which is the standard choice when using Cisco Systems access servers, routers, and firewalls. If the AAA client is a Cisco device-management application, such as Management Center for Firewalls, you must use this option.
- **RADIUS (Cisco Airespace)**—RADIUS using Cisco Airespace VSAs. Select this option if the network device is a Cisco Airespace WLAN device supporting authentication via RADIUS.
- **RADIUS (Cisco Aironet)**—RADIUS using Cisco Aironet VSAs. Select this option if the network device is a Cisco Aironet Access Point used by users who authenticate with the Lightweight and Efficient Application Protocol (LEAP) or the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) protocol, provided that these protocols are enabled on the Global Authentication Setup page in the System Configuration section.

When an authentication request from a RADIUS (Cisco Aironet) AAA client arrives, ACS first attempts authentication by using LEAP; if this fails, ACS fails over to EAP-TLS. If LEAP is not enabled on the Global Authentication Setup page, ACS immediately attempts EAP-TLS authentication. If neither LEAP nor EAP-TLS is enabled on the Global Authentication Setup, any authentication attempt received from a Cisco Aironet RADIUS client fails. For more information about enabling LEAP or EAP-TLS, see [Global Authentication Setup, page 9-21](#).

Using this option enables ACS to send the wireless network device a different session-timeout value for user sessions than ACS sends to wired end-user clients.

Users accessing the network through a Cisco Aironet network device can only be authenticated against the:

- ACS internal database
- Windows user database
- ODBC user database
- MCIS database



Note

If all authentication requests from a particular Cisco Aironet Access Point are PEAP or EAP-TLS requests, use RADIUS (IETF) instead of RADIUS (Cisco Aironet). ACS cannot support PEAP authentication by using the RADIUS (Cisco Aironet) protocol.

- **RADIUS (Cisco BBSM)**—RADIUS using Cisco Broadband Services Manager (BBSM) Vendor Specific Attributes (VSAs). Select this option if the network device is a Cisco BBSM network device supporting authentication via RADIUS.
- **RADIUS (Cisco IOS/PIX 6.0)**—RADIUS using Cisco IOS/PIX 6.0 VSAs. This option enables you to pack commands sent to a Cisco IOS or Project Information Exchange (PIX)S 6.0 AAA client. The commands are defined in the Group Setup section. Select this option for RADIUS environments in which key TACACS+ functions are required to support Cisco IOS and PIX equipment.
- **RADIUS (Cisco VPN 3000/ASA/PIX7.x+)**—RADIUS using Cisco VPN 3000 concentrator, ASA device, and PIX 7.x device VSAs. Select this option if the network device is a Cisco VPN 3000 series concentrator, an ASA, or PIX 7.x+ device supporting authentication via RADIUS.
- **RADIUS (Cisco VPN 5000)**—RADIUS using Cisco VPN 5000 VSAs. Select this option if the network device is a Cisco VPN 5000 series Concentrator.

- **RADIUS (IETF)**—IETF-standard RADIUS, using no VSAs. Select this option if the AAA client represents RADIUS-enabled devices from more than one manufacturer and you want to use standard IETF RADIUS attributes. If the AAA client represents a Cisco Aironet Access Point used only by users who authenticate with PEAP or EAP-TLS, this is also the protocol to select.
- **RADIUS (Ascend)**—RADIUS using Ascend RADIUS VSAs. Select this option if the network device is an Ascend network device that supports authentication via RADIUS.
- **RADIUS (Juniper)**—RADIUS using Juniper RADIUS VSAs. Select this option if the network device is a Juniper network device that supports authentication via RADIUS.
- **RADIUS (Nortel)**—RADIUS using Nortel RADIUS VSAs. Select this option if the network device is a Nortel network device that supports authentication via RADIUS.
- **RADIUS (iPass)**—RADIUS for AAA clients using iPass RADIUS. Select this option if the network device is an iPass network device supporting authentication via RADIUS. The iPass RADIUS is identical to IETF RADIUS.
- **RADIUS (3COMUSR)**—RADIUS using 3COMUSR RADIUS VSAs. Select this option if the network device is a 3COMUSR network device that supports authentication via RADIUS.
- **Single Connect TACACS+ AAA Client (Record stop in accounting on failure)**—If you select TACACS+ (Cisco IOS) from the Authenticate Using list, you can use this option to specify that ACS use a single TCP connection for all TACACS+ communication with the AAA client, rather than a new one for every TACACS+ request. In single connection mode, multiple requests from a network device are multiplexed over a single TCP session. By default, this check box is unchecked.

If this feature is selected and the connection fails, a stop record is sent to the TACACS+ accounting log for each user connected through the AAA client.



Note If TCP connections between ACS and the AAA client are unreliable, do not use this feature.

- **Log Update/Watchdog Packets from this AAA Client**—Enables logging of update or watchdog packets. Watchdog packets are interim packets that are sent periodically during a session. They provide you with an approximate session length if the AAA client fails and, therefore, no stop packet is received to mark the end of the session. By default, this check box is unchecked.
- **Log RADIUS Tunneling Packets from this AAA Client**—Enables logging of RADIUS tunneling accounting packets. Packets are recorded in the RADIUS Accounting reports of Reports and Activity. By default, this check box is unchecked.
- **Replace RADIUS Port info with Username from this AAA Client**—Enables use of username, rather than port number, for session-state tracking. This option is useful when the AAA client cannot provide unique port values, such as a gateway GPRS support node (GGSN). For example, if you use the ACS IP pools server and the AAA client does not provide a unique port for each user, ACS assumes that a reused port number indicates that the previous user session has ended and ACS may reassign the IP address that was previously assigned to the session with the non-unique port number. By default, this check box is unchecked.



Note If this option is enabled, ACS cannot determine the number of user sessions for each user. Each session uses the same session identifier, the username; therefore, the Max Sessions feature is ineffective for users accessing the network through the AAA client with this feature enabled.

- **Match Framed-IP-Address with user IP address for accounting packets from this AAA Client**—Select this option when the AAA client uses Cisco SSL WebVPN. This action ensures that ACS assigns different IP addresses to two different users when they log in via a Cisco SSL WebVPN client. By default, this check box is unchecked.

Adding AAA Clients

You can use this procedure to add AAA client configurations.

Before You Begin

For ACS to provide AAA services to AAA clients, you must ensure that gateway devices between AAA clients and ACS allow communication over the ports needed to support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see [AAA Protocols—TACACS+ and RADIUS, page 1-3](#).

To add AAA clients:

-
- Step 1** In the navigation bar, click **Network Configuration**.
- The Network Configuration page opens.
- Step 2** Do one of the following:
- If you are using NDGs, click the name of the NDG to which you want to assign the AAA client. Then, click **Add Entry** below the AAA Clients table.
 - To add AAA clients when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.
- The Add AAA Client page appears.
- Step 3** Enter the AAA client settings, as needed. For information about the configuration options available for the AAA client, see [AAA Client Configuration Options, page 3-8](#).
- Step 4** To save your changes and apply them immediately, click **Submit + Apply**.



Note

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter.



Tip

If you want to save your changes and apply them later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

Editing AAA Clients

You can use the following procedure to edit the settings for AAA client configurations.



Note

You cannot directly edit the names of AAA clients; rather, you must delete the AAA client entry and then reestablish the entry with the corrected name. For steps about deleting AAA client configurations, see [Deleting AAA Clients, page 3-14](#). For steps about creating AAA client configurations, see [Adding AAA Clients, page 3-12](#).

Before You Begin

For ACS to provide AAA services to AAA clients, you must ensure that gateway devices between AAA clients and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see [AAA Protocols—TACACS+ and RADIUS, page 1-3](#).

To edit AAA clients:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the name of the AAA client.
- To edit AAA clients when you have not enabled NDGs, click the name of the AAA client in the AAA Client Hostname column of the AAA Clients table.

The AAA Client Setup For *Name* page appears.

Step 3 Modify the AAA client settings, as needed. For information about the configuration options available for the AAA client, see [AAA Client Configuration Options, page 3-8](#).



Note

You cannot directly edit the name of the AAA client; rather, you must delete the AAA client entry and then re-establish the entry with the corrected name. For steps about deleting the AAA client entry, see [Deleting AAA Clients, page 3-14](#). For steps about creating the AAA client entry, see [Adding AAA Clients, page 3-12](#).

Step 4 To save your changes and apply them immediately, click **Submit + Apply**.



Tip

To save your changes and apply them later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.



Note

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter.

Configuring a Default AAA Client

You can configure a default AAA Client to accommodate any unrecognized AAA Clients (NAS):

-
- Step 1** Follow the steps for [Adding AAA Clients, page 3-12](#).
- Step 2** Leave the AAA Client Hostname and AAA Client IP address blank.
- Step 3** Complete the rest of the fields and continue with the rest of the procedure for adding AAA Clients.

**Note**

Only TACACS+ can have a default AAA Client configured. The default name for the client is **Others** and the default IP address is 0.0.0.0.

Deleting AAA Clients

To delete AAA clients:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** Do one of the following:
- If you are using NDGs, click the name of the NDG to which the AAA client is assigned. Then, click the AAA client hostname in the AAA Clients table.
 - To delete AAA clients when you have not enabled NDGs, click the AAA client hostname in the AAA Clients table.

The AAA Client Setup for the *Name* page appears.

- Step 3** To delete the AAA client and have the deletion take effect immediately, click **Delete + Apply**.

**Note**

Restarting ACS services clears the Logged-in User report and temporarily interrupts all ACS services. As an alternative to restarting when you delete AAA clients, you can click **Delete**. However, when you do, the change does not take effect until you restart the system, which you can do by choosing **System Configuration > Service Control**. Then, choose **Restart**.

A confirmation dialog box appears.

- Step 4** Click **OK**.

ACS restarts AAA services and the AAA client is deleted.

If you have a configured RADIUS/TACACS source-interface command on the AAA client, ensure that you configure the client on ACS by using the IP address of the interface that is specified.

Configuring AAA Servers

This section presents procedures for configuring AAA servers in the ACS web interface. For additional information about AAA servers, see [AAA Servers in Distributed Systems, page 3-2](#).

To configure distributed system features for a given ACS, you must first define the other AAA server(s). For example, all ACSs that are involved in replication, remote logging, authentication proxying, and RDBMS synchronization must have AAA server configurations for each other; otherwise, incoming communication from an unknown ACS is ignored and the distributed system feature will fail.



Tip

If the AAA Servers table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

This section contains:

- [AAA Server Configuration Options, page 3-15](#)
- [Adding AAA Servers, page 3-17](#)
- [Editing AAA Servers, page 3-17](#)
- [Deleting AAA Servers, page 3-18](#)

AAA Server Configuration Options

AAA server configurations enable ACS to interact with the AAA server that the configuration represents. AAA servers that do not have a corresponding configuration in ACS, or whose configuration in ACS is incorrect, do not receive AAA services from ACS, such as proxied authentication requests, database replication communication, remote logging, and RDBMS synchronization. Also, several distributed systems features require that the other ACSs included in the distributed system be represented in the AAA Servers table. For more information about distributed systems features, see [About ACS in Distributed Systems, page 3-2](#).

After installation, the AAA Servers table automatically lists the machine on which ACS is installed. This machine is also defined as the default proxy server in the Proxy Distribution table, and appears by default in the RDBMS table.



Note

In ACS SE, the name of the machine in the AAA servers table is listed as *self*; in the Proxy Distribution and RDBMS tables the appliance hostname is listed.

The Add AAA Server and AAA Server Setup pages include the following options:

- **AAA Server Name**—The name that you assign to the AAA server configuration. The AAA server hostname that is configured in ACS does not have to match the hostname configured on a network device. We recommend that you adopt a descriptive, consistent naming convention for AAA server names. Maximum length for AAA server names is 32 characters.



Note

After you submit the AAA server name, you cannot change it. If you want to use a different name for the AAA server, delete the AAA server configuration and create the AAA server configuration by using the new name.

- **AAA Server IP Address**—The IP address of the AAA server, in dotted, four-octet format. For example, 10.77.234.3.
- **Key**—The shared secret of the AAA server. Maximum length for AAA server keys is 64 characters. For correct operation, the key must be identical on the remote AAA server and ACS. Keys are case sensitive. Because shared secrets are not synchronized, you could easily make mistakes when entering them on remote AAA servers and ACS. If the shared secret does not match, ACS discards all packets from the remote AAA server.
- **Network Device Group**—The name of the NDG to which this AAA server should belong. To make the AAA server independent of NDGs, use the Not Assigned selection.

**Note**

This option does not appear if you have not configured ACS to use NDGs. To enable NDGs, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

- **Log Update/Watchdog Packets from this remote AAA Server**—Enables logging of update or watchdog packets from AAA clients that are forwarded by the remote AAA server to this ACS. Watchdog packets are interim packets that are sent periodically during a session. They provide you with an approximate session length if the AAA client fails and, therefore, no stop packet is received to mark the end of the session.
- **AAA Server Type**—One of types:
 - **RADIUS**—Select this option if the remote AAA server is configured by using any type of RADIUS protocol.
 - **TACACS+**—Select this option if the remote AAA server is configured by using the TACACS+ protocol.
 - **ACS**—Select this option if the remote AAA server is another ACS. This action enables you to configure features that are only available with other ACSs, such as ACS internal database replication and remote logging.
- **Traffic Type**—The Traffic Type list defines the direction in which traffic to and from the remote AAA server is permitted to flow from this ACS. The list includes:
 - **Inbound**—The remote AAA server accepts requests that have been forwarded to it and does not forward the requests to another AAA server. Select this option if you do not want to permit any authentication requests to be forwarded from the remote AAA server.
 - **Outbound**—The remote AAA server sends out authentication requests but does not receive them. If a Proxy Distribution Table entry is configured to proxy authentication requests to the AAA server that is configured for Outbound, the authentication request is not sent.
 - **Inbound/Outbound**—The remote AAA server forwards and accepts authentication requests, allowing the selected server to handle authentication requests in any manner that is defined in the distribution tables.
- **AAA Server RADIUS Authentication Port**—Specify the port on which the AAA server accepts authentication requests. The standard port is 1812, and another commonly used port is 1645. If you select **TACACS+** in the AAA Server Type field, this RADIUS Authentication Port field is dimmed.
- **AAA Server RADIUS Accounting Port**—Specify the port on which the AAA server accepts accounting information. The standard port is 1813, and another commonly used port is 1646. If you select **TACACS+** in the AAA Server Type field, this RADIUS Accounting Port field is dimmed.

Adding AAA Servers

Before You Begin

For descriptions of the options that are available while adding a remote AAA server configuration, see [AAA Server Configuration Options, page 3-15](#).

For ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see [AAA Protocols—TACACS+ and RADIUS, page 1-3](#).

To add and configure AAA servers:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** Do one of the following:
- If you are using NDGs, click the name of the NDG to which the AAA server is to be assigned. Then, click **Add Entry** below the [name] AAA Servers table.
 - To add AAA servers when you have not enabled NDGs, below the AAA Servers table, click **Add Entry**.
- The Add AAA Server page appears.
- Step 3** Enter the AAA server settings, as needed. For information about the configuration options available for the AAA server, see [AAA Server Configuration Options, page 3-15](#).
- Step 4** To save your changes and apply them immediately, click **Submit + Apply**.



Tip

To save your changes and apply them later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.



Note

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to (0).

Editing AAA Servers

Use this procedure to edit the settings for AAA servers that you have previously configured.



Note

You cannot edit the names of AAA servers. To rename AAA servers, you must delete the existing AAA server entry and then add a new server entry with the new name.

Before You Begin

For descriptions of the options available while editing a remote AAA server entry, see [AAA Server Configuration Options, page 3-15](#).

For ACS to provide AAA services to a remote AAA server, you must ensure that gateway devices between the remote AAA server and ACS permit communication over the ports that support the applicable AAA protocol (RADIUS or TACACS+). For information about ports that AAA protocols use, see [AAA Protocols—TACACS+ and RADIUS, page 1-3](#).

To edit AAA servers:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, in the AAA Servers table, click the name of the AAA server to be edited.
- If you have not enabled NDGs, in the AAA Servers table, click the name of the AAA server to be edited.

The AAA Server Setup for *X* page appears.

Step 3 Enter or change AAA server settings, as needed. For information about the configuration options available for the AAA server, see [AAA Server Configuration Options, page 3-15](#).

Step 4 To save your changes and apply them immediately, click **Submit + Apply**.



Tip

To save your changes and apply them later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.



Note

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to (0).

Deleting AAA Servers

To delete AAA servers:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using NDGs, click the name of the NDG to which the AAA server is assigned. Then, click the AAA server name in the AAA Servers table.
- If you have not enabled NDGs, click the AAA server name in the AAA Servers table.

The AAA Server Setup for *X* page appears.

Step 3 To delete the AAA server and have the deletion take effect immediately, click **Delete + Apply**.

**Note**

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. As an alternative to restarting when you delete AAA servers, in the preceding step you can click **Delete**. However, when you do this, the change does not take effect until you restart the system, which you can do by choosing **System Configuration > Service Control**. Then, choose **Restart**.

A confirmation dialog box appears.

Step 4 Click **OK**.

ACS performs a restart and the AAA server is deleted.

Configuring Remote Agents (ACS SE Only)

This section presents information about remote agents and procedures for configuring remote agents in the ACS web interface.

This section contains:

- [About Remote Agents, page 3-19](#)
- [Remote Agent Configuration Options, page 3-19](#)
- [Adding a Remote Agent, page 3-21](#)
- [Editing a Remote Agent Configuration, page 3-22](#)
- [Deleting a Remote Agent Configuration, page 3-23](#)

About Remote Agents

An ACS SE can use remote agents for remote logging and authentication of users with a Windows external user database. Before you can configure remote logging and authentication by using a Windows external user database, you must add at least one remote agent configuration to the Remote Agents table in the Network Configuration section.

For more information about remote agents, including how to install and configure them, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Remote Agent Configuration Options

The Add Remote Agent and Remote Agent Setup pages include the following options:

**Note**

A remote agent that does not have a corresponding configuration in ACS, or whose configuration in ACS is incorrect, cannot communicate with ACS to receive its configuration, logging data, or Windows authentication requests.

- **Remote Agent Name**—The name that you assign to the remote agent configuration. You configure remote agent logging and Windows authentication by using remote agent names. We recommend that you adopt a descriptive, consistent naming convention for remote agents. For example, you could assign the same name as the hostname of the server that runs the remote agent. The maximum length for a remote agent name is 32 characters.



Note After you submit the remote agent name, you cannot change it. If you want to use a different name for a remote agent, delete the remote agent configuration, create a new remote agent configuration by using the new name, and change remote logging and Windows authentication configurations that use the remote agent.

- **Remote Agent IP Address**—The IP address of the remote agent, in dotted-decimal format. For example, 10.77.234.3.
- **Remote Agent Port**—The TCP port on which the remote agent listens for communication from ACS. The maximum length for the TCP port number is 6 characters. The Remote Agent Port must be a numeric value in the range of 0 to 65535.



Note If the port number that you provide does not match the port the remote agent that you configured for listening, ACS cannot communicate with the remote agent. For information about configuring the remote agent port, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

- **Network Device Group**—The name of the NDG to which this remote agent should belong. To make the remote agent independent of NDGs, chose the **Not Assigned** selection.

In addition to the options in the preceding list, the Remote Agent Setup page includes the following options:

- **Running Status**—Information about the status of the remote agent. If ACS can contact the remote agent, the uptime for the remote agent appears. If ACS cannot contact the remote agent, the message `Not responding` appears.
- **Configuration Provider**—The ACS from which the remote agent receives its configuration.



Tip

Click on the ACS name to access the web interface for the ACS that provides configuration data to a remote agent. A new browser window displays the web interface for the ACS that provides configuration data to the remote agent.

- **Service Table**—ACS displays a table of remote agent services below the Configuration Provider. The table includes the following columns:
 - **Service**—A list of services that a remote agent can provide: remote logging and Windows authentication.
 - **Available**—Whether the remote agent can currently provide the corresponding service.
 - **Used by this ACS**—Whether the ACS into which you are logged is currently using the corresponding service.

Adding a Remote Agent

Before You Begin

For descriptions of the options available while adding a remote agent configuration, see [Remote Agent Configuration Options, page 3-19](#).

For ACS to communicate with a remote agent, you must ensure that gateway devices between a remote agent and ACS permit communication over the TCP ports used by remote agents. For information about ports used by remote agents, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

To add and configure a remote agent:

-
- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration section opens.
- Step 2** Perform one of the following steps, based on your use of NDGs:
- If you are using NDGs, click the name of the NDG to which you want to assign the remote agent. Then, in the NDG Remote Agents table, click **Add Entry**.
 - If you are not using NDGs, click **Add Entry** in the Remote Agents table.
- The Add Remote Agent page appears.
- Step 3** In the **Remote Agent Name** box, type a name for the remote agent (up to 32 characters).
- Step 4** In the **Remote Agent IP Address** box, type the IP address of the computer that runs the remote agent.
- Step 5** In the **Port** box, type the number of the TCP port on which the remote agent listens for communication from ACS (up to 6 digits). The default TCP port is 2004.



Note If this port number does not match the port on which the remote agent is configured to listen, ACS cannot communicate with the remote agent. For information about configuring the port number on which the remote agent listens, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

- Step 6** From the **Network Device Group** list, select the NDG to which this remote agent belongs.



Note The Network Device Group list appears only if NDGs are enabled. To enable NDGs, click **Interface Configuration > Advanced Options**, and then click **Network Device Groups**.

- Step 7** To save your changes and immediately apply them, click **Submit + Apply**.



Tip To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration > Service Control**, and then click **Restart**.



Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. The Max Sessions counter is reset to 0.

Editing a Remote Agent Configuration

Use this procedure to edit the settings for a remote agent that you have previously configured.

**Note**

You cannot edit the name of a remote agent. If you want to use a different name for a remote agent, delete the remote agent configuration, create a remote agent configuration by using the new name, and change remote logging and Windows authentication configurations that use the remote agent.

Before You Begin

For descriptions of the options available while editing a remote agent configuration, see [Remote Agent Configuration Options, page 3-19](#).

**Note**

For ACS to communicate with a remote agent, you must ensure that gateway devices between a remote agent and ACS permit communication over the TCP ports used by remote agents. For information about ports used by remote agents, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

To edit a remote agent configuration:

- Step 1** In the navigation bar, click **Network Configuration**.
- The Network Configuration section opens.
- Step 2** Perform one of the following steps, based on your use of NDGs:
- If you are using NDGs, click the name of the NDG to which the remote agent belongs. Then, in the NDG Remote Agents table, click the name of the remote agent configuration you want to edit.
 - If you are not using NDGs, in the **Remote Agents** table, click the name of the remote agent that you want to edit.

The Remote Agent Setup for the *agent* page appears.

- Step 3** Enter or select new settings for one or more of the following options:
- Remote Agent IP Address
 - Port
 - Network Device Group (displayed if enabled in Advanced Options in the interface configuration)

**Note**

If the ACS into which you are currently logged does not provide configuration data for the remote agent, none of the options can be edited. You can access the web interface for the ACS that does provide configuration data to the remote agent by clicking the ACS name listed as the Configuration Provider.

- Step 4** To save your changes and apply them immediately, click **Submit + Apply**.

**Tip**

To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, click **System Configuration > Service Control**, and then click **Restart**.

**Note**


Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. The Max Sessions counter is reset to 0.

Deleting a Remote Agent Configuration

**Note**

You cannot delete a remote agent that you have configured to use for remote logging or Windows authentication.

To delete a remote agent configuration:

- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration section opens.
- Step 2** Perform one of the following steps, based on your use of NDGs:
- If you are using NDGs, click the name of the NDG to which the remote agent belongs. Then, in the NDG Remote Agents table, click the name of the remote agent configuration you want to delete.
 - If you are not using NDGs, in the Remote Agents table, click the name of the remote agent configuration that you want to delete.
- The Remote Agent Setup for the *agent* page appears.
- Step 3** To delete the remote agent and have the deletion take effect immediately, click **Delete + Apply**.
-  **Note** Restarting services clears the Logged-in User report and temporarily interrupts all ACS services. As an alternative to restarting when you delete a remote agent, in the preceding step you can click **Delete**. However, when you do this, the change does not take effect until you restart services, which you can do by clicking **System Configuration > Service Control > Restart**.
- A confirmation dialog box appears.
- Step 4** Click **OK**.
ACS restarts its services and the remote agent configuration is deleted.

Configuring Network Device Groups

Network Device Grouping is an advanced feature that you use to view and administer a collection of network devices as a single logical group. To simplify administration, you can assign each group a name that can be used to refer to all devices within that group. This action creates two levels of network devices within ACS—single discrete devices such as an individual router or network-access server, and an NDG; that is, a collection of routers or AAA servers.

**Caution**

To see the Network Device Groups table in the web interface, you must check the Network Device Groups option on the Advanced Options page of the Interface Configuration section. Unlike in other areas of Interface Configuration, it is possible to remove from sight an active NDG if you uncheck the Network Device Groups option. Therefore, if you choose to configure NDGs, ensure that you leave the Network Device Groups option selected on the Advanced Option page.

This section contains:

- [Adding a Network Device Group, page 3-24](#)
- [Assigning an Unassigned AAA Client or AAA Server to an NDG, page 3-25](#)
- [Reassigning AAA Clients or AAA Servers to an NDG, page 3-26](#)
- [Editing a Network Device Group, page 3-26](#)
- [Deleting a Network Device Group, page 3-27](#)

Adding a Network Device Group

You can assign users or groups of users to NDGs. For more information, see:

- [Setting TACACS+ Enable Password Options for a User, page 6-23](#)
- [Setting Enable Privilege Options for a User Group, page 5-13](#)

To add an NDG:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Under the Network Device Groups table, click **Add Entry**.

**Tip**

If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then, choose **Network Device Groups**.

Step 3 In the Network Device Group Name box, type the name of the new NDG.

**Tip**

The maximum name length is 24 characters. Quotation marks (") and commas (,) are not allowed. Spaces are allowed.

Step 4 In the **Shared Secret** box, enter a key for the Network Device Group. The maximum length is 64 characters.

Each device that is assigned to the Network Device Group will use the shared key that you enter here. The key that was assigned to the device when it was added to the system is ignored. If the key entry is null, the AAA client key is used. See [AAA Client Configuration Options, page 3-8](#). This feature simplifies key management for devices.

Step 5 In the **RADIUS Key Wrap** section, enter the shared secret keys for RADIUS Key Wrap in PEAP, EAP-FAST, and EAP-TLS authentications.

Each key must be unique, and must also be distinct from the RADIUS shared key. These shared keys are configurable for each AAA Client, as well as for each NDG. The NDG key configuration overrides the AAA Client configuration. If the key entry is null, the AAA client key is used. See [AAA Client Configuration Options, page 3-8](#).

- **Key Encryption Key (KEK)**—This is used for encryption of the Pairwise Master Key (PMK). In ASCII mode, enter a key length of exactly 16 characters; in hexadecimal mode, enter a key length of 32 characters.
- **Message Authentication Code Key (MACK)**—This is used for the keyed hashed message authentication code (HMAC) calculation over the RADIUS message. In ASCII mode, enter a key length of exactly 20 characters; in hexadecimal mode, enter a key length of 40 characters.



Note If you leave a key field empty when key wrap is enabled, the key will contain only zeros.

- **Key Input Format**—Select whether to enter the keys as ASCII or hexadecimal strings (the default is ASCII).



Note You must enable the Key Wrap feature in the NAP Authentication Settings page to implement these shared keys in PEAP, EAP-FAST, and EAP-TLS authentication.



Note Click **Submit**.

The Network Device Groups table displays the new NDG.

Step 6 To populate the newly established NDG with AAA clients or AAA servers, perform one or more of the following procedures, as applicable:

- [Adding AAA Clients, page 3-12](#)
- [Adding AAA Servers, page 3-17](#)
- [Assigning an Unassigned AAA Client or AAA Server to an NDG, page 3-25](#)
- [Reassigning AAA Clients or AAA Servers to an NDG, page 3-26](#)

Assigning an Unassigned AAA Client or AAA Server to an NDG

You use this procedure to assign an unassigned AAA client or AAA server to an NDG. Before you begin this procedure, you should have already configured the client or server and it should appear in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

To assign a network device to an NDG:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Network Device Groups table, click **Not Assigned**.

**Tip**

If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

- Step 3** Click the name of the network device that you want to assign to an NDG.
- Step 4** From the Network Device Groups list, select the NDG to which you want to assign the AAA client or AAA server.
- Step 5** Click **Submit**.
- The client or server is assigned to an NDG.

Reassigning AAA Clients or AAA Servers to an NDG

To reassign AAA clients or AAA servers to a new NDG:

- Step 1** In the navigation bar, click **Network Configuration**.
- The Network Configuration page opens.
- Step 2** In the Network Device Groups table, click the name of the current group of the network device.
- Step 3** In the AAA Clients table or AAA Servers table, as applicable, click the name of the client or server that you want to assign to a new NDG.
- Step 4** From the Network Device Group list, select the NDG to which you want to reassign the network device.
- Step 5** Click **Submit**.
- The network device is assigned to the NDG you selected.

Editing a Network Device Group

You can rename an NDG, change the shared secret, and the key wrap configuration.

**Caution**

When renaming an NDG, ensure that there are no NARs or other shared profile components (SPCs) that invoke the original NDG name. ACS performs no automatic checking to determine whether the original NDG is still invoked. If a user's authentication request incorporates an SPC that invokes a nonexistent (or renamed) NDG, the attempt will fail and the user will be rejected.

To edit an NDG:

- Step 1** In the navigation bar, click **Network Configuration**.
- The Network Configuration page opens.
- Step 2** In the Network Device Groups table, click the NDG that you want to edit.

**Tip**

If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Network Device Groups** check box.

- Step 3** At the bottom of the page, click **Edit Properties**.
- Step 4** Change the network device group properties as required. For more information about these properties, see [Adding a Network Device Group, page 3-24](#).
- Step 5** Click **Submit**.
- The NDG properties are changed.

Deleting a Network Device Group

When you delete an NDG, all AAA clients and AAA servers that belong to the deleted group appear in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

**Tip**

It might be useful to empty an NDG of AAA clients and AAA servers before you delete it. You can do this manually by performing the procedure [Reassigning AAA Clients or AAA Servers to an NDG, page 3-26](#); or, in cases where you have a large number of devices to reassign, use the RDBMS Synchronization feature.

**Caution**

When deleting an NDG, ensure that there are no NARs or other SPCs that invoke the original NDG. ACS performs no automatic checking to determine whether the original NDG is still invoked. If a user authentication request incorporates an SPC that invokes a nonexistent (or renamed) NDG, the attempt will fail and the user will be rejected.

To delete an NDG:

- Step 1** In the navigation bar, click **Network Configuration**.
- The Network Configuration page opens.
- Step 2** In the Network Device Groups table, click the NDG that you want to delete.

**Tip**

If the Network Device Groups table does not appear, choose **Interface Configuration > Advanced Options**. Then check the **Network Device Groups** check box.

- Step 3** At the bottom of the page, click **Delete Group**.
- A confirmation dialog box appears.
- Step 4** Click **OK**.
- The NDG is deleted and its name is removed from the Network Device Groups table. Any AAA clients and AAA servers that were in the NDG are now in the Not Assigned AAA Clients or Not Assigned AAA Servers table.

Configuring Proxy Distribution Tables

This section describes the Proxy Distribution Table.

This section contains:

- [About the Proxy Distribution Table, page 3-28](#)
- [Adding a New Proxy Distribution Table Entry, page 3-28](#)
- [Sorting the Character String Match Order of Distribution Entries, page 3-29](#)
- [Editing a Proxy Distribution Table Entry, page 3-30](#)
- [Deleting a Proxy Distribution Table Entry, page 3-30](#)

About the Proxy Distribution Table

If you enabled the Distributed Systems Settings, when you click Network Configuration, you will see the Proxy Distribution Table.



Tip

To enable Distributed Systems Settings in the ACS, choose **Interface Configuration > Advanced Options**. Then, check the **Distributed System Settings** check box.

The Proxy Distribution Table includes entries that show the character strings on which to proxy, the AAA servers to proxy to, whether to strip the character string, and where to send the accounting information (Local/Remote, Remote, or Local). For more information about the proxy feature, see [Proxy in Distributed Systems, page 3-3](#).

The entries that you define and place in the Proxy Distribution Table are treated one at a time for each authentication request that ACS receives from the AAA client. The authentication request is defined in the Proxy Distribution Table according to the forwarding destination. If a match to an entry in the Proxy Distribution Table that contains proxy information is found, ACS forwards the request to the appropriate AAA server.

The Character String column in the Proxy Distribution Table always contains an entry of (Default). The (Default) entry matches authentication requests that are received by the local ACS that do not match any other defined character strings. While you cannot change the character string definition for the (Default) entry, you can change the distribution of authentication requests matching the (Default) entry. At installation, the AAA server associated with the (Default) entry is the local ACS. You might sometimes find it easier to define strings that match authentication requests to be processed locally rather than defining strings that match authentication requests to be processed remotely. In such a case, associating the (Default) entry with a remote AAA server permits you to configure your Proxy Distribution Table with the more easily written entries.

Adding a New Proxy Distribution Table Entry

To create a Proxy Distribution Table entry:

- Step 1** In the navigation bar, click **Network Configuration**.
The Network Configuration page opens.
- Step 2** Under the Proxy Distribution Table, click **Add Entry**.

**Note**

If the Proxy Distribution Table does not appear, choose **Interface Configuration > Advanced Options**. Then, select the **Distributed System Settings** check box.

- Step 3** In the Character String box, type the string of characters, including the delimiter to forward on when users dial in to be authenticated. For example, *.uk*.

**Note**

Angle brackets (<>) cannot be used.

- Step 4** From the Position list, select **Prefix** if the character string that you typed appears at the beginning of the username or **Suffix** if the character string appears at the end of the username.
- Step 5** From the Strip list, select **Yes** to strip the character string from the username that you entered, or select **No** to leave it.
- Step 6** In the AAA Servers column, select the AAA server that you want to use for proxy. Click the --> (right arrow button) to move it to the Forward To column.

**Tip**

You can also select additional AAA servers to use for backup proxy if the prior servers fail. To set the order of AAA servers, in the Forward To column, click the name of the applicable server and click **Up** or **Down** to move it into the position that you want.

**Tip**

If the AAA server that you want to use is not listed, choose **Network Configuration > AAA Servers**. Then, choose **Add Entry** and complete the applicable information.

- Step 7** From the Send Accounting Information list, select one of the following areas to which to report accounting information:
- **Local**—Keep accounting packets on the local ACS.
 - **Remote**—Send accounting packets to the remote ACS.
 - **Local/Remote**—Keep accounting packets on the local ACS and send them to the remote ACS.

**Tip**

This information is especially important if you are using the Max Sessions feature to control the number of connections that a user is allowed. Max Sessions depends on accounting start and stop records, and where the accounting information is sent determines where the Max Sessions counter is tracked. The Failed Attempts log and the Logged in Users report are also affected by where the accounting records are sent. See [Remote Use of Accounting Packets, page 3-5](#) for an example.

- Step 8** When you finish, click **Submit** or **Submit + Apply**.

Sorting the Character String Match Order of Distribution Entries

You can use this procedure to set the priority by which ACS searches character string entries in the Proxy Distribution Table when users dial in.

To determine the order by which ACS searches entries in the Proxy Distribution Table:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 Below the Proxy Distribution Table, click **Sort Entries**.



Tip

Before you sort the entries, you must configure at least two unique Proxy Distribution Table entries in addition to the (Default) table entry.

Step 3 Select the character string entry to reorder, and then click **Up** or **Down** to move its position to reflect the search order that you want.

Step 4 When you finish sorting, click **Submit** or **Submit + Apply**.

Editing a Proxy Distribution Table Entry

To edit a Proxy Distribution Table entry:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Character String column of the Proxy Distribution Table, click the distribution entry that you want to edit.

The Edit Proxy Distribution Entry page appears.

Step 3 Edit the entry as necessary.



Tip

For information about the parameters that make up a distribution entry, see [Adding a New Proxy Distribution Table Entry, page 3-28](#).

Step 4 When you finish editing the entry, click **Submit** or **Submit + Apply**.

Deleting a Proxy Distribution Table Entry

To delete a Proxy Distribution Table entry:

Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the Character String column of the Proxy Distribution Table, click the distribution entry that you want to delete.

The Edit Proxy Distribution Entry page appears.

Step 3 Click **Delete**.

A confirmation dialog box appears.

Step 4 Click **OK**.

The distribution entry is deleted from the Proxy Distribution Table.



CHAPTER 4

Shared Profile Components

This chapter contains information about the features in the Shared Profile Components section of the web interface for the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

This chapter contains:

- [About Shared Profile Components, page 4-1](#)
- [Network Access Filters, page 4-2](#)
- [RADIUS Authorization Components, page 4-6](#)
- [Downloadable IP ACLs, page 4-13](#)
- [Network Access Restrictions, page 4-18](#)
- [Command Authorization Sets, page 4-25](#)

About Shared Profile Components

You use the Shared Profile Components section to develop and name reusable, shared sets of authorization components that may be applied to one or more users or groups of users, and referenced by name within their profiles. These include network-access filters (NAFs), RADIUS Authorization Components (RACs), downloadable IP access control lists (IP ACLs), Network Access Restrictions (NARs), and command-authorization sets.

The Shared Profile Components section addresses the scalability of selective authorization. Shared profile components can be configured and then applied to many users or groups. Without this ability, you could only accomplish flexible and comprehensive authorization explicitly configuring the authorization of each user group on each device. Creating and applying these named shared-profile components (downloadable IP ACLs, NAFs, RACs, NARs, and command-authorization sets) makes it unnecessary to repeatedly enter long lists of devices or commands when defining network-access parameters.

This section contains the following topic:

[802.1X Example Setup, page 4-1](#)

802.1X Example Setup

[Table 4-1](#) describes an example scenario to help you understand how SPCs are deployed. If, for example, you are deploying 802.1X and Network Admission Control (NAC), you might configure:

Table 4-1 802.1X Example SPC Scenario

Shared Profile Component	Description	Notes
Network Access Filters	NAFs are the most common way of defining which devices will be part of a given network service and, therefore, Network Access Profile (NAP).	<ul style="list-style-type: none"> If you have switches or routers being upgraded for NAC, you can use a NAF to distinguish between those devices that can and cannot do NAC. If you have Network Device Groups (NDGs) for groups of devices based on geography, NAFs allow you to aggregate the NDGs. In this case, you might want to set up a NAF for each NAP configured.
ACLs	NAC uses ACLs in order to manage clients that required limited access (for example, if there is no NAC-suppliant or to enforce an upgrade policy).	<ul style="list-style-type: none"> Create ACLs related to posture and NAC agentless hosts (NAH). Use ACLs to control access to servers running network applications (such as software for sales, human resource, or accounting) which can be mapped from the users group. For example, the HR group gets an HR ACL.
RACs	Use RACs to set up service-differentiated RADIUS authorization.	<ul style="list-style-type: none"> Set up RACs for each network service (VPN, WLAN, dial, and so on). For example, set different session-timeouts for VPN and WLAN. Use NAP templates to save time setting up 802.1X profiles. They require different provisioning and so require SRACs for each.
NARs	Use NARs to create additional conditions that must be met before a user can access the network. ACS applies these conditions by using information from attributes sent by authentication, authorization, and accounting (AAA) clients.	<ul style="list-style-type: none"> Create a CLI/DNIS NAR listing the MAC addresses of all the non-NAC devices (maybe a printer or legacy system) that are allowed to access the network. This method will protect your network. With NAC, use NARs for NAH scenarios with MAC and IP exceptions handling. Wildcarding the MAC and IP addresses is allowed.

Network Access Filters

This section describes NAFs and provides instructions for creating and managing them.

This section contains:

- [About Network Access Filters, page 4-2](#)
- [Adding a Network Access Filter, page 4-3](#)
- [Editing a Network Access Filter, page 4-5](#)
- [Deleting a Network Access Filter, page 4-6](#)

About Network Access Filters

A NAF is a named group of any combination of one or more of the following network elements:

- IP addresses
- AAA clients (network devices)
- Network device groups (NDGs)

Using a NAF to specify a downloadable IP ACL or NAR—based on the AAA clients by which the user may access the network—saves you the effort of listing each AAA client explicitly. NAFs are the most common way of defining which devices will be part of a given network service and, therefore, Network Access Profile (NAP). NAFs exhibit the following characteristics:

- **NAFs in downloadable IP ACLs**—You can associate a NAF with specific ACL contents. A downloadable IP ACL comprises one or more ACL contents (sets of ACL definitions) that are associated with a single NAF or, by default, “All-AAA-Clients”. This pairing of ACL content with a NAF permits ACS to determine which ACL content is downloaded according to the IP address of the AAA client making the access request. For more information on using NAFs in downloadable IP ACLs, see [About Downloadable IP ACLs, page 4-13](#).
- **NAFs in shared Network Access Restrictions**—An essential part of specifying a shared NAR is listing the AAA clients from which user access is permitted or denied. Rather than list every AAA client that makes up a shared NAR, you can simply list one or more NAFs instead of, or in combination with, individual AAA clients. For more information on using NAFs in shared NARs, see [About Network Access Restrictions, page 4-18](#).



Tip

Shared NARs can contain NDGs, or NAFs, or both. NAFs can contain one or more NDGs.

You can add a NAF that contains any combination of NDG, network devices (AAA clients), or IP addresses. For these network devices or NDGs to be selectable you must have previously configured them in ACS.

The network elements that a NAF comprises can be arranged in any order. For best performance, place the elements most commonly encountered at the top of the Selected Items list. For example, in a NAF where the majority of users gain network access through the NDG accounting, but you also grant access to a single technical support AAA client with the IP address 205.205.111.222, you would list the NDG first (higher) in the list of network elements to prevent all NAF members from having to be examined against the specified IP address.

Adding a Network Access Filter

To add a NAF:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Filtering**.

The Network Access Filtering table page appears.



Tip

If Network Access Filtering does not appear as a selection on the Shared Profile Components page, you must enable it on the Advanced Options page of the Interface Configuration section.

Step 3 Click **Add**.

The Network Access Filtering edit page appears.

Step 4 In the **Name** box, type the name of the new network-access filter.



Note The name of a NAF can contain up to 31 characters. Spaces are not allowed. Names cannot contain: left bracket ([), right bracket (]), comma(,), slash (/), dash (–), hyphen (-), quotes (“), apostrophe (’), right angle bracket (>), left angle bracket (<).

Step 5 In the **Description** box, type a description of the new network-access filter. The description can be up to 1,000 characters.

Step 6 Add network elements to the NAF definition as applicable:

- a. To include an NDG in the NAF definition, from the **Network Device Groups** box, select the NDG; then click -> (right arrow button) to move it to the **Selected Items** box.
- b. To include a AAA client in the NAF definition, from the **Network Device Groups** box, select the applicable NDG and then, from the **Network Devices** box, select the AAA client you want to include. Finally, click --> (right arrow button) to move it to the **Selected Items** box.



Tip If you are using NDGs, the AAA clients appear in the Network Devices box only when you have selected the NDG to which they belong. Otherwise, if you are not using NDGs, you can select the AAA client from the **Network Devices** box with no prior NDG selection.

- c. To include an IP address in the NAF definition, type the IP address in the **IP Address** box. Click --> (right arrow button) to move it to the **Selected Items** box.



Note You can use the asterisk (*), which is the wildcard character, to designate a range within an IP address.

Step 7 Ensure that the order of the items is correct. To change the order of items, in the **Selected Items** box, click the name of an item, and then click **Up** or **Down** to move it to the position that you want.



Tip You can also remove an item from the Selected Items box by selecting the item and then clicking <-- (left arrow button) to remove it from the list.

Step 8 To save your NAF and apply it immediately, choose **Submit + Apply**.



Tip To save your NAF and apply it later, choose **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.



Note Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to zero (0).

The Network Access Filtering table page appears, and lists the name and description of the new NAF.

Editing a Network Access Filter

To edit a NAF:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Network Access Filtering**.
The Network Access Filtering table appears.
- Step 3** In the Name column, click the NAF that you want to edit.
The Network Access Filter page appears with information visible for the selected NAF.
- Step 4** Edit the Name or Description of the NAF; type and delete information, as applicable. The description can be up to 1,000 characters.



Caution

If you change the name of a NAF, you invalidate all existing references to that NAF; this action might affect the access of users or groups that are associated with NARs or downloadable ACLs that use that NAF.

-
- Step 5** To add a NDG to the NAF definition, from the Network Device Groups box, select the NDG that you want to add. Click --> (right arrow button) to move it to the **Selected Items** box.
- Step 6** To add a AAA client in the NAF definition, from the **Network Device Groups** box select the applicable NDG and then, from the Network Devices box, select the AAA client that you want to add. Click --> (right arrow button) to move it to the Selected Items box.



Tip

If you are not using NDGs, you begin by selecting the AAA client from the **Network Devices** box.

-
- Step 7** To add an IP address to the NAF definition, in the **IP Address** box, type the IP address that you want to add. Click --> (right arrow button) to move it to the **Selected Items** box.
- Step 8** To edit an IP address, choose it in the **Selected Items** box and then click <-- (left arrow button) to move it to the IP address box. Type the changes to the IP address and then click --> (right arrow button) to move it back to the **Selected Items** box.
- Step 9** To remove an element from the **Selected Items** box, choose the item and then click <-- (left arrow button) to remove it.
- Step 10** To change the order of items, in the **Selected Items** box, click the name of an item, and then click **Up** or **Down** to move it into the position that you want. For more information on arranging the order of NAFs see [About Network Access Filters, page 4-2](#).
- Step 11** To save the changes to your NAF and apply them immediately, click **Submit + Apply**.



Tip

To save your NAF and apply it later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

**Note**

Restarting the service clears the Logged-in User report and temporarily interrupts all ACS services. This action affects the Max Sessions counter and resets it to zero (0).

ACS reenters the NAF with the new information, which takes effect immediately.

Deleting a Network Access Filter

Before You Begin

Before you delete a NAF you should remove its association with any NAR, downloadable IP ACL, or network access profile that uses it. Otherwise, any NAR, downloadable IP ACL, or network access profile that references the deleted NAF will be misconfigured and will produce an error.

To delete a NAF:

-
- Step 1** In the navigation bar, click **Network Access Filtering**.
The Network Access Filtering table page appears.
- Step 2** Click the name of the NAF that you want to delete.
The Network Access Filtering edit page appears.
- Step 3** Click **Delete** and then click **OK** to confirm.
The Network Access Filtering table page appears with the name and description of the NAF removed from the table.
-

RADIUS Authorization Components

This section describes RADIUS Authorization Components (RACs) and provides instructions for configuring and managing them.

The following topics are described:

- [About RADIUS Authorization Components, page 4-7](#)
- [Before You Begin Using RADIUS Authorization Components, page 4-8](#)
- [Adding RADIUS Authorization Components, page 4-10](#)
- [Cloning a RADIUS Authorization Component, page 4-10](#)
- [Editing a RADIUS Authorization Component, page 4-11](#)
- [Deleting a RADIUS Authorization Component, page 4-11](#)

About RADIUS Authorization Components

Shared Radius Authorization Components (RACs) contain groups of RADIUS attributes that you can dynamically assign to user sessions based on a policy. Using the Network Access Profile configuration, you can map a policy type with set conditions, such as Network Device Groups and posture, to a shared RAC.

Understanding RACs and NAPs

ACS RACs contain a set of attributes (also referred to as a network-access profile) that can be specific to a single network device, or to several network devices. The authorization policy maps from various groups and postures to a set of RACs and ACLs. For more information on setting up network-access profiles, see [Chapter 14, “Network Access Profiles.”](#)

ACS user groups contain attributes that are related to the type of user (for example, administrators, contractors, and so on) and do not cater to the same groups of users that require authorization for different network services (WLAN and VPN, for example).

RACs hold attributes that can be specific to a single network profile by using authorization policies. RACs also can be used by several different network profiles. You can map from various groups and postures to a set of RACs and ACLs. Use RACs with NAPs when you require service-differentiated RADIUS authorization. For example, when you must set the session-timeout to be several days for VPN and several hours for WLAN.

You can use group attributes so that you can apply service-independent attributes to all users of the group without having to duplicate each RAC for each profile. You can configure RADIUS attributes in three places:

- RAC
- Group level
- User level

You can use the authorization policy to indicate if you want to include attributes from the group, the user, or both.

If your network strategy demands policy-based profiles, we recommend that you use RACs instead of groups. You must define appropriate access services and policies:

- Plan what user group and posture should get which level of authorization.
- Identify all similar authorization cases and create RACs for them.
- Remove any legacy attributes from the user groups if necessary.
- Define appropriate network-access policies and define rules.

You can create a base template authorization at group level and then supply the profile-specific attributes by using RACs. For example, setting a different Session-Timeout for VPN and WLAN.

Vendors



Note

RADIUS security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco IOS/PIX 6.0) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco IOS/PIX 6.0) in the Authenticate Using list.

The RADIUS vendor-specific attribute (VSA) sets that ACS supports are:

- **Cisco Aironet**—VSAs for Cisco Aironet Access Point products. *Not* supported for shared RAC; use IETF session timeout instead.
- **Cisco Airespace**—VSAs for Cisco Airespace wireless LAN devices.
- **Cisco BBSM**—VSAs for Cisco Building Broadband Service Manager (BBSM) products.
- **Cisco IOS/PIX 6.0**—VSAs for Cisco IOS products and Cisco PIX firewalls earlier than 6.0 releases.
- **Cisco VPN 3000/ASA/PIX 7.x+**—VSAs for Cisco VPN 3000-series Concentrators, ASA devices, and PIX devices later than 7.x releases.
- **Cisco VPN 5000**—VSAs for Cisco VPN 5000-series Concentrators.
- **Ascend**—VSAs for Ascend products.
- **Microsoft**—VSAs for Microsoft Point-to-Point Encryption and Point-to-Point Compression.
- **Nortel**—VSAs for Nortel products.
- **Juniper**—VSAs for Juniper products.
- **3COMUSR**—VSAs for 3COMUSR products.

Attribute Types

The vendor-specific attributes are not defined. You can find definitions in the vendor's software documentation. For Cisco vendor-specific attributes, see [Appendix B, "RADIUS Attributes."](#)

ACS for Windows

You can import vendor-specific attributes by using the **CSUtil** command (see [Appendix C, "CSUtil Database Utility"](#)) or RDBMS Synchronization (see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#)).

ACS SE

You can import vendor-specific attributes by using RDBMS Synchronization, see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#).

Before You Begin Using RADIUS Authorization Components

For you to use the Shared Profile Components' RACs, you must ensure that you have properly set up ACS. Review this checklist before you create shared profile components:



Tip

Use the Network Access Profile templates to save time. NAP templates automatically create a set of shared profile components if none are configured. For details, see [Using Profile Templates, page 14-7](#).

1. Add devices to ACS. For ACS to interact with AAA clients and servers you must add their network information. For instructions on how to add devices by using Network Configuration, see [Adding AAA Clients, page 3-12](#).
2. Enable the attributes (VSAs) that you want to use. Disable those attributes that you do not want to use. If attributes are not enabled, they will not appear on the RADIUS Authorization Components page, the Interface Configuration set up pages. For details on enabling VSAs, see [Chapter 2, "Using the Web Interface."](#)

3. Map out your network access profile design. You must identify the network services that require provisioning. You will probably identify at least one shared RADIUS authorization component (SRAC) for each profile. For details on linking a SRAC to a profile, see [Classification of Access Requests, page 14-2](#) or [Using Profile Templates, page 14-7](#).
4. For each profile that you are creating, identify how you plan to classify network-access requests and any exception cases (for example, special users or groups, bad posture status, and so on) and create SRACs for each. See [About RADIUS Authorization Components, page 4-7](#).
5. Decide whether any attributes are user or group-specific (rather than network service-specific). If you must assign attributes to a user or group, regardless of network service, add these to the user or group record and enable attribute merging in the network access profile. For details on attribute merging, see [Merging Attributes, page 14-35](#).

For specific steps on enabling RADIUS Authorization Components, see [Enabling Use of RAC, page 4-9](#).

Enabling Use of RAC

To enable use of RAC:

-
- Step 1** Before setting RADIUS Authorization Components, add your devices by using Network Configuration and configure them to authenticate by using the correct security protocol (such as RADIUS Cisco VPN 3000/ASA/PIX 7.x+).

If your attribute does not appear in the Authenticate Using list, check the Interface Configuration or your User Setup/Group Setup parameters.

- Step 2** In the navigation bar, click **Interface Configuration** and select **RADIUS (IETF)**.



Note RADIUS security protocols only appear as options on this page if you have configured a AAA client to support the security protocol. For example, RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) only appears once you have configured a AAA client in Network Configuration that specifies RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) in the Authenticate Using list.

- Step 3** Select the desired RADIUS attributes and click **Submit**.
- Step 4** Repeat [Step 2](#) and [Step 3](#) for each RADIUS security protocol in your network configuration.
- Step 5** Ensure that Tunneling RADIUS attributes are selected in Advanced Options.
- Choose **Interface Configuration > RADIUS (IETF)**.
 - Choose the Tunnel attributes.
 - Click **Submit**.
- Step 6** In the navigation bar, click **Shared Profile Components** and select **RADIUS Authorization Components**.

For details on adding RACs, see [Adding RADIUS Authorization Components, page 4-10](#). For details on changing RACs, see [Editing a RADIUS Authorization Component, page 4-11](#). For details on how to add RACs to network access profiles, see [Configuring an Authorization Rule, page 14-36](#).

Adding RADIUS Authorization Components

Before You Begin

You should have already configured any RADIUS options that you plan to use on ACS. For details on what to configure, see [Vendors, page 4-7](#).

To add a RAC:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **RADIUS Authorization Components**.
The RADIUS Authorization Components Table Page appears.
- Step 3** Click **Add** to create a new RADIUS Authorization Component.
The Edit RADIUS Authorization Component Page appears.
- Step 4** To add a new attribute, select the correct vendor attribute by using the drop-down list and click the **Add** button.
The RAC Attribute Add/Edit Page appears.



Note The vendors that are available for selection are those that have devices defined in the Network Configuration and that have attributes configured for display (at the group or user level) under Interface Configuration.

- Step 5** Select the attribute value and click **Submit**.
-

Cloning a RADIUS Authorization Component

To make a copy of an existing RAC by using the clone feature:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **RADIUS Authorization Components**.
The RADIUS Authorization Components Table Page appears.
- Step 3** Select the RAC name of the component that you want to clone.
The Edit RADIUS Authorization Component Page appears.
- Step 4** To clone an existing RAC with all of its attributes, click **Clone**.
A clone named Copy of RACname is created in the Edit RADIUS Authorization Component page.
- Step 5** Click **Submit to save the new RAC**.
-

Editing a RADIUS Authorization Component

To edit an existing RAC:

-
- | | |
|---------------|---|
| Step 1 | In the navigation bar, click Shared Profile Components .
The Shared Profile Components page appears. |
| Step 2 | Click RADIUS Authorization Components .
The RADIUS Authorization Components Table Page appears. |
| Step 3 | Select the RAC name of the component that you want to edit.
The Edit RADIUS Authorization Component Page appears. |
| Step 4 | To add a new attribute, select the correct vendor attribute by using the drop-down list and click the adjacent Add button. |
| Step 5 | To alter an existing attribute, select the value in Assigned Attributes.
The RAC Attribute Add/Edit Page appears.
To delete an attribute and its value, click Delete . |
| Step 6 | Select the attribute value and click Submit . |
-

Deleting a RADIUS Authorization Component

Before You Begin

You should remove the association of an RAC with any network access profile before deleting the RAC.

To delete an RAC:

-
- | | |
|---------------|--|
| Step 1 | In the navigation bar, click Shared Profile Components .
The Shared Profile Components page appears. |
| Step 2 | Click RADIUS Authorization Components .
The RADIUS Authorization Components Table Page appears. |
| Step 3 | Select the RAC name of the component that you want to delete.
The Edit RADIUS Authorization Component Page appears. |
| Step 4 | Click Delete to remove the RADIUS Authorization Component. |
| Step 5 | Click OK to remove the RADIUS Authorization Component.
The current configuration changes. A dialog box appears and asks that you restart ACS by choosing System Configuration > Service Control to adopt the new settings. |
-

RADIUS Authorization Components Table Page

You use this page to list defined RACs, display defined RAC configurations, or add a new RAC name. [Table 4-2](#) describes the fields on this page.

Table 4-2 RAC Display Fields

Field	Description
Name	Click to display the configuration for the RAC. Opens the Edit RADIUS Authorization Component Page.
Description	Displays the RAC description. The description can be up to 1,000 characters.
Add	Click to add a new RAC. Opens the Edit RADIUS Authorization Component Page.

Edit RADIUS Authorization Component Page

You use this page to configure the RAC. [Table 4-3](#) describes the RAC configuration fields.

Table 4-3 RAC Configuration Fields

Field	Description
Name	Enter the name that you want to assign to the RADIUS Authorization Components.
Description	Enter a description for the RAC. The description can be up to 1,000 characters.
Add New Attribute	Use the Vendor and Service Type fields to add new attribute values. Vendors available for selection are those that have devices defined in the Network Configuration and that have attributes configured for display (at group level) under Interface Configuration. For details on setting up devices, see Chapter 3, “Network Configuration.” For details on setting up the interface, see Chapter 2, “Using the Web Interface.” Select the vendor attribute from the drop-down list and click Add . This action opens the RAC Attribute Add/Edit Page .
Assigned Attributes	Use this table to view, edit, and select the list of RADIUS attributes assigned to the Authorization Component. To edit or delete an already assigned attribute, click on the attribute value. Opens the RAC Attribute Add/Edit Page .
Vendor Attribute Value	Appears if assigned attributes are present. Click on the value to edit or delete. Opens the RAC Attribute Add/Edit Page .
Submit	Click to submit the RAC configuration to ACS.
Delete	Appears if assigned attributes are present. Click to delete the RAC. To delete a single attribute, go to the RAC Attribute Add/Edit Page .

RAC Attribute Add/Edit Page

You use this page to add or edit RAC attributes. [Table 4-4](#) describes the fields on this page.

Table 4-4 Add or Edit RAC Attributes Fields

Field	Description
RAC	Name assigned to the RADIUS Authorization Component.
Vendor	Name of the organization the vendor-specific attributes.
Clone	Copy an existing RAC attributes into a new RAC named Copy of RAC name.
Attribute	Attribute defined for RAC.
Type	Attribute type of integer or text.
Value	Drop-down box or text value settings.
Submit	Click to submit the RAC configuration to ACS.
Delete	Click to delete this single attribute.

Downloadable IP ACLs

This section describes downloadable ACLs and provides detailed instructions for configuring and managing them.

This section contains:

- [About Downloadable IP ACLs, page 4-13](#)
- [Adding a Downloadable IP ACL, page 4-15](#)
- [Editing a Downloadable IP ACL, page 4-16](#)
- [Deleting a Downloadable IP ACL, page 4-17](#)

About Downloadable IP ACLs

You can use downloadable IP ACLs to create sets of ACL definitions that you can apply to many users or user groups. These sets of ACL definitions are called ACL contents. Also, by incorporating NAFs, you can control the ACL contents that are sent to the AAA client from which a user is seeking access. That is, a downloadable IP ACL comprises one or more ACL content definitions, each of which is associated with a NAF or (by default) associated to all AAA clients. (The NAF controls the applicability of specified ACL contents according to the AAA client's IP address. For more information on NAFs and how they regulate downloadable IP ACLs, see [About Network Access Filters, page 4-2](#)).

Downloadable IP ACLs operate this way:

1. When ACS grants a user access to the network, ACS determines whether a downloadable IP ACL is assigned to that user or the user's group.
2. If ACS locates a downloadable IP ACL that is assigned to the user or the user's group, it determines whether an ACL content entry is associated with the AAA client that sent the RADIUS authentication request.
3. ACS sends, as part of the user session, RADIUS access-accept packet an attribute specifying the named ACL and the version of the named ACL.

4. If the AAA client responds that it does not have the current version of the ACL in its cache (that is, the ACL is new or has changed), ACS sends the ACL (new or updated) to the device.

Downloadable IP ACLs are an alternative to configuring ACLs in the RADIUS Cisco **cisco-av-pair** attribute [26/9/1] of each user or user group. You can create a downloadable IP ACL once, give it a name, and then assign the downloadable IP ACL to each applicable user or user group by referencing its name. This method is more efficient than configuring the RADIUS Cisco **cisco-av-pair** attribute for each user or user group.

**Note**

Downloadable ACLs are not meant to be used in per-user profiles of PPP/DDR clients.

Further, by employing NAFs, you can apply different ACL contents to the same user or group of users, according to the AAA client that they are using. No additional configuration of the AAA client is necessary after you have configured the AAA client to use downloadable IP ACLs from ACS. Downloadable ACLs are protected by the backup or replication regimen that you have established.

While entering the ACL definitions in the ACS web interface, do not use keyword and name entries; in all other respects, use standard ACL command syntax and semantics for the AAA client on which you intend to apply the downloadable IP ACL. The ACL definitions that you enter into ACS comprise one or more ACL commands. Each ACL command must be on a separate line.

You can add one or more named ACL contents to a downloadable IP ACL. By default each ACL content applies to all AAA clients; however, if you have defined NAFs, you can limit the applicability of each ACL content to the AAA clients that are listed in the NAF that you associate to it. That is, by employing NAFs, you can make each ACL content, within a single downloadable IP ACL, applicable to multiple different network devices or network device groups in accordance with your network security strategy. For more information on NAFs, see [About Network Access Filters, page 4-2](#).

Also, you can change the order of the ACL contents in a downloadable IP ACL. ACS examines ACL contents starting from the top of the table and downloads the *first* ACL content that it finds with a NAF that includes the AAA client that is being used. In setting the order, you should seek to ensure system efficiency by positioning the most widely applicable ACL contents higher on the list. You should realize that, if your NAFs include overlapping populations of AAA clients, you must proceed from the more specific to the more general. For example, ACS will download any ACL contents with the **All-AAA-Clients** NAF setting and not consider any that are lower on the list.

To use a downloadable IP ACL on a particular AAA client, the AAA client must:

- Use RADIUS for authentication.
- Support downloadable IP ACLs.

Examples of Cisco devices that support downloadable IP ACLs are:

- PIX Firewalls
- VPN 3000-series concentrators, ASA and PIX devices
- Cisco devices running IOS version 12.3(8)T or greater

[Example 4-1](#) shows the format that you should use to enter PIX Firewall ACLs in the ACL Definitions box.

Example 4-1

```
permit tcp any host 10.0.0.254
permit udp any host 10.0.0.254
permit icmp any host 10.0.0.254
permit tcp any host 10.0.0.253
```


[Example 4-2](#) shows the format that you should use to enter VPN 3000/ASA/PIX 7.x+ ACLs in the **ACL Definitions** box.

Example 4-2

```
permit ip 10.153.0.0 0.0.255.255 host 10.158.9.1
permit ip 10.154.0.0 0.0.255.255 10.158.10.0 0.0.0.255
permit 0 any host 10.159.1.22
deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log
permit TCP any host 10.160.0.1 eq 80 log
permit TCP any host 10.160.0.2 eq 23 log
permit TCP any host 10.160.0.3 range 20 30
permit 6 any host HOSTNAME1
permit UDP any host HOSTNAME2 neq 53
deny 17 any host HOSTNAME3 lt 137 log
deny 17 any host HOSTNAME4 gt 138
deny ICMP any 10.161.0.0 0.0.255.255 log
permit TCP any host HOSTNAME5 neq 80
```

For detailed ACL definition information, see the command reference section of your device configuration guide.

Adding a Downloadable IP ACL

Before You Begin

You should have already configured any NAFs that you intend to use in your downloadable IP ACL.

To add a downloadable IP ACL:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Downloadable IP ACLs**.



Tip

If Downloadable IP ACLs does not appear on the Shared Profile Components page, you must enable the User-Level Downloadable ACLs or Group-Level Downloadable ACLs option, or both, on the Advanced Options page of the Interface Configuration section.

Step 3 Click **Add**.

The Downloadable IP ACLs page appears.

Step 4 In the **Name** box, type the name of the new IP ACL.



Note

The name of an IP ACL may contain up to 27 characters. The name *must not* contain spaces nor any of the following characters: hyphen (-), left bracket ([), right bracket (]), slash (/), backslash (\), quotes ("), left angle bracket (<), right angle bracket (>), dash (-).

Step 5 In the **Description** box, type a description of the new IP ACL. The description can be up to 1,000 characters.

Step 6 To add an ACL content to the new IP ACL, click **Add**.

Step 7 In the **Name** box, type the name of the new ACL content.

**Note**

The name of an ACL content may contain up to 27 characters. The name *must not* contain spaces nor any of the following characters: hyphen (-), left bracket ([), right bracket (]), slash (/), backslash (\), quotes ("), left angle bracket (<), right angle bracket (>), dash (-).

Step 8 In the **ACL Definitions** box, type the new ACL definition.

**Tip**

In entering ACL definitions in the ACS web interface, you do not use keyword and name entries; rather, you begin with a **permit** or **deny** keyword. For examples of the proper format of the ACL definitions, see [Example 4-1 on page 4-14](#) and [Example 4-1 on page 4-14](#).

Step 9 To save the ACL content, click **Submit**.

The Downloadable IP ACLs page appears with the new ACL content listed by name in the ACL Contents column.

Step 10 To associate a NAF to the ACL content, select a NAF from the Network Access Filtering box to the right of the new ACL content. For information on adding a NAF see [Adding a Network Access Filter, page 4-3](#).

**Note**

If you do not assign a NAF, ACS associates the ACL content to all network devices, which is the default.

Step 11 Repeat [Step 3](#) through [Step 10](#) until you have completely specified the new IP ACL.

Step 12 To set the order of the ACL contents, click the radio button for an ACL definition, and then click **Up** or **Down** to reposition it in the list.

**Tip**

The order of ACL contents is significant. Working from top to bottom, ACS downloads only the *first* ACL definition that has an applicable NAF setting (including the **All-AAA-Clients** default setting if used). Typically your list of ACL contents will proceed from the one with the most specific (narrowest) NAF to the one with the most general (**All-AAA-Clients**) NAF.

Step 13 To save the IP ACL, click **Submit**.

ACS enters the new IP ACL, which takes effect immediately. For example, if the IP ACL is for use with PIX Firewalls, it is available to be sent to any PIX Firewall that is attempting authentication of a user who has that downloadable IP ACL assigned to his or her user or group profile. For information on assigning a downloadable IP ACL to user or a user group, see [Assigning a Downloadable IP ACL to a User, page 6-14](#), or [Assigning a Downloadable IP ACL to a Group, page 5-22](#).

Editing a Downloadable IP ACL

Before You Begin

You should have already configured any NAFs that you intend to use in your editing of the downloadable IP ACL.

To edit a downloadable IP ACL:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Downloadable IP ACLs**.
The Downloadable IP ACLs table appears.
- Step 3** In the **Name** column, click the IP ACL that you want to edit.
The Downloadable IP ACLs page appears and displays with information for the selected ACL.
- Step 4** Edit the Name or Description information, as applicable. The description can be up to 1,000 characters.
- Step 5** To edit ACL content, click on the ACL Contents entry that you want to change. For examples of the proper format of the ACL definitions, see [Example 4-1 on page 4-14](#) and [Example 4-1 on page 4-14](#).
The Downloadable IP ACL Content page appears.
- Step 6** Edit the Name or ACL Definitions, as applicable.



Tip Do not use keyword and name entries in the ACL Definitions box; instead, begin with a permit or deny keyword. For an example of the proper format of the ACL definitions, see [About Downloadable IP ACLs, page 4-13](#).

- Step 7** To save the edited ACL definition, click **Submit**.
- Step 8** To change the NAF that is associated with an ACL content, select a new NAF setting from the corresponding Network Access Filtering box. You can change as many of the NAF associations in a downloadable IP ACL as you want. For more information on NAFs, see [About Network Access Filters, page 4-2](#).
- Step 9** Repeat [Step 3](#) through [Step 8](#) until you are finished.
- Step 10** To change the order of the ACL contents, select the radio button for an ACL definition, and then click **Up** or **Down** to reposition it in the list.
- Step 11** To save the edited IP ACL, click **Submit**.
ACS saves the IP ACL with the new information, which takes effect immediately.
-

Deleting a Downloadable IP ACL

Before You Begin

You should remove the association of a IP ACL with any user, user group profile, or network access profile before deleting the IP ACL.

To delete an IP ACL:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
The Shared Profile Components page appears.
- Step 2** Click **Downloadable IP ACLs**.
- Step 3** Click the name of the downloadable IP ACL that you want to delete.

- The Downloadable IP ACLs page appears and displays information for the selected IP ACL.
- Step 4** At the bottom of the page, click **Delete**.
- A dialog box warns you that you are about to delete an IP ACL.
- Step 5** To confirm that you want to delete the IP ACL, click **OK**.
- The selected IP ACL is deleted.
-

Network Access Restrictions

This section describes network access restrictions (NARs), and provides detailed instructions for configuring and managing shared NARs.

This section contains:

- [About Network Access Restrictions, page 4-18](#)
- [Adding a Shared NAR, page 4-21](#)
- [Editing a Shared NAR, page 4-23](#)
- [Deleting a Shared NAR, page 4-24](#)

About Network Access Restrictions

A network access restriction (NAR) is a definition, which you make in ACS, of additional conditions that you must meet before a user can access the network. ACS applies these conditions by using information from attributes that your AAA clients sent. Although you can set up NARs in several ways, they all are based on matching attribute information that a AAA client sent. Therefore, you must understand the format and content of the attributes that your AAA clients sends if you want to employ effective NARs.

In setting up a NAR you can choose whether the filter operates positively or negatively. That is, in the NAR you specify whether to permit or deny network access, based on information sent from AAA clients when compared to the information stored in the NAR. However, if a NAR does not encounter sufficient information to operate, it defaults to denied access. [Table 4-5](#) shows these conditions.

Table 4-5 *NAR Permit or Deny Conditions*

	IP-Based	Non-IP Based	Insufficient Information
Permit	Access Granted	Access Denied	Access Denied
Deny	Access Denied	Access Granted	Access Denied

ACS supports two types of NAR filters:

- **IP-based filters**—IP-based NAR filters limit access based on the IP addresses of the end-user client and the AAA client. For more information on this type of NAR filter, see [About IP-Based NAR Filters, page 4-19](#).
- **Non-IP-based filters**—Non-IP-based NAR filters limit access based on simple string comparison of a value sent from the AAA client. The value may be the calling line identification (CLI) number, the Dialed Number Identification Service (DNIS) number, the MAC address, or other value

originating from the client. For this type of NAR to operate, the value in the NAR description must exactly match what is being sent from the client, including whatever format is used. For example, the telephone number (217) 555-4534 does not match 217-555-4534. For more information on this type of NAR filter, see [About Non-IP-based NAR Filters, page 4-20](#).

You can define a NAR for, and apply it to, a specific user or user group. For more information, see [Setting Network Access Restrictions for a User, page 6-8](#), or [Setting Network Access Restrictions for a User Group, page 5-6](#). However, in the Shared Profile Components section of ACS you can create and name a *shared* NAR without directly citing any user or user group. You give the shared NAR a name that can be referenced in other parts of the ACS web interface. Then, when you set up users or user groups, you can select none, one, or multiple shared restrictions to be applied. When you specify the application of multiple shared NARs to a user or user group, you choose one of two access criteria:

- All selected filters must permit
- Any one selected filter must permit

You must understand the order of precedence that is related to the different types of NARs. The order of NAR filtering is:

1. Shared NAR at the user level
2. Shared NAR at the group level
3. Nonshared NAR at the user level
4. Nonshared NAR at the group level

You should also understand that denial of access at *any* level takes precedence over settings at another level that do not deny access. This is the one exception in ACS to the rule that user-level settings override group-level settings. For example, a particular user might have no NAR restrictions at the user level that apply; but, if that user belongs to a group that is restricted by a shared or nonshared NAR, the user is denied access.

Shared NARs are kept in the ACS internal database. You can use the ACS backup and restore features to back up, and restore them. You can also replicate the shared NARs, along with other configurations, to secondary ACSs.

About IP-Based NAR Filters

For IP-based NAR filters, ACS uses the attributes in [Table 4-6](#), depending on the AAA protocol of the authentication request.

Table 4-6 **Attributes for IP-Based NAR Filters**

Protocol	Attributes
TACACS+	<p>The <code>rem_addr</code> field from the TACACS+ start packet body is used.</p> <p>Note When an authentication request is forwarded by proxy to an ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.</p>
RADIUS IETF	The <code>calling-station-id</code> (attribute 31) must be used.

**Note**

IP-based NAR filters work only if ACS receives the Radius Calling-Station-Id (31) attribute. The Calling-Station-Id (31) must contain a valid IP address. If it does not, it will fall over to DNIS rules.

AAA clients that do not provide sufficient IP address information (for example, some types of firewall) do not support full NAR functionality.

Table 4-7 describes additional attributes for **IP-based** restrictions, per protocol.

Table 4-7 *Attributes for IP-Based Restrictions*

Protocol	Attributes
TACACS+	<p>The NAR fields in ACS use the following values:</p> <ul style="list-style-type: none">• AAA client—The <code>NAS-IP-address</code> is taken from the source address in the socket between ACS and the TACACS+ client.• Port—The <code>port</code> field is taken from the TACACS+ start packet body.

About Non-IP-based NAR Filters

A non-IP-based NAR filter (that is, a DNIS/CLI-based NAR filter) is a list of permitted or denied calling or point of access locations that you can use in restricting a AAA client when you do not have an established IP-based connection. The non-IP-based NAR feature generally uses the CLI number and the Dialed Number Identification Service (DNIS) number.

However, by entering an IP address in place of the CLI, you can use the non-IP-based filter; even when the AAA client does not use a Cisco IOS release that supports CLI or DNIS. In another exception to entering a CLI, you can enter a MAC address to permit or deny access; for example, when you are using a Cisco Aironet AAA client. Likewise, you could enter the Cisco Aironet AP MAC address in place of the DNIS. The format of what you specify in the CLI box—CLI, IP address, or MAC address—must match the format of what you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

Table 4-6 shows the attributes for DNIS/CLI-based restrictions, per protocol.

Table 4-8 **Attributes for DNIS/CLI-Based Restrictions**

Protocol	Attributes
TACACS+	<p>The NAR fields can contain:</p> <ul style="list-style-type: none"> • AAA client—The <code>NAS-IP-address</code> is taken from the source address in the socket between ACS and the TACACS+ client. • Port—The <code>port</code> field in the TACACS+ start packet body is used. • CLI—The <code>rem-addr</code> field in the TACACS+ start packet body is used. • DNIS—The <code>rem-addr</code> field taken from the TACACS+ start packet body is used. In cases in which the <code>rem-addr</code> data begins with the slash (/) the DNIS field contains the <code>rem-addr</code> data without the slash (/). <p>Note When a proxy forwards an authentication request to an ACS, any NARs for TACACS+ requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.</p>
RADIUS	<p>The NAR fields can contain:</p> <ul style="list-style-type: none"> • AAA client—The <code>NAS-IP-address</code> (attribute 4) or, if <code>NAS-IP-address</code> does not exist, <code>NAS-identifier</code> (RADIUS attribute 32) is used. • Port—The <code>NAS-port</code> (attribute 5) or, if <code>NAS-port</code> does not exist, <code>NAS-port-ID</code> (attribute 87) is used. • CLI—The <code>calling-station-ID</code> (attribute 31) must contain a valid IP address. If the <code>Calling-Station-Id</code> (31) does not contain a valid IP address, it will fall over to DNIS rules. • DNIS—The <code>called-station-ID</code> (attribute 30) is used.

When specifying a NAR you can use an asterisk (*) as a wildcard for any value, or as part of any value to establish a range. All the values or conditions in a NAR description must be met for the NAR to restrict access; that is, the values contain a Boolean AND.

Adding a Shared NAR

You can create a shared NAR that contains many access restrictions. Although the ACS web interface does not enforce limits to the number of access restrictions in a shared NAR or to the length of each access restriction, you must adhere to the following limits:

- The combination of fields for each line item cannot exceed 1024 characters.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS-based NAR where the AAA client names are 10 characters, the port numbers are 5 characters, the CLI entries are 15 characters, and the DNIS entries are 20 characters, you can add 450 line items before reaching the 16 KB limit.

Before You Begin

Before defining a NAR, you should be certain ensure that you have established the elements you intend to use in that NAR; you must have specified all NAFs and NDGs, and defined all relevant AAA clients, before making them part of the NAR definition. For more information see [About Network Access Restrictions, page 4-18](#).

To add a shared NAR:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

Step 3 Click **Add**.

The Network Access Restriction page appears.

Step 4 In the **Name** box, type a name for the new shared NAR.



Note The name can contain up to 31 characters. Leading and trailing spaces are not allowed. Names cannot contain the following characters: left bracket ([), right bracket (]), comma (,), or slash (/).

Step 5 In the **Description** box, type a description of the new shared NAR. The description can be up to 1,000 characters.

Step 6 If you want to permit or deny access based on IP addressing:

- a. Check the **Define IP-based access descriptions** check box.
- b. To specify whether you are listing addresses that are permitted or denied, from the Table Defines list, select the applicable value.
- c. Select or type the applicable information in each of the following boxes:
 - **AAA Client**—Select **All AAA clients**, or the name of the NDG, or the NAF, or the individual AAA client, to which access is permitted or denied.
 - **Port**—Type the number of the port to which you want to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports on the selected AAA client.
 - **Src IP Address**—Type the IP address to filter on when performing access restrictions. You can use the asterisk (*) as a wildcard to specify all IP addresses.



Note The total number of characters in the AAA Client list, and the Port and Src IP Address boxes, must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

d. Click **Enter**.

The AAA client, port, and address information appear as a line item in the table.

e. To enter additional IP-based line items, repeat steps c and d.

Step 7 If you want to permit or deny access based on calling location or values other than IP addresses:

- a. Select the **Define CLI/DNIS based access restrictions** check box.
- b. To specify whether you are listing locations that are permitted or denied from the Table Defines list, select the applicable value.

- c. To specify the clients to which this NAR applies, select one of the following values from the AAA Client list:
- The name of the NDG
 - The name of the particular AAA client
 - All AAA clients



Tip Only NDGs that you have already configured are listed.

- d. To specify the information on which this NAR should filter, type values in the following boxes, as applicable:



Tip You can type an asterisk (*) as a wildcard to specify **all** as a value.

- **Port**—Type the number of the port on which to filter.
- **CLI**—Type the CLI number on which to filter. You can also use this box to restrict access based on values other than CLIs, such as an IP address or MAC address; for information, see [About Network Access Restrictions, page 4-18](#).
- **DNIS**—Type the number being dialed in to on which to filter.



Note The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

- e. Click **Enter**.

The information specifying the NAR line item appears in the table.

- f. To enter additional non-IP-based NAR line items, repeat steps c. through e.

Step 8 To save the shared NAR definition, click **Submit**.

ACS saves the shared NAR and lists it in the **Network Access Restrictions** table.

Editing a Shared NAR

To edit a shared NAR:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page appears.

Step 2 Click **Network Access Restrictions**.

The Network Access Restrictions table appears.

Step 3 In the **Name** column, click the shared NAR that you want to edit.

The Network Access Restriction page appears and displays information for the selected NAR.

Step 4 Edit the Name or Description of the NAR, as applicable. The description can be up to 1,000 characters.

Step 5 To edit a line item in the IP-based access-restrictions table:

- a. Double-click the line item that you want to edit.

Information for the line item is removed from the table and written to the boxes below the table.

- b. Edit the information, as necessary.



Note

The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and ACS cannot accurately apply it to users.

- c. Click **Enter**.

The edited information for this line item is written to the IP-based access-restrictions table.

Step 6 To remove a line item from the IP-based access-restrictions table:

- a. Select the line item.
- b. Below the table, click **Remove**.

The line item is removed from the IP-based access-restrictions table.

Step 7 To edit a line item in the CLI/DNIS access-restrictions table:

- a. Double-click the line item that you want to edit.

Information for the line item is removed from the table and written to the boxes below the table.

- b. Edit the information, as necessary.



Note

The total number of characters in the AAA Client list and the Port, CLI, and DNIS boxes must not exceed 1024. Although ACS is capable of accepting more than 1024 characters when you add a NAR, you cannot edit such a NAR and ACS cannot accurately apply it to users.

- c. Click **Enter**.

The edited information for this line item is written to the CLI/DNIS access-restrictions table.

Step 8 To remove a line item from the CLI/DNIS access-restrictions table:

- a. Select the line item.
- b. Below the table, click **Remove**.

The line item is removed from the CLI/DNIS access-restrictions table.

Step 9 To save the changes you have made, click **Submit**.

ACS reenters the filter with the new information, which takes effect immediately.

Deleting a Shared NAR

Before You Begin

Ensure that you remove the association of a shared NAR to any user or group before you delete that NAR.

To delete a shared NAR:

-
- | | |
|---------------|--|
| Step 1 | In the navigation bar, click Shared Profile Components .
The Shared Profile Components page appears. |
| Step 2 | Click Network Access Restrictions . |
| Step 3 | Click the Name of the shared NAR that you want to delete.
The Network Access Restriction page appears and displays information for the selected NAR. |
| Step 4 | At the bottom of the page, click Delete .
A dialog box warns you that you are about to delete a shared NAR. |
| Step 5 | To confirm that you want to delete the shared NAR, click OK .
The selected shared NAR is deleted. |
-

Command Authorization Sets

This section describes command-authorization sets and pattern matching, and provides detailed instructions for configuring and managing them.

This section contains:

- [About Command Authorization Sets, page 4-25](#)
 - [Command Authorization Sets Description, page 4-26](#)
 - [Command Authorization Sets Assignment, page 4-27](#)
 - [Case Sensitivity and Command Authorization, page 4-27](#)
 - [Arguments and Command Authorization, page 4-28](#)
 - [About Pattern Matching, page 4-28](#)
- [Adding a Command Authorization Set, page 4-29](#)
- [Editing a Command Authorization Set, page 4-30](#)
- [Deleting a Command Authorization Set, page 4-31](#)

About Command Authorization Sets

This section contains:

- [Command Authorization Sets Description, page 4-26](#)
- [Command Authorization Sets Assignment, page 4-27](#)
- [Case Sensitivity and Command Authorization, page 4-27](#)
- [Arguments and Command Authorization, page 4-28](#)
- [About Pattern Matching, page 4-28](#)

Command Authorization Sets Description

Command authorization sets provide a central mechanism to control the authorization of each command that is issued on any given network device. This feature greatly enhances the scalability and manageability of setting authorization restrictions. In ACS, the default command-authorization sets include Shell Command Authorization Sets and PIX Command Authorization Sets. Cisco device-management applications, such as Management Center for Firewalls, can instruct ACS to support additional command-authorization set types.



Note

PIX Command Authorization Sets require that the TACACS+ command-authorization request identify the service as **pixshell**. Verify that this service has been implemented in the version of PIX OS that your firewalls use; if not, use Shell Command Authorization Sets to perform command authorization for PIX devices. For information, see [Configuring a Shell Command Authorization Set for a User Group](#), page 5-23.



Tip

As of PIX OS version 6.3, the pixshell service has not been implemented.

To offer more control of device-hosted, administrative Telnet sessions, a network device using TACACS+ can request authorization for each command line before its execution. You can define a set of commands that are permitted or denied for execution by a particular user on a given device. ACS has further enhanced this capability with:

- **Reusable Named Command Authorization Sets**—Without directly citing any user or user group, you can create a named set of command authorizations. You can define several command-authorization sets, each delineating different access profiles. For example:
 - A **Help desk** command-authorization set could permit access to high level browsing commands, such as **show run**, and deny any configuration commands.
 - An **All network engineers** command-authorization set could contain a limited list of permitted commands for any network engineer in the enterprise.
 - A **Local network engineers** command-authorization set could permit all commands, including IP address configuration.
- **Fine Configuration Granularity**—You can create associations between named command-authorization sets and NDGs. Thus, you can define different access profiles for users depending on which network devices they access. You can associate the same named command-authorization set with more than one NDG and use it for more than one user group. ACS enforces data integrity. Named command-authorization sets are kept in the ACS internal database. You can use the ACS Backup and Restore features to back up and restore them. You can also replicate command-authorization sets to secondary ACSs along with other configuration data.

For command-authorization set types that support Cisco device-management applications, the benefits of using command-authorization sets are similar. You can enforce authorization of various privileges in a device-management application by applying command-authorization sets to ACS groups that contain users of the device-management application. The ACS groups can correspond to different roles within the device-management application and you can apply different command-authorization sets to each group, as applicable.

ACS has three sequential stages of command-authorization filtering. Each command-authorization request is evaluated in the following order:

1. **Command Match**—ACS determines whether the command being processed matches a command listed in the command-authorization set. If no matching command is found, command-authorization is determined by the Unmatched Commands setting: permit or deny. Otherwise, if the command is matched, evaluation continues.
2. **Argument Match**—ACS determines whether the command arguments presented match the command arguments listed in the command-authorization set.
 - If any argument is unmatched, command authorization is determined by whether the Permit Unmatched Args option is enabled. If unmatched arguments are permitted, the command is authorized and evaluation ends; otherwise, the command is not authorized and evaluation ends.
 - If all arguments are matched, evaluation continues.
3. **Argument Policy**—Having determined that the arguments in the command being evaluated match the arguments listed in the command-authorization set, ACS determines whether each command argument is explicitly permitted. If all arguments are explicitly permitted, ACS grants command authorization. If any arguments is not permitted, ACS denies command authorization.

Command Authorization Sets Assignment

For information on assigning command-authorization sets, see the following procedures:

- **Shell Command Authorization Sets**—See one of the following:
 - [Configuring a Shell Command Authorization Set for a User Group, page 5-23](#)
 - [Configuring a Shell Command Authorization Set for a User, page 6-17](#)
- **PIX Command Authorization Sets**—See one of the following:
 - [Configuring a PIX Command Authorization Set for a User Group, page 5-25](#)
 - [Configuring a PIX Command Authorization Set for a User, page 6-19](#)
- **Device Management Command Authorization Sets**—See one of the following:
 - [Configuring Device Management Command Authorization for a User Group, page 5-26](#)
 - [Configuring Device-Management Command Authorization for a User, page 6-20](#)

Case Sensitivity and Command Authorization

When performing command authorization, ACS evaluates commands and arguments in a case-sensitive manner. For successful command authorization, you must configure command-authorization sets with case-sensitive commands and arguments.

As an additional complication, a device requesting command authorization might send commands and arguments by using a case different from the one you typed to issue the command.

For example, if you type the following command during a router-hosted session:

```
interface FASTETHERNET 0/1
```

the router might submit the command and arguments to ACS as:

```
interface FastEthernet 0 1
```

If, for the **interface** command, the command-authorization set explicitly permits the FastEthernet argument by using the spelling **fastethernet**, ACS fails the command-authorization request. If the command-authorization rule instead permits the argument **FastEthernet**, ACS grants the command-authorization request. The case used in command-authorization sets must match what the device sends, which might or might not match the case you use when you type the command.

Arguments and Command Authorization

When you explicitly permit or deny arguments rather than rely on ACS to permit unmatched arguments, you must make certain that you know how devices send arguments to ACS. A device requesting command authorization might send different arguments than what the user typed to issue the command.

For example, if during a router-hosted session a user typed the following command:

```
interface FastEthernet0/1
```

the router might send the following command and arguments ACS:

```
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd=interface
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=FastEthernet
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=0
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=1
01:44:53: tty2 AAA/AUTHOR/CMD(390074395): send AV cmd-arg=<cr>
```

In this example, the router sees multiple arguments where the user typed one string of characters without spaces after the command. It also omits the slash (/) that separated 0 and 1 when the user issued the command.

If the command-authorization rule for the **interface** command explicitly permits the FastEthernet argument to use the spelling **FastEthernet0/1**, ACS fails the command-authorization request because it does not match what the router submitted to ACS. If the command-authorization rule instead permits the argument **FastEthernet 0 1**, ACS grants the command-authorization request. The case of arguments specified in command-authorization sets must match what the device sends, which might or might not match the case that you use when you type the arguments.

About Pattern Matching

For **permit** or **deny** command arguments, ACS applies pattern matching. That is, the argument **permit wid** matches any argument that contains the string **wid**. Thus, for example, **permit wid** would allow not only the argument **wid** but also the arguments **anywid** and **widget**.

To limit the extent of pattern matching you can add the following expressions:




- **Dollarsign (\$)**—Expresses that the argument must end with what has gone before. Thus **permit wid\$** would match **wid** or **anywid**, but not **widget**.
- **Caret (^)**—Expresses that the argument must begin with what follows. Thus **permit ^wid** would match **wid** or **widget**, but not **anywid**.

You can combine these expressions to specify absolute matching. In the example given, you would use **permit ^wid\$** to ensure that only **wid** was permitted, and not **anywid** or **widget**.

To **permit** or **deny** commands that carry no arguments, you can use absolute matching to specify the null argument condition. For example, you use **permit ^\$** to permit a command with no arguments. Alternatively, entering **permit <cr>** has the same effect. You can use either method, with the **Permit Unmatched Args** option unchecked, to match and permit or deny commands that have no argument.

Adding a Command Authorization Set

To add a command-authorization set:

-
- Step 1** In the navigation bar, click **Shared Profile Components**.
- The Shared Profile Components page lists the command-authorization set types that are available. These always include Shell Command Authorization Sets and may include others, such as command-authorization set types that support Cisco device-management applications.
- Step 2** Click one of the listed command-authorization set types, as applicable.
- The selected Command Authorization Sets table appears.
- Step 3** Click **Add**.
- The applicable Command Authorization Set page appears. Depending on the type of command-authorization set that you are adding, the contents of the page vary. Below the Name and Description boxes, ACS displays additional boxes or an expandable checklist tree. The expandable checklist tree appears for device command set types that support a Cisco device-management application.
- Step 4** In the **Name** box, type a name for the command-authorization set.
-  **Note** The set name can contain up to 27 characters. Names cannot contain the following characters: pound sign (#), question mark (?), quotes ("), asterisk (*), right angle bracket (>), left angle bracket (<). Leading and trailing spaces are not allowed.
-
- Step 5** In the **Description** box, type a description of the command-authorization set. The description can be up to 1,000 characters.
- Step 6** If ACS displays an expandable checklist tree below the Name and Description boxes, use the checklist tree to specify the actions permitted by the command-authorization set:
- a. To expand a checklist node, click the plus sign (+) to its left.
 - b. To enable an action, select its check box. For example, to enable a Device View action, select the **View** check box under the Device checklist node.
-  **Tip** Selecting an expandable check box node selects all check boxes within that node. Selecting the first check box in the checklist tree selects all check boxes in the checklist tree.
-
- c. To enable other actions in this command-authorization set, repeat Step a and Step b, as needed.
- Step 7** If ACS displays additional boxes below the Name and Description boxes, use the boxes to specify the commands and arguments permitted or denied by the command-authorization set:
- a. To specify how ACS should handle unmatched commands, select the **Permit** or **Deny** option, as applicable.
-  **Note** The default setting is **Deny**.
-
- b. In the box just above the Add Command button, type a command that is to be part of the set.

**Caution**

Enter the full command; if you use command abbreviations, authorization control might not function.

**Note**

Enter only the command portion of the command/argument string here. Arguments are added only after the command is listed. For example, with the command/argument string **show run** you would type only the command **show**.

- c. Click **Add Command**.

The typed command is added to the command list box.

- d. To add an argument to a command, in the **Command List** box, select the command and then type the argument in the box to the right of the command.

**Note**

The correct format for arguments is <permit | deny> <*argument*>. For example, with the command **show** already listed, you might enter **permit run** as the argument.

**Tip**

You can list several arguments for a single command by pressing **Enter** between arguments.

- e. To allow arguments, which you have not listed, to be effective with this command, select the **Permit Unmatched Args** check box.
- f. To add other commands to this command-authorization set, repeat Step a through Step e.

- Step 8** To save the command-authorization set, click **Submit**.

ACS displays the name and description of the new command-authorization set in the applicable Command Authorization Sets table.

Editing a Command Authorization Set

To edit a command-authorization set:

- Step 1** In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command-authorization set types available.

- Step 2** Click a command-authorization set type, as applicable.

The selected Command Authorization Sets table appears.

- Step 3** From the Name column, click the name of the set you want to change.

Information for the selected set appears on the applicable Command Authorization Set page.

- Step 4** If an expandable checklist tree appears below the Name and Description boxes, you can do any or all of the following:

- To expand a checklist node, click the plus (+) symbol to its left. To collapse an expanded checklist node, click the minus (-) symbol to its left.

- To enable an action, check its check box. For example, to enable a Device View action, check the **View** check box under the Device checklist node.

**Tip**

Selecting an expandable check box node selects all check boxes within that node. Selecting the first check box in the checklist tree selects all check boxes in the checklist tree.

- To disable an action, uncheck its check box. For example, to disable a Device View action, uncheck the **View** check box under the Device checklist node.

Step 5 If additional boxes appear below the Name and Description boxes, you can do any or all of the following:

- To change the set Name or Description, edit the words in the corresponding box. The description can be up to 1,000 characters.
- To remove a command from the set, from the Matched Commands list, select the command, and then click **Remove Command**.
- To edit arguments of a command, from the command list box, select the command and then type changes to the arguments in the box to the right of the command list box.

Step 6 To save the set, click **Submit**.

Deleting a Command Authorization Set

To delete a command-authorization set:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page lists the command-authorization set types available.

Step 2 Click a command-authorization set type, as applicable.

The selected Command Authorization Sets table appears.

Step 3 From the Name column, click the name of the command set that you want to delete.

Information for the selected set appears on the applicable Command Authorization Set page.

Step 4 Click **Delete**.

A dialog box warns you that you are about to delete a command-authorization set.

Step 5 To confirm that you want to delete that command-authorization set, click **OK**.

ACS displays the applicable Command Authorization Sets table. The command-authorization set is no longer listed.



CHAPTER 5

User Group Management

This chapter contains information about setting up and managing user groups for authorization control in the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS. You use ACS to group network users for more efficient administration. Each user can belong to only one group in ACS. You can establish up to 500 groups for different levels of authorization.

ACS also supports external database group mapping; that is, if your external user database distinguishes user groups, you can map these groups into ACS. And if the external database does not support groups, you can map all users from that database to an ACS user group. For information about external database mapping, see [Group Mapping by External User Database, page 16-1](#).



Caution

ACS 4.0 introduced the concept of Network Access Profiles (NAPs) that affects how group authorization occurs. If you are not using NAPs, ACS functions similar to previous versions. If you do plan to use NAPs, you must understand how Remote Access Dial-in User Service (RADIUS) authorization can be split between group, user, and NAP (via RACs).

This chapter contains:

- [About User Group Setup Features and Functions, page 5-2](#)
- [Basic User Group Settings, page 5-3](#)
- [Configuration-Specific User Group Settings, page 5-12](#)
- [Group Setting Management, page 5-40](#)

Before you configure Group Setup, you should understand how this section functions. ACS dynamically builds the Group Setup section interface depending on the configuration of your network devices and the security protocols being used. That is, what you see under Group Setup is affected by settings in the Network Configuration and Interface Configuration sections. Also, you can replace any group settings for downloadable access-control lists (DACLS) and RADIUS authorization components (RACs) with the settings in the network authorization policies (NAPs). Not every setting that you add to a group may work if you perform attribute merging. For more information on attribute merging, see [Understanding RACs and NAPs, page 4-7](#).

About User Group Setup Features and Functions

The Group Setup section of the ACS web interface is the centralized location for operations regarding user group configuration and administration. For information about network device groups (NDGs), see [Configuring Network Device Groups, page 3-23](#).

This section contains:

- [Default Group, page 5-2](#)
- [Group TACACS+ Settings, page 5-2](#)
- [Group RADIUS Settings, page 5-3](#)

Default Group

If you have not configured group mapping for an external user database, ACS assigns users who are authenticated by the Unknown User Policy to the Default Group the first time they log in. The privileges and restrictions for the default group are applied to first-time users. If you have upgraded from a previous version of ACS and kept your database information, ACS retains the group mappings that you configured before upgrading.

Group TACACS+ Settings

You can use ACS to create a full range of settings for Terminal Access Controller Access Control System (TACACS+) at the group level. If you have configured an authentication, authorization, and accounting (AAA) client to use TACACS+ as the security control protocol, you can configure standard service protocols, including Point-to-Point Protocol (PPP IP), Point-to-Point Protocol Link Control Protocol (PPP LCP), AppleTalk Remote Access Protocol (ARAP), Serial Line Internet Protocol (SLIP), and shell (exec), to apply for the authorization of each user who belongs to a particular group.



Note

You can also configure TACACS+ settings at the user level. User-level settings always override group-level settings.

You can also use ACS to enter and configure new TACACS+ services. For information about how to configure a new TACACS+ service to appear on the group setup page, see [Displaying TACACS+ Configuration Options, page 2-6](#).

If you have configured ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed, to support the device-management application. For more information about ACS interaction with device-management applications, see [Support for Cisco Device-Management Applications, page 1-14](#).

You can use the Shell Command Authorization Set feature to configure TACACS+ group settings. You use this feature to apply shell commands to a particular user group:

- Assign a shell command-authorization set, which you have already configured, for any network device.
- Assign a shell command-authorization set, which you have already configured, to particular NDGs.
- Permit or deny specific shell commands, which you define, on a per-group basis.

For more information about shell command-authorization sets, see [Command Authorization Sets, page 4-25](#).

Group RADIUS Settings

ACS contains a full range of settings for RADIUS at the group level. If a AAA client has been configured to use RADIUS as the security control protocol, you can configure standard services, including Internet Engineering Task Force (IETF), Microsoft, and Ascend, to apply to the authorization of each user who belongs to a particular group.



Note

You can also configure RADIUS settings at the user level. User-level settings always override group-level settings.

You can also use ACS to enter and configure new RADIUS services. For information about how to configure a new RADIUS service to appear on the group setup page, see [Displaying RADIUS Configuration Options, page 2-7](#).

If you decide to allow attribute merging in ACS, any RADIUS settings in all three (user, Shared Radius Authorization Component (SRAC), or group) will be overwritten by the user attributes first, then the shared RADIUS authorization component attributes, before allowing any group attributes settings.

Basic User Group Settings

This section presents the basic activities that you perform when configuring a new user group.

This section contains:

- [Group Disablement, page 5-3](#)
- [Enabling VoIP Support for a User Group, page 5-4](#)
- [Enabling VoIP Support for a User Group, page 5-4](#)
- [Setting Default Time-of-Day Access for a User Group, page 5-5](#)
- [Setting Callback Options for a User Group, page 5-5](#)
- [Setting Network Access Restrictions for a User Group, page 5-6](#)
- [Setting Max Sessions for a User Group, page 5-9](#)
- [Setting Usage Quotas for a User Group, page 5-10](#)

Group Disablement

You perform this procedure to disable a user group and, therefore, to prevent any member of the disabled group from authenticating.



Note

Group Disablement is the only setting in ACS where the setting at the group level may override the setting at the user level. If group disablement is set, all users within the disabled group are denied authentication, regardless of whether the user account is disabled. However, if a user account is disabled, it remains disabled; regardless of the status of the corresponding user group disablement setting. In other words, when group and user account disablement settings differ, ACS defaults to preventing network access.

To disable a group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group you want to disable, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Group Disabled table, check the check box labeled **Members of this group will be denied access to the network**.
- Step 4** To disable the group immediately, click **Submit + Apply**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
The group is disabled, and all members of the group are disabled.
-

Enabling VoIP Support for a User Group



Note

If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Voice-over-IP (VoIP) Group Settings** check box.

Perform this procedure to enable support for the null password function of VoIP. This action enables users to authenticate (session or telephone call) on only the user ID (telephone number).

When you enable VoIP at the group level, all users in this group become VoIP users, and the user IDs are treated similarly to a telephone number. VoIP users must not enter passwords to authenticate.



Caution

Enabling VoIP disables password authentication and most advanced settings, including password aging and protocol attributes. If a password is submitted with a VoIP user ID, ACS fails the attempt.

To enable VoIP support for a group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group that you want to configure for VoIP support, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Voice-over-IP Support table, check the check box labeled **This is a Voice-over-IP (VoIP) group - and all users of this group are VoIP users**.
- Step 4** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 5** To continue and specify other group settings, perform other procedures in this chapter, as applicable.
-

Setting Default Time-of-Day Access for a User Group



Note

If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Default Time-of-Day / Day-of-Week Specification** check box.

To define the times during which users in a particular group are permitted or denied access:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Default Time-of-Day Access Settings table, check the **Set as default Access Times** check box.
-
- Note
- You must check the **Set as default Access Times** check box to limit access based on time or day.
- Times at which the system permits access are highlighted in green on the day-and-hour matrix.
-
- Note
- The default sets accessibility during all hours.
- Step 4** In the day-and-hour matrix, click the times at which you do *not* want to permit access to members of this group.
-
- Tip
- Clicking times of day on the graph clears those times; clicking again rechecks them. At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.
- Step 5** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Setting Callback Options for a User Group

Callback is a command string that is passed back to the access server. You can use callback strings to initiate a modem to call the user back on a specific number for added security or reversal of line charges. The three options are:

- **No callback allowed**—Disables callback for users in this group. This is the default setting.
- **Dialup client specifies callback number**—Allows the dialup client to specify the callback number. The dialup client must support RFC 1570, PPP LCP Extensions.

- **Use Windows Database callback settings (where possible)**—Uses the Microsoft Windows callback settings. If a Windows account for a user resides in a remote domain, the domain in which ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.



Note If you enable the Windows Database callback settings, the Windows Callback feature must also be enabled in the Windows Database Configuration Settings. See [Windows User Database Configuration Options, page 12-18](#).



Note The **Password Aging** feature does not operate correctly if you also use the callback feature. When you use callback, users cannot receive password aging messages at login.

To set callback options for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** Select a group from the Group list, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Callback table, select one of the following three options:
- No callback allowed.
 - Dialup client specifies callback number.
 - Use Windows Database callback settings (where possible).
- Step 4** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 5** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Setting Network Access Restrictions for a User Group

You use the Network Access Restrictions table in Group Setup to apply network-access restrictions (NARs) in three distinct ways:

- Apply existing shared NARs by name.
- Define IP-based group access restrictions to permit or deny access to a specified AAA client or to specified ports on a AAA client when an IP connection has been established.
- Define CLI/DNIS-based group NARs to permit or deny access to either, or both, the calling line ID (CLI) number or the Dialed Number Identification Service (DNIS) number used.



Note You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see [About Network Access Restrictions, page 4-18](#).

Typically, you define (shared) NARs from within the Shared Components section so that these restrictions can apply to more than one group or user. For more information, see [Adding a Shared NAR, page 4-21](#). You must check the **Group-Level Shared Network Access Restriction** check box on the **Advanced Options** page of the Interface Configuration section for these options to appear in the ACS web interface.

However, you can also use ACS to define and apply a NAR for a single group from within the **Group Setup** section. You must check the **Group-Level Network Access Restriction** setting under the Advanced Options page of the Interface Configuration section for single group IP-based filter options and single group CLI/DNIS-based filter options to appear in the ACS web interface.

**Note**

When an authentication request is forwarded by proxy to an ACS server, any NARs for RADIUS requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

To set NARs for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** To apply a previously configured shared NAR to this group:

**Note**

To apply a shared NAR, you must have configured it under Network Access Restrictions in the Shared Profile Components section. For more information, see [Adding a Shared NAR, page 4-21](#).

- a. Check the **Only Allow network access when** check box.
- b. To specify whether one or all shared NARs must apply for a member of the group to be permitted access, check one of the following options:
 - All selected shared NARS result in permit.
 - Any one selected shared NAR results in permit.
- c. Select a shared NAR name in the Shared NAR list, and then click --> (right arrow button) to move the name into the Selected Shared NARs list.

**Tip**

To view the server details of the shared NARs that you have applied, you can click **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

- Step 4** To define and apply a NAR for this particular user group, that permits or denies access to this group based on IP address, or IP address and port:

**Tip**

You should define most NARs from within the Shared Components section so that the restrictions can apply to more than one group or user. For more information, see [Adding a Shared NAR, page 4-21](#).

- a. In the Per Group Defined Network Access Restrictions section of the Network Access Restrictions table, check the **Define IP-based access restrictions** check box.
- b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select **Permitted Calling/Point of Access Locations** or **Denied Calling/Point of Access Locations**.
- c. Select or enter the information in the following boxes:
 - **AAA Client**—Select All AAA Clients or the name of the NDG or the name of the individual AAA client to which you want to permit or deny access.
 - **Port**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports on the selected AAA client.
 - **Address**—Type the IP address or addresses to filter on when performing access restrictions. You can use the asterisk (*) as a wildcard.

**Note**

The total number of characters in the AAA Client list and the Port and Src IP Address boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

- d. Click **enter**.

The specified the AAA client, port, and address information appears in the **NAR Access Control** list.

Step 5 To permit or deny access to this user group based on calling location or values other than an established IP address:

- a. Check the **Define CLI/DNIS-based access restrictions** check box.
- b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one:
 - **Permitted Calling/Point of Access Locations**
 - **Denied Calling/Point of Access Locations**
- c. From the AAA Client list, choose **All AAA Clients**, or the name of the NDG or the name of the particular AAA client to which to permit or deny access.
- d. Complete the following boxes:

**Note**

You must type an entry in each box. You can use the asterisk (*) as a wildcard for all or part of a value. The format that you use must match the format of the string you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **PORT**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number or all numbers.

**Tip**

CLI is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet client MAC address. For more information, see [About Network Access Restrictions, page 4-18](#).

- **DNIS**—Type the DNIS number to restrict access based on the number into which the user will be dialing. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number or all numbers.

**Tip**

CLI is also the selection to use if you want to restrict access based on other values, such as a Cisco Aironet AP MAC address. For more information, see [About Network Access Restrictions, page 4-18](#).

**Note**

The total number of characters in the AAA Client list, and the Port, CLI, and DNIS boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

- e. Click **enter**.

The information, that specifies the AAA client, port, CLI, and DNIS appears in the list.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Setting Max Sessions for a User Group

**Note**

If the **Max Sessions** feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Max Sessions** check box.

Perform this procedure to define the maximum number of sessions that are available to a group, or to each user in a group, or both. The settings are:

- **Sessions available to group**—Sets the maximum number of simultaneous connections for the entire group.
- **Sessions available to users of this group**—Sets the maximum number of total simultaneous connections for each user in this group.


**Tip**

As an example, Sessions available to group is set to 10 and Sessions available to users of this group is set to 2. If each user is using the maximum 2 simultaneous sessions, no more than five users can log in.

A session is any type of connection that RADIUS or TACACS+ supports, such as PPP, NAS prompt, Telnet, ARAP, and IPX/SLIP.

The default setting for group Max Sessions is Unlimited for the group and the user within the group.

To configure Max Sessions settings for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** In the Max Sessions table, under Sessions available to group, select one of the following options:
- **Unlimited**—Allows this group an unlimited number of simultaneous sessions. (This action effectively disables Max Sessions.)
 - *n*—Type the maximum number of simultaneous sessions to allow this group.
- Step 4** In the lower portion of the Max Sessions table, under Sessions available to users of this group, select one of the following two options:
- **Unlimited**—Allows each individual in this group an unlimited number of simultaneous sessions. (This action effectively disables Max Sessions.)
 - *n*—Type the maximum number of simultaneous sessions to allow each user in this group.
-
-  **Note** Settings made in User Setup override group settings. For more information, see [Setting Max Sessions Options for a User, page 6-11](#).
-
- Step 5** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 6** Ensure the AAA client device has accounting enabled to allow Max Sessions checks to work. If accounting is not enabled, Max Sessions will not work.
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Setting Usage Quotas for a User Group



Note

If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Usage Quotas** check box.

Perform this procedure to define usage quotas for members of a group. Session quotas affect each user of a group individually, not the group collectively. You can set quotas for a given period in two ways:

- Total duration of session
- The total number of sessions

If you make no selections in the Usage Quotas section for a group, no usage quotas are enforced on users who are assigned to that group; unless you configure usage quotas for the individual users.

**Note**

The Usage Quotas section on the Group Settings page does not show usage statistics. Usage statistics are available only on the settings page for an individual user. For more information, see [Options for Setting User Usage Quotas, page 6-12](#).

When a user exceeds his or her assigned quota, ACS denies that user access on attempting to start a session. If a quota is exceeded during a session, ACS allows the session to continue.

You can reset the usage quota counters for all users of a group from the Group Settings page. For more information about resetting usage quota counters for a whole group, see [Resetting Usage Quota Counters for a User Group, page 5-40](#).

**Tip**

To support time-based quotas, we recommend enabling accounting-update packets on all AAA clients. If update packets are not enabled, the quota is updated when the user logs off. If the AAA client through which the user is accessing your network fails, the quota is not updated. In the case of multiple sessions, such as with Integrated Services Digital Network (ISDN), the quota is not updated until all sessions terminate. A second channel will, therefore, be accepted; even if the first channel has exhausted the quota for the user.

To set user usage quotas for a user group:

Step 1 In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

Step 2 From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 To define usage quotas based on duration of sessions:

- a. In the Usage Quotas table, check the **Limit each user of this group to x hours of online time per time unit** check box.
- b. Type the number of hours to which you want to limit group members in the **to x hours** box. Use decimal values to indicate minutes. For example, a value of 10.5 would equal ten hours and 30 minutes.

**Note**

Up to five characters are allowed in the to x hours box.

c. Select the period for which the quota is effective:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of hours, with no end.

Step 4 To define user session quotas based on number of sessions:

- a. In the Usage Quotas table, check the **Limit each user of this group to x sessions** check box.
- b. Type the number of sessions to which you want to limit users in the **to x sessions** box.



Note Up to five characters are allowed in the to x sessions box.

c. Select the period for which the session quota is effective:

- **per Day**—From 12:01 a.m. until midnight.
- **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
- **Total**—An ongoing count of session, with no end.

Step 5 To save the group settings, that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 6 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuration-Specific User Group Settings

This section details procedures that you perform only as applicable to your particular network-security configuration. For instance, if you have no token server configured, you do not have to set token card settings for each group.



Note

When you configure a vendor-specific variety of RADIUS for use by network devices, the RADIUS (IETF) attributes are available because they are the base set of attributes, that all RADIUS vendors use per the RADIUS IETF specifications.

The web interface content corresponding to these procedures is dynamic and its appearance is based on:

- For a particular protocol (RADIUS or TACACS+) to be listed, at least one AAA client entry in the Network Configuration section of the web interface must use that protocol. For more information, see [Configuring AAA Clients, page 3-8](#).
- For specific protocol attributes to appear on a group profile page, you must enable the display of those attributes in the Interface Configuration section of the web interface. For more information, see [Displaying TACACS+ Configuration Options, page 2-6](#), or [Displaying RADIUS Configuration Options, page 2-7](#).



Caution

If you are using SRACs in 4.0, you should be aware of certain issues regarding attribute merging, and overwriting DACLS and RADIUS attributes on a user or group level. You should not assign RADIUS attributes to an individual user (only as a last resort). Use group or SRACs to assign RADIUS attributes in the user's group or profile levels. For more information on how to select RAC, the authorization rules that you use to set up your network profiles, see [Configuring an Authorization Rule, page 14-36](#).

This section contains:

- [Setting Enable Privilege Options for a User Group, page 5-13](#)
- [Setting Enable Privilege Options for a User Group, page 5-13](#)
- [Enabling Password Aging for the ACS Internal Database, page 5-15](#)

- [Enabling Password Aging for Users in Windows Databases, page 5-19](#)
- [Setting IP Address Assignment Method for a User Group, page 5-21](#)
- [Assigning a Downloadable IP ACL to a Group, page 5-22](#)
- [Configuring TACACS+ Settings for a User Group, page 5-22](#)
- [Configuring a Shell Command Authorization Set for a User Group, page 5-23](#)
- [Configuring a PIX Command Authorization Set for a User Group, page 5-25](#)
- [Configuring Device Management Command Authorization for a User Group, page 5-26](#)
- [Configuring IETF RADIUS Settings for a User Group, page 5-27](#)
- [Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group, page 5-28](#)
- [Configuring Cisco Airespace RADIUS Settings for a User Group, page 5-29](#)
- [Configuring Cisco Aironet RADIUS Settings for a User Group, page 5-30](#)
- [Configuring Ascend RADIUS Settings for a User Group, page 5-31](#)
- [Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group, page 5-32](#)
- [Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 5-33](#)
- [Configuring Microsoft RADIUS Settings for a User Group, page 5-34](#)
- [Configuring Nortel RADIUS Settings for a User Group, page 5-36](#)
- [Configuring Juniper RADIUS Settings for a User Group, page 5-37](#)
- [Configuring BBSM RADIUS Settings for a User Group, page 5-38](#)
- [Configuring Custom RADIUS VSA Settings for a User Group, page 5-39](#)

Setting Enable Privilege Options for a User Group



Note

If this section does not appear, choose **Interface Configuration > TACACS+ (Cisco)**. At the bottom of the page in the Advanced Configuration Options table, check the **Advanced TACACS+ features** check box.

Perform this procedure to configure group-level TACACS+ enabling parameters. The three possible TACACS+ enable options are:

- **No Enable Privilege**—(default) Disallows enable privileges for this user group.
- **Max Privilege for Any AAA Client**—Selects the maximum privilege level for this user group for any AAA client on which this group is authorized.
- **Define max Privilege on a per-network device group basis**—Defines maximum privilege levels for an NDG. To use this option, you create a list of device groups and corresponding maximum privilege levels. See your AAA client documentation for information about privilege levels.



Note

To define levels in this manner, you must have configured the option in Interface Configuration; if you have not done so already, choose **Interface Configuration > Advanced Settings**. Then, check the **Network Device Groups** check box.

If you are using NDGs, you use this option to configure the NDG for enable-level mapping; rather than having to do it for each user in the group.

To set enable privilege options for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **Enable Options**.
- Step 4** Do one of the following:
- Disallow enable privileges for this user group, choose the **No Enable Privilege** option.
 - Set the maximum privilege level for this user group, for any ACS on which this group is authorized. Choose:
 - **Max Privilege for Any Access Server** option
 - Maximum privilege level from the list
 - Define the maximum NDG privilege level for this user group:
 - select the **Define max Privilege on a per-network device group basis** option
 - from the lists, choose the NDG and a corresponding privilege level
 - click **Add Association**
- Result:** The association of NDG and maximum privilege level appears in the table.
- Step 5** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Setting Token Card Settings for a User Group



Note

If this section does not appear, configure a token server. Then, choose **External User Databases> Database Configuration**. Then, add the applicable token card server.

Perform this procedure to allow a token to be cached. Users, therefore, can use a second B channel without having to enter a second one-time password (OTP).



Caution

This option is for use with token caching only for ISDN terminal adapters. You should fully understand token caching, and ISDN concepts and principles before implementing this option. Token caching allows you to connect to multiple B channels without having to provide a token for each channel connection. Token card settings are applied to all users in the selected group.

Options for token caching include the following:

- **Session**—You can select Session to cache the token for the entire session. This option allows the second B channel to dynamically go in and out of service.
- **Duration**—You can select Duration and specify a period of time to have the token cached (from the time of first authentication). If this time period expires, the user cannot start a second B channel.
- **Session and Duration**—You can select Session and Duration so that, if the session runs longer than the duration value, a new token is required to open a second B channel. Type a value high enough to allow the token to be cached for the entire session. If the session runs longer than the duration value, a new token is required to open a second B channel.

To set token card settings for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **Token Cards**.
- Step 4** In the Token Card Settings table, to cache the token for the entire session, choose **Session**.
- Step 5** Also in the Token Card Settings table, to cache the token for a specified time period (measured from the time of first authentication):
- Choose **Duration**.
 - Type the duration length in the box.
 - Choose the unit of measure: **Seconds**, **Minutes** or **Hours**.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Enabling Password Aging for the ACS Internal Database

You use the **Password Aging** feature of ACS to force users to change their passwords under one or more of the following conditions:

- After a specified number of days (age-by-date rules).
- After a specified number of logins (age-by-uses rules).
- The first time a new user logs in (password change rule).

Varieties of Password Aging Supported by ACS

ACS supports four distinct password-aging mechanisms:

- **Protected Extensible Authentication Protocol (PEAP) and Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) Windows Password Aging**—Users must be in the Windows user database and be using a Microsoft client that supports

EAP, such as Windows XP. For information on the requirements and configuration of this password-aging mechanism, see [Enabling Password Aging for Users in Windows Databases, page 5-19](#).

- **RADIUS-based Windows Password Aging**—Users must be in the Windows user database and be using a RADIUS client/supplicant that supports changing passwords by using Microsoft-Challenge Authentication Handshake Protocol (MS-CHAP). For information on the requirements and configuration of this password aging mechanism, see [Enabling Password Aging for Users in Windows Databases, page 5-19](#).
- **Password Aging for Device-hosted Sessions**—Users must be in the ACS internal database, the AAA client must be running TACACS+, and the connection must use Telnet. You can control the ability of users to change passwords during a device-hosted Telnet session. You can also control whether ACS propagates passwords changed by using this feature. For more information, see [Local Password Management, page 7-4](#).
- **Password Aging for Transit Sessions**—Users must be in the ACS internal database. Users must use a PPP dialup client. Further, the end-user client must have Cisco Authentication Agent (CAA) installed.

**Tip**

The CAA software is available at <http://www.cisco.com>.

Also, to run password aging for transit sessions, the AAA client can be running RADIUS or TACACS+; moreover, the AAA client must be using Cisco IOS Release 11.2.7 or later and be configured to send a watchdog accounting packet (`aaa accounting new-info update`) with the IP address of the calling station. (Watchdog packets are interim packets sent periodically during a session. They provide an approximate session length in the event that no stop packet is received to mark the end of the session.)

You can control whether ACS propagates passwords changed by using this feature. For more information, see [Local Password Management, page 7-4](#).

ACS supports password aging by using the RADIUS protocol under MS CHAP versions 1 and 2. ACS does not support password aging over Telnet connections that use the RADIUS protocol.

**Caution**

If a user with a RADIUS connection tries to make a Telnet connection to the AAA client during or after the password aging warning or grace period, the Change Password option does not appear, and the user account is expired.

Password Aging Feature Settings

This section details only the Password Aging for Device-hosted Sessions and Password Aging for Transit Sessions mechanisms. For information on the Windows Password Aging mechanism, see [Enabling Password Aging for Users in Windows Databases, page 5-19](#). For information on configuring local password validation options, see [Local Password Management, page 7-4](#).

**Note**

The Password Aging feature does not operate correctly if you also use the Callback feature. When callback is used, users cannot receive password-aging messages at login.

The Password Aging feature in ACS has the following options:

- **Apply age-by-date rules**—Configures ACS to determine password aging by date. The age-by-date rules contain the following settings:
 - **Active period**—The number of days users will be allowed to log in before being prompted to change their passwords. For example, if you enter 20, users can use their passwords for 20 days without being prompted to change them. The default Active period is 20 days.
 - **Warning period**—The number of days, after which users will be notified to change their passwords. The existing password can be used; but the ACS presents a warning indicating that the password must be changed and displays the number of days left before the password expires. For example, if you enter 5 in this box and 20 in the Active period box, users will be notified to change their passwords on the 21st through 25th days.
 - **Grace period**—The number of days for the user grace period, which allows a user to log in once to change the password. The existing password can be used one last time after the number of days specified in the active and warning period fields has been exceeded. Then, a dialog box warns the user that the account will be disabled if the password is not changed, and prompts the user to change it. Continuing with the previous examples, if you allow a 5-day grace period, a user who did not log in during the active and warning periods would be permitted to change passwords up to and including the 30th day. However, even though the grace period is set for 5 days, a user is allowed only one attempt to change the password when the password is in the grace period. ACS displays the “last chance” warning only once. If the user does not change the password, this login is still permitted, but the password expires, and the next authentication is denied. An entry is logged in the Failed-Attempts log, and the user must contact an administrator to have the account reinstated.



Note All passwords expire at midnight of the date that you enter, not the time of day at which they were set.

- **Apply age-by-uses rules**—Configures ACS to determine password aging by the number of logins. The age-by-uses rules contain the following settings:
 - **Issue warning after x logins**—The number of the login after which ACS begins prompting users to change their passwords. For example, if you enter 10, users are allowed to log in 10 times without a change-password prompt. On the 11th login, they are prompted to change their passwords.



Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Require change after x logins**—The number of logins after which to notify users that they must change their passwords. If this number is set to 12, users receive prompts requesting them to change their passwords on their 11th and 12th login attempts. On the 13th login attempt, they receive a prompt telling them that they must change their passwords. If users do not change their passwords now, their accounts expire and they cannot log in. This number must be greater than the **Issue warning after x login** number.



Tip To allow users to log in an unlimited number of times without changing their passwords, type **-1**.

- **Apply password change rule**—Forces new users to change their passwords the first time they log in.

- **Generate greetings for successful logins**—Displays Greetings message whenever users log in successfully via the CAA client. The message contains the latest password information specific to this user account.

The password aging rules are not mutually exclusive; a rule is applied for each check box that is selected. For example, users can be forced to change their passwords every 20 days, and every 10 logins, and to receive warnings and grace periods accordingly.

If no options are selected, passwords never expire.


Unlike most other parameters, which have corresponding settings at the user level, password aging parameters are configured only on a group basis.

Users who fail authentication because they have not changed their passwords and have exceeded their grace periods are logged in the Failed Attempts log. The accounts expire and appear in the Accounts Disabled list.

Before You Begin

- Verify that your AAA client is running the TACACS+ or RADIUS protocol. (TACACS+ only supports password aging for device-hosted sessions.)
- Set up your AAA client to perform authentication *and* accounting using the same protocol, TACACS+ or RADIUS.
- Verify that you have configured your password validation options. For more information, see [Local Password Management, page 7-4](#).
- Set up your AAA client to use Cisco IOS Release 11.2.7 or later and to send a watchdog accounting packet (`aaa accounting new-info update`) with the IP address of the calling station.

To set **Password Aging** rules for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **Password Aging**.
The Password Aging Rules table appears.
- Step 4** To set password aging by date, check the **Apply age-by-date rules** check box and type the number of days for the following options, as applicable:
- Active period
 - Warning period
 - Grace period
-  **Note** Up to five characters are allowed in each field.
-
- Step 5** To set password aging by use, check the **Apply age-by-uses rules** check box and type the number of logins for each of the following options, as applicable:
- Issue warning after *x* logins
 - Require change after *x* logins



Note Up to five characters are allowed in each field.

- Step 6** To force the user to change the password on the first login after an administrator has changed it, check the **Apply password change rule** check box.
- Step 7** To display a Greetings message, check the **Generate greetings for successful logins** check box.
- Step 8** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 9** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Enabling Password Aging for Users in Windows Databases

ACS supports three types of password aging for users in Windows databases. Both types of Windows password aging mechanisms are separate and distinct from the other ACS password aging mechanisms. For information on the requirements and settings for the password aging mechanisms that control users in the ACS internal database, see [Enabling Password Aging for the ACS Internal Database, page 5-15](#).



Note You can run Windows Password Aging and ACS Password Aging for Transit Sessions mechanisms concurrently, provided that the users authenticate from the two different databases.

The types of password aging in Windows databases are:

- **RADIUS-based password aging**—RADIUS-based password aging depends on the RADIUS AAA protocol that you use to send and receive the password change messages. Requirements for implementing the RADIUS-based Windows password aging mechanism include the following:
 - Communication between ACS and the AAA client must be using RADIUS.
 - The AAA client must support MS CHAP password aging in addition to MS CHAP authentication.
 - Users must be in a Windows user database.
 - Users must be using the Windows RADIUS client and server that supports changing passwords by using MS-CHAP.
 - You must enable MS CHAP version 1 or MS CHAP version 2, or both, in the Windows configuration within the External User Databases section.



Tip For information on enabling MS CHAP for password changes, see [Configuring a Windows External User Database, page 12-21](#). For information on enabling MS CHAP in System Configuration, see [Global Authentication Setup, page 9-21](#).

- **PEAP password aging**—PEAP password aging depends on the PEAP (EAP-GTC) or PEAP (EAP-MSCHAPv2) authentication protocol to send and receive the password change messages. Requirements for implementing the PEAP Windows password aging mechanism include:
 - The AAA client must support EAP.
 - Users must be in a Windows user database.

- Users must be using a Microsoft PEAP client, such as Windows XP.
- You must enable PEAP on the Global Authentication Configuration page within the System Configuration section.

**Tip**

For information about enabling PEAP in System Configuration, see [Global Authentication Setup, page 9-21](#).

- You must enable PEAP password changes on the Windows Authentication Configuration page within the External User Databases section.

**Tip**

For information about enabling PEAP password changes, see [Windows User Database, page 12-5](#).

- **EAP-FAST password aging**—If password aging occurs during phase zero of EAP-FAST, it depends on EAP-MSCHAPv2 to send and receive the password change messages. If password aging occurs during phase two of EAP-FAST, it depends on Extensible Authentication Protocol - Generic Token Card (EAP-GTC) to send and receive the password change messages. Requirements for implementing the EAP-FAST Windows password aging mechanism include:
 - The AAA client must support EAP.
 - Users must be in a Windows user database.
 - Users must be using a client that supports EAP-FAST.
 - You must enable EAP-FAST on the Global Authentication Configuration page within the System Configuration section.

**Tip**

For information about enabling EAP-FAST in System Configuration, see [Global Authentication Setup, page 9-21](#).

- You must enable EAP-FAST password changes on the Windows Authentication Configuration page within the External User Databases section.

**Tip**

For information about enabling EAP-FAST password changes, see [Windows User Database, page 12-5](#).

Users whose Windows accounts reside in remote domains (that is, not the domain within which ACS is running) can only use the Windows-based password aging if they supply their domain names.



The methods and functionality of Windows password aging differ according to the Microsoft Windows operating system that you are using, and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). Setting password aging for users in the Windows user database is only one part of the larger task of setting security policies in Windows. For comprehensive information on Windows procedures, refer to your Windows system documentation.

Setting IP Address Assignment Method for a User Group

Perform this procedure to configure the way ACS assigns IP addresses to users in the group. The four possible methods are:

- **No IP address assignment**—No IP address is assigned to this group.
- **Assigned by dialup client**—Use the IP address that is configured on the dialup client network settings for TCP/IP.
- **Assigned from AAA Client pool**—The IP address is assigned by an IP address pool that is assigned on the AAA client.
- **Assigned from AAA server pool**—The IP address is assigned by an IP address pool that is assigned on the AAA server.

To set an IP address assignment method for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **IP Address Assignment**.
- Step 4** In the IP Assignment table, select one:
- **No IP address assignment.**
 - **Assigned by dialup client.**
 - **Assigned from AAA Client pool.** Then, type the AAA client IP pool name.
 - **Assigned from AAA pool.** Then, choose the AAA server IP pool name in the Available Pools list and click --> (right arrow button) to move the name into the Selected Pools list.
- 
- Note** If the Selected Pools list contains more than one pool, the users in this group are assigned to the first available pool in the order listed.
- 
- Tip** To change the position of a pool in the list, choose the pool name and click **Up** or **Down** until the pool is in the order that you want.
-
- Step 5** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 6** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Assigning a Downloadable IP ACL to a Group

You use the Downloadable ACLs feature to assign an IP ACL at the group level.

**Note**

You must have established one or more IP ACLs before attempting to assign one. For instructions on how to add a downloadable IP ACL by using the Shared Profile Components section of the ACS web interface, see [Adding a Downloadable IP ACL, page 4-15](#).

**Tip**

The Downloadable ACLs table does not appear if you have not enabled it. To enable the Downloadable ACLs table, choose **Interface Configuration > Advanced Options**. Then, check the **Group-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
 - Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
 - Step 3** From the Jump To list at the top of the page, choose **Downloadable ACLs**.
 - Step 4** Under the Downloadable ACLs section, click the **Assign IP ACL** check box.
 - Step 5** Select an IP ACL from the list.
 - Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
 - Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring TACACS+ Settings for a User Group

Perform this procedure to configure and enable the service or protocol parameters to apply to the authorization of each user who belongs to the group. For information on how to configure settings for the Shell Command Authorization Set, see [Configuring a Shell Command Authorization Set for a User Group, page 5-23](#).

**Note**

To display or hide additional services or protocols, choose **Interface Configuration > TACACS+ (Cisco IOS)**, and then choose or clear items in the group column, as applicable.

To configure TACACS+ settings for a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
 - Step 2** From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

Step 3 From the Jump To list at the top of the page, choose **TACACS+**.

The system displays the TACACS+ Settings table section.

Step 4 To configure services and protocols in the TACACS+ Settings table to be authorized for the group:

- a. Select one or more service or protocol check boxes (for example, PPP IP or ARAP).
- b. Under each service or protocol that you selected in Step a, select attributes and then type in the corresponding values, as applicable, to further define authorization for that service or protocol.

To employ custom attributes for a particular service, you must check the **Custom attributes** check box under that service, and then specify the attribute or value in the box below the check box.

For more information about attributes, see [Appendix A, “TACACS+ Attribute-Value Pairs,”](#) or your AAA client documentation.



Tip

For ACLs and IP address pools, enter the name of the ACL or pool as defined on the AAA client. (An ACL is a list of Cisco IOS commands that you use to restrict access to or from other devices and users on the network.)



Note

Leave the attribute value box blank to use the default (as defined on the AAA client).



Note

You can define and download an ACL. Click **Interface Configuration > TACACS+ (Cisco IOS)**, and then select **Display a window for each service selected in which you can enter customized TACACS+ attributes**. A box opens under each service or protocol in which you can define an ACL.

Step 5 To allow all services to be permitted unless specifically listed and disabled, check the **Default (Undefined) Services** check box under the Checking this option will PERMIT all UNKNOWN Services table.



Caution

The Default (Undefined) Services option is an advanced feature and should only be used by administrators who understand the security implications.

Step 6 To save the group settings that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring a Shell Command Authorization Set for a User Group

Use this procedure to specify the shell command-authorization set parameters for a group. The four options are:

- **None**—No authorization for shell commands.

- **Assign a Shell Command Authorization Set for any network device**—One shell command-authorization set is assigned, and it applies to all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Associates particular shell command-authorization sets to be effective on particular NDGs.
- **Per Group Command Authorization**—Permits or denies specific Cisco IOS commands and arguments at the group level.

**Note**

This feature requires that you have previously configured a shell command-authorization set. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

To specify shell command-authorization set parameters for a user group:

- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **TACACS+**.
The system displays the TACACS+ Settings table section.
- Step 4** Use the vertical scroll bar to scroll to the Shell Command Authorization Set feature area.
- Step 5** To prevent the application of any shell command-authorization set, select (or accept the default of) the **None** option.
- Step 6** To assign a particular shell command-authorization set to be effective on any configured network device:
 - a. Select the **Assign a Shell Command Authorization Set for any network device** option.
 - b. Then, from the list directly below that option, choose the shell command-authorization set that you want applied to this group.
- Step 7** To create associations that assign a particular shell command-authorization set to be effective on a particular NDG, for each association:
 - a. Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.
 - b. Select a **Device Group** and a corresponding **Command Set**.

**Tip**

You can select a **Command Set** that will be effective for all **Device Groups**, that are not otherwise assigned, by assigning that set to the *<default>* Device Group.

- c. Click **Add Association**.
The associated NDG and shell command-authorization set appear in the table.
- Step 8** To define the specific Cisco IOS commands and arguments to be permitted or denied at the group level:
 - a. Select the **Per Group Command Authorization** option.
 - b. Under Unmatched Cisco IOS commands, select **Permit** or **Deny**.
If you select **Permit**, users can issue all commands not specifically listed. If you select **Deny**, users can issue only those commands listed.

- c. To list particular commands to be permitted or denied, check the **Command** check box and then type the name of the command, define its arguments by using standard **Permit** or **Deny** syntax, and select whether unlisted arguments should be permitted or denied.

**Caution**

Only an administrator who is skilled with Cisco IOS commands should use this powerful, advanced feature. Correct syntax is the responsibility of the administrator. For information on how ACS uses pattern matching in command arguments, see [About Pattern Matching, page 4-28](#).

**Tip**

To enter several commands, you must click **Submit** after specifying a command. A new command entry box appears below the box that you just completed.

Configuring a PIX Command Authorization Set for a User Group

Use this procedure to specify the PIX command-authorization set parameters for a user group. The three options are:

- **None**—No authorization for PIX commands.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command-authorization set is assigned and it applies all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command-authorization sets are to be effective on particular NDGs.

Before You Begin:

- Ensure that you configure a AAA client to use TACACS+ as the security control protocol.
- On the TACACS+ (Cisco) page of Interface Configuration section, ensure that you check the PIX Shell (**pixShell**) option in the Group column.
- Be certain that you have already configured one or more PIX command-authorization sets. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

To specify PIX command-authorization set parameters for a user group:

- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **TACACS+**.
The system displays the TACACS+ Settings table section.
- Step 4** Scroll down to the PIX Command Authorization Set feature area within the TACACS+ Settings table.
- Step 5** To prevent the application of any PIX command-authorization set, select (or accept the default of) the **None** option.

- Step 6** To assign a particular PIX command-authorization set that is to be effective on any configured network device:
- Select the **Assign a PIX Command Authorization Set for any network device** option.
 - From the list directly below that option, choose the PIX command-authorization set that you want applied to this user group.
- Step 7** To create associations that assign a particular PIX command-authorization set to be effective on a particular NDG, for each association:
- Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.
 - Select a **Device Group** and an associated **Command Set**.
 - Click **Add Association**.

The associated NDG and PIX command-authorization sets appear in the table.



Note To remove or edit an existing PIX command-authorization set association, you can select the association from the list, and then click **Remove Association**.

Configuring Device Management Command Authorization for a User Group

Use this procedure to specify the device-management command-authorization set parameters for a group. Device-management command-authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use ACS for authorization. The three options are:

- None**—No authorization is performed for commands that are issued in the applicable Cisco device-management application.
- Assign a device-management application** for any network device—For the applicable device-management application, one command-authorization set is assigned and it applies to management tasks on all network devices.
- Assign a device-management application** on a per Network Device Group Basis—For the applicable device-management application, you use this option to apply command-authorization sets to specific NDGs, so that it affects all management tasks on the network devices belonging to the NDG.



Note To use this feature, you must configure a command-authorization set for the applicable Cisco device-management application. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

To specify device-management application command-authorization for a user group:

- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.

- Step 3** From the Jump To list at the top of the page, choose **TACACS+**.
The system displays the TACACS+ Settings table section.
- Step 4** Use the vertical scroll bar to scroll to the *device-management application* feature area, where *device-management application* is the name of the applicable Cisco device-management application.
- Step 5** To prevent the application of any command-authorization set for the applicable device-management application, select the **None** option.
- Step 6** To assign a particular command-authorization set that affects device-management application actions on any network device:
- Select the **Assign a device-management application** for any network device option.
 - Then, from the list directly below that option, choose the command-authorization set that you want applied to this group.
- Step 7** To create associations that assign a particular command-authorization set that affects device-management application actions on a particular NDG, for each association:
- Select the **Assign a device-management application** on a per Network Device Group Basis option.
 - Select a **Device Group** and a corresponding **device-management application**.
 - Click **Add Association**.
- The associated NDG and command-authorization sets appear in the table.
-

Configuring IETF RADIUS Settings for a User Group

These parameters appear only when the following are true. You have configured:

- A AAA client to use one of the RADIUS protocols in Network Configuration.
- Group-level RADIUS attributes on the RADIUS (IETF) page in the Interface Configuration section of the web interface.

RADIUS attributes are sent as a profile for each user from ACS to the requesting AAA client. To display or hide any of these attributes, see [Displaying RADIUS Configuration Options, page 2-7](#). For a list and explanation of RADIUS attributes, see [Appendix B, “RADIUS Attributes.”](#) For more information about how your AAA client uses RADIUS, refer to your AAA client vendor documentation.

To configure IETF RADIUS attribute settings to apply as an authorization for each user in the current group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 3** From the Jump To list at the top of the page, choose **RADIUS (IETF)**.
- Step 4** For each IETF RADIUS attribute you must authorize the current group. Check the check box next to the attribute, and then define the authorization for the attribute in the field or fields next to it.
- Step 5** To save the group settings that you have just made and apply them immediately, click **Submit + Apply**.

**Tip**

To save your group settings and apply them later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 6 To configure the vendor-specific attributes (VSAs) for any RADIUS network device vendor that ACS supports, see the appropriate section:

- [Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group, page 5-28](#)
- [Configuring Cisco Airespace RADIUS Settings for a User Group, page 5-29](#)
- [Configuring Cisco Aironet RADIUS Settings for a User Group, page 5-30](#)
- [Configuring Ascend RADIUS Settings for a User Group, page 5-31](#)
- [Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group, page 5-32](#)
- [Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group, page 5-33](#)
- [Configuring Microsoft RADIUS Settings for a User Group, page 5-34](#)
- [Configuring Nortel RADIUS Settings for a User Group, page 5-36](#)
- [Configuring Juniper RADIUS Settings for a User Group, page 5-37](#)
- [Configuring BBSM RADIUS Settings for a User Group, page 5-38](#)

Step 7 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Cisco IOS/PIX 6.0 RADIUS Settings for a User Group

The Cisco IOS/PIX 6.x RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use RADIUS (Cisco IOS/PIX 6.x) in Network Configuration.
- Group-level RADIUS (Cisco IOS/PIX 6.x) attributes in Interface Configuration: RADIUS (Cisco IOS/PIX 6.x).

Cisco IOS/PIX 6.x RADIUS represents only the Cisco VSAs. You must configure the IETF RADIUS and Cisco IOS/PIX 6.x RADIUS attributes.

**Note**

To hide or display Cisco IOS/PIX 6.x RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have configured no AAA clients of this (vendor) type, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco IOS/PIX 6.x RADIUS attributes to apply as an authorization for each user in the current group:

Step 1 Before you configure Cisco IOS/PIX 6.x RADIUS attributes, you must configure your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).

Step 2 If you want to use the [009\001] `cisco-av-pair` attribute to specify authorizations, check the check box next to the attribute and then type the attribute-value pairs in the text box. Separate each attribute-value pair by pressing **Enter**.

For example, you use the current group for assigning authorizations to Network Admission Control (NAC) clients to which ACS assigns a system posture token of `Infected`, you could specify the following values for the `url-redirect`, `posture-token`, and `status-query-timeout` attributes:

```
url-redirect=http://10.1.1.1
posture-token=Infected
status-query-timeout=150
```

Step 3 If you want to use other Cisco IOS/PIX 6.x RADIUS attributes, check the corresponding check box and specify the required values in the adjacent text box.

Step 4 To save the group settings that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

Step 5 To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Advanced Configuration Options

You use the Advanced Configuration Options section to enable the `cisco-av-pair` for authenticated port mapping.

When you enable the `cisco-av-pair` attribute, the following string is sent to the Cisco IOS/PIX device:

```
aaa:supplicant_name=username_attribute <content of User-Name attribute>
```



Note

The Enable Authenticated Port `cisco-av-pair` check box is ignored when the `cisco-av-pair` has the value `aaa:supplicant_name=` configured on the User level, Group level, or both.

The `cisco-av-pair` attribute for Layer 2 802.1X Authenticated Port Mapping is supported for the Catalyst 6000 devices that are running Cat OS.

Configuring Cisco Airespace RADIUS Settings for a User Group

The Cisco Airespace RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use **RADIUS (Cisco Airespace)** in **Network Configuration**.
- Group-level **RADIUS (Cisco Airespace)** attributes in **Interface Configuration > RADIUS (Cisco-Airespace)**.

Cisco Airespace RADIUS represents only the Cisco VSAs. Interface Configuration will display IETF RADIUS and Cisco IOS/PIX 6.x RADIUS attributes. You must configure the specific attributes manually.



Note

To hide or display Cisco Airespace RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA that is applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco Airespace RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that you have configured your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
ACS cannot allow for partial support of IETF; hence, adding a Cisco Airespace device (into the Network Config) will automatically enable IETF attributes just as adding a Cisco IOS device does.
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco Airespace)**.
- Step 5** In the Cisco Airespace RADIUS Attributes table, set the attributes to authorize for the group by checking the check box next to the attribute. Be certain to define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, "RADIUS Attributes,"](#) or your AAA client documentation.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring Cisco Aironet RADIUS Settings for a User Group

The single Cisco Aironet RADIUS Vendor Specific Attribute (VSA), Cisco-Aironet-Session-Timeout, is a virtual VSA. It is a specialized implementation of the IETF RADIUS `Session-Timeout` attribute (27) that ACS uses only when it responds to a RADIUS request from a AAA client by using RADIUS (Cisco Aironet). You can, therefore, provide different timeout values for users accessing your network through wireless and wired access devices. By specifying a timeout value specifically for WLAN connections, you avoid the conflicts that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes).



Tip

In ACS 3.3, you only enable and configure the `Cisco-Aironet-Session-Timeout` when some or all members of a group connect through wired or wireless access devices. If members of a group always connect with a Cisco Aironet Access Point (AP) or always connect only with a wired access device, you do not need to use `Cisco-Aironet-Session-Timeout`; but you should instead configure RADIUS (IETF) attribute 27, `Session-Timeout`. In ACS 4.0 and later ACS versions, use a network-access profile to create a wireless-specific policy, which makes the Aironet timeout VSA obsolete. Existing configurations will not break because this VSA is supported for those configurations. RACs do not include support for this VSA.

Imagine a user group `Cisco-Aironet-Session-Timeout` set to 600 seconds (10 minutes) and that same user group IETF RADIUS `Session-Timeout` set to 3 hours. When a member of this group connects through a VPN concentrator, ACS uses three hours as the timeout value. However, if that same user connects via a Cisco Aironet AP, ACS responds to an authentication request from the Aironet AP by sending 600

seconds in the IETF RADIUS Session-Timeout attribute. Thus, with the Cisco-Aironet-Session-Timeout attribute configured, different session timeout values can be sent depending on whether the end-user client is a wired access device or a Cisco Aironet AP.

The Cisco-Aironet-Session-Timeout VSA appears on the **Group Setup** page only when the following are true. You have configured:

- A AAA client to use **RADIUS (Cisco Aironet)** in **Network Configuration**.
- Group-level **RADIUS (Cisco Aironet)** attribute in **Interface Configuration > RADIUS (Cisco Aironet)**.



Note

To hide or display the Cisco Aironet RADIUS VSA, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA that is applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients configured to use RADIUS (Cisco Aironet), the VSA settings do not appear in the group configuration interface.

To configure and enable the Cisco Aironet RADIUS attribute to apply as an authorization for each user in the current group:

- Step 1** Confirm that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco Aironet)**.
- Step 5** In the Cisco Aironet RADIUS Attributes table, check the **[5842\001] Cisco-Aironet-Session-Timeout** check box.
- Step 6** In the **[5842\001] Cisco-Aironet-Session-Timeout** box, type the session timeout value (in seconds) that ACS is to send in the IETF RADIUS `Session-Timeout` (27) attribute when you configure the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.
For more information about the IETF RADIUS `Session-Timeout` (27) attribute, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 7** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 8** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Ascend RADIUS Settings for a User Group

The Ascend RADIUS parameters appear only when the following are true. You have configured:

- A AAA client to use RADIUS (Ascend) or RADIUS (Cisco IOS/PIX) in Network Configuration.
- Group-level RADIUS (Ascend) attributes in Interface Configuration: RADIUS (Ascend).

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting for RADIUS is `Ascend-Remote-Addr`.



Note

To hide or display Ascend RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA that is applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Ascend RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that you configured your IETF RADIUS attributes properly. For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
 - Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
 - Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
 - Step 4** From the Jump To list at the top of the page, choose **RADIUS (Ascend)**.
 - Step 5** In the Ascend RADIUS Attributes table, determine the attributes to authorize for the group by checking the check box next to the attribute. Be certain to define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, "RADIUS Attributes,"](#) or your AAA client documentation.
 - Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
 - Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring VPN 3000/ASA/PIX v7.x+ RADIUS Settings for a User Group

To control Microsoft Point-to-Point Encryption (MPPE) settings for users accessing the network through Cisco VPN 3000 concentrators, for example, use the `CVPN3000-PPTP-Encryption (VSA 20)` and `CVPN3000-L2TP-Encryption (VSA 21)` attributes. Settings for `CVPN3000-PPTP-Encryption (VSA 20)` and `CVPN3000-L2TP-Encryption (VSA 21)` override Microsoft MPPE RADIUS settings.

If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000) attributes; regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The VPN 3000/ASA/PIX v7.x+ RADIUS attribute configurations appear only if the following are true. You have configured:

- A AAA client to use RADIUS (Cisco VPN 3000/ASA/PIX v7.x+) in Network Configuration.
- Group-level RADIUS (Cisco VPN 3000/ASA/PIX v7.x+) attributes on the RADIUS (VPN 3000/ASA/PIX v7.x+) page of the Interface Configuration section.

Cisco VPN 3000/ASA/PIX v7.x+ RADIUS represents only the Cisco VPN 3000/ASA/PIX v7.x+ VSAs. You must configure the IETF RADIUS and VPN 3000/ASA/PIX v7.x+ RADIUS attributes.

**Note**

To hide or display VPN 3000/ASA/PIX v7.x+ RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable VPN 3000/ASA/PIX v7.x+VPN 3000/ASA/PIX v7.x+ RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that you properly configured your IETF RADIUS attributes.
- For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
- The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
- The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 3000/ASA/PIX v7.x+)**.
- Step 5** In the Cisco VPN 3000/ASA/PIX v7.x+ RADIUS Attributes table, determine the attributes to authorize for the group by checking the check box next to the attribute. Further define the authorization for that attribute in the field next to it.
- For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.
- Step 6** To save the group settings that you have just made, click **Submit**.
- For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring Cisco VPN 5000 Concentrator RADIUS Settings for a User Group

The Cisco VPN 5000 Concentrator RADIUS attribute configurations appear only when the following are true. You have configured:

- A network device to use RADIUS (Cisco VPN 5000) in Network Configuration.
- Group-level RADIUS (Cisco VPN 5000) attributes on the RADIUS (Cisco VPN 5000) page of the Interface Configuration section.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.

**Note**

To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that your IETF RADIUS attributes are configured properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Cisco VPN 5000)**.
- Step 5** In the Cisco VPN 5000 Concentrator RADIUS Attributes table, choose the attributes that should be authorized for the group by checking the check box next to the attribute. Further define the authorization for each attribute in the field next to it.
For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that use RADIUS.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring Microsoft RADIUS Settings for a User Group

Microsoft RADIUS provides VSAs that support MPPE, which encrypts PPP links. These PPP connections can be via a dial-in line or over a VPN tunnel.

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, for example, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX v7.x+) attributes; regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The Microsoft RADIUS attribute configurations appear only when the following are true. You have configured:

- A network device in Network Configuration that uses a RADIUS protocol that supports the Microsoft RADIUS VSA.

- Group-level Microsoft RADIUS attributes on the RADIUS (Microsoft) page of the Interface Configuration section.

The following ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX v7.x+
- Ascend
- Cisco Airespace

Microsoft RADIUS represents only the Microsoft VSA. You must configure the IETF RADIUS and Microsoft RADIUS attributes.



Note

To hide or display Microsoft RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Microsoft RADIUS attributes to apply as an authorization for each user in the current group:

- Step 1** Confirm that your IETF RADIUS attributes are configured properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Microsoft)**.
- Step 5** In the Microsoft RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices by using RADIUS.



Note

The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.

- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Nortel RADIUS Settings for a User Group

The Nortel RADIUS attribute configurations appear only when the following are true. You have configured:


- A network device in Network Configuration that uses a RADIUS protocol that supports the Nortel RADIUS VSA.
- Group-level Nortel RADIUS attributes on the RADIUS (Nortel) page of the Interface Configuration section.

Nortel RADIUS represents only the Nortel VSA. You must configure the IETF RADIUS and Nortel RADIUS attributes.

**Note**

To hide or display Nortel RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Nortel RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that your IETF RADIUS attributes are configured properly.
- For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
- The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
- The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (Nortel)**.
- Step 5** In the Nortel RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.
-
-  **Note** ACS autogenerates the MS-CHAP-MPPE-Keys attribute value; there is no value to set in the web interface.
-
- Step 6** To save the group settings that you have just made, click **Submit**.
- For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.
-

Configuring Juniper RADIUS Settings for a User Group


Juniper RADIUS represents only the Juniper VSA. You must configure the IETF RADIUS and Juniper RADIUS attributes.



Note

To hide or display Juniper RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable Juniper RADIUS attributes to apply as an authorization for each user in the current group:

- Step 1** Confirm that you configured your IETF RADIUS attributes properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
 - Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
 - Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
 - Step 4** From the Jump To list at the top of the page, choose **RADIUS (Juniper)**.
 - Step 5** In the Juniper RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.
- 

Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
 - Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring 3COMUSR RADIUS Settings for a User Group

3COMUSR RADIUS represents only the 3COMUSR VSA. You must configure the IETF RADIUS and 3COMUSR RADIUS attributes.

The 3COMUSR VSA format differs from other VSAs in that 3COMUSR VSAs have a 32-bit extended Vendor-Type field and no length field.




Note

3Com/USR VSAs should be used for any device that uses these VSAs, not just the HiperARC cards.

To hide or display 3COMUSR RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable 3COMUSR RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that you configured your IETF RADIUS attributes properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 3** From the Group list, select a group, and then click **Edit Settings**.
The name of the group appears at the top of the Group Settings page.
- Step 4** From the Jump To list at the top of the page, choose **RADIUS (3COMUSR)**.
- Step 5** In the 3COMUSR RADIUS Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.
-  **Note** The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.
-
- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring BBSM RADIUS Settings for a User Group

BBSM RADIUS represents only the BBSM RADIUS VSA. You must configure the IETF RADIUS and BBSM RADIUS attributes.



- Note** To hide or display BBSM RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular group persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the group configuration interface.

To configure and enable BBSM RADIUS attributes to apply as an authorization for each user in the current group:

-
- Step 1** Confirm that you configured your IETF RADIUS attributes properly.
For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).
- Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

- Step 3** From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

- Step 4** From the Jump To list at the top of the page, choose **RADIUS (BBSM)**.

- Step 5** In the BBSM RADIUS Attributes table, specify the attribute to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.



Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.

- Step 6** To save the group settings that you have just made, click **Submit**.

For more information, see [Saving Changes to User Group Settings, page 5-41](#).

- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Configuring Custom RADIUS VSA Settings for a User Group

User-defined, custom Radius VSA configurations appear only when all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#).)
- You have configured a network device in Network Configuration that uses a RADIUS protocol that supports the custom VSA.
- You have configured group-level custom RADIUS attributes on the RADIUS (*Name*) page of the Interface Configuration section.

You must configure the IETF RADIUS and the custom RADIUS attributes.

To configure and enable custom RADIUS attributes to apply as an authorization for each user in the current group:

- Step 1** Confirm that you configured your IETF RADIUS attributes properly.

For more information about setting IETF RADIUS attributes, see [Configuring IETF RADIUS Settings for a User Group, page 5-27](#).

- Step 2** In the navigation bar, click **Group Setup**.

The Group Setup Select page opens.

- Step 3** From the Group list, select a group, and then click **Edit Settings**.

The name of the group appears at the top of the Group Settings page.

- Step 4** From the Jump To list at the top of the page, choose **RADIUS (*custom name*)**.

- Step 5** In the RADIUS (*custom name*) Attributes table, specify the attributes to authorize for the group by checking the check box next to the attribute. Where applicable, further define the authorization for that attribute in the field next to it. For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or the documentation for network devices that are using RADIUS.



Note The MS-CHAP-MPPE-Keys attribute value is autogenerated by ACS; there is no value to set in the web interface.

- Step 6** To save the group settings that you have just made, click **Submit**.
For more information, see [Saving Changes to User Group Settings, page 5-41](#).
- Step 7** To continue specifying other group settings, perform other procedures in this chapter, as applicable.

Group Setting Management

This section describes how to use the **Group Setup** section to perform a variety of managerial tasks.

This section contains:

- [Listing Users in a User Group, page 5-40](#)
- [Resetting Usage Quota Counters for a User Group, page 5-40](#)
- [Renaming a User Group, page 5-41](#)
- [Saving Changes to User Group Settings, page 5-41](#)

Listing Users in a User Group

To list all users in a specified group:

- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group.
- Step 3** Click **Users in Group**.
The User List page for the particular group that you selected opens in the display area.
- Step 4** To open a user account (to view, modify, or delete a user), click the name of the user in the User List.
The User Setup page for the particular user account selected appears.

Resetting Usage Quota Counters for a User Group

You can reset the usage quota counters for all members of a group, before or after a quota has been exceeded.

To reset usage quota counters for all members of a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group and click **Edit Settings**.
- Step 3** In the Usage Quotas section, check the **On submit reset all usage counters for all users of this group** check box.
- Step 4** Click **Submit** at the bottom of the browser page.
The usage quota counters for all users in the group are reset. The Group Setup Select page appears.
-

Renaming a User Group

To rename a user group:

-
- Step 1** In the navigation bar, click **Group Setup**.
The Group Setup Select page opens.
- Step 2** From the Group list, choose the group.
- Step 3** Click **Rename Group**.
The Renaming Group: *Group Name* page appears.
- Step 4** Type the new name in the **Group** field. Group names cannot contain angle brackets (< >).
- Step 5** Click **Submit**.



Note The group remains in the same position in the list. The number value of the group is still associated with this group name. Some utilities, such as the database import utility, use the numeric value that is associated with the group.

The Select page opens with the new group name selected.

Saving Changes to User Group Settings

After you have completed configuration for a group, you must save your work.

To save the configuration for the current group:

-
- Step 1** To save your changes and apply them immediately, click **Submit + Apply**. This action restarts ACS services and applies the changes.
You can click only the **Submit** button if you do not want to affect your network with a restart.
- Step 2** To save your changes and apply them later, click **Submit**. When you are ready to implement the changes, choose **System Configuration > Service Control**. Then, choose **Restart**.
The group attributes are applied and services are restarted. The Edit page opens.

**Note**

Restarting the service clears the Logged-in User Report and temporarily interrupts all ACS services. This action affects the Max Sessions counter.

Step 3 To verify that your changes were applied, choose the group and click **Edit Settings**. View the settings.



CHAPTER 6

User Management

This chapter contains information about setting up and managing user accounts in the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

This chapter contains:

- [About User Setup Features and Functions, page 6-1](#)
- [About User Databases, page 6-2](#)
- [Basic User Setup Options, page 6-2](#)
- [Advanced User Authentication Settings, page 6-15](#)
- [User Management, page 6-37](#)



Caution

Settings at the user level override settings that you configured at the group level.

Before you configure User Setup, you should understand how this section functions. ACS dynamically builds the User Setup section interface depending on the configuration of your Authentication, Authorization, and Accounting (AAA) client and the security protocols that you use. That is, what you see under User Setup is affected by settings in the Network Configuration and Interface Configuration sections.

About User Setup Features and Functions

The User Setup section of the ACS web interface is the centralized location for all operations regarding user account configuration and administration.

From within the User Setup section, you can:

- View a list of all users in the ACS internal database.
- Find a user.
- Add a user.
- Assign the user to a group, including Voice-over-IP (VoIP) groups.
- Edit user account information.
- Establish or change user authentication type.
- Configure callback information for the user.
- Set network-access restrictions (NARs) for the user.

- Configure Advanced Settings.
- Set the maximum number of concurrent sessions (Max Sessions) for the user.
- Disable or reenable the user account.
- Delete the user.

About User Databases

ACS authenticates users against one of several possible databases, including its ACS internal database. Regardless of which database that you configure ACS to use when authenticating a user, all users have accounts within the ACS internal database, and authorization of users is always performed against the user records in the ACS internal database. The following list details the basic user databases that are used and provides links to greater details on each:

- **ACS internal database**—Authenticates a user from the local ACS internal database. For more information, see [ACS Internal Database, page 12-1](#).



Tip

The following authentication types appear in the web interface only when the corresponding external user database has been configured in the Database Configuration area of the External User Databases section.

- **Windows Database**—Authenticates a user with an existing account in the Windows user database in the local domain or in domains that you configure in the Windows user database. For more information, see [Windows User Database, page 12-5](#).
- **Generic LDAP**—Authenticates a user from a Generic LDAP external user database (including Network. Directory Services (NDS) users). For more information, see [Generic LDAP, page 12-23](#).
- **ODBC Database (ACS for Windows only)**—Authenticates a user from an Open Database Connectivity-compliant database server. For more information, see [ODBC Database \(ACS for Windows Only\), page 12-35](#).
- **LEAP Proxy RADIUS Server Database**—Authenticates a user from a Lightweight and Efficient Application Protocol (LEAP) Proxy Remote Access Dial-In User Service (RADIUS) server. For more information, see [LEAP Proxy RADIUS Server Database \(Both Platforms\), page 12-48](#).
- **Token Server**—Authenticates a user from a token server database. ACS supports the use of a variety of token servers for the increased security that one-time passwords provide. For more information, see [Token Server User Databases, page 12-50](#).

Basic User Setup Options

This section presents the basic tasks that you perform when configuring a new user. At its most basic level, configuring a new user requires only three steps:

-
- | | |
|--------|--|
| Step 1 | Specify a name. |
| Step 2 | Specify an external user database or a password. |
| Step 3 | Submit the information. |

The steps for editing user account settings are nearly identical to those used when adding a user account; but, to edit, you navigate directly to the field or fields to change. You cannot edit the name that is associated with a user account. To change a username, you must delete the user account and establish another.

What other procedures that you perform when setting up new user accounts is a function of the complexity of your network and of the granularity of control that you want.

This section contains:

- [Adding a Basic User Account, page 6-3](#)
- [Setting Supplementary User Information, page 6-4](#)
- [Setting a Separate CHAP/MS-CHAP/ARAP Password, page 6-5](#)
- [Assigning a User to a Group, page 6-5](#)
- [Setting the User Callback Option, page 6-6](#)
- [Assigning a User to a Client IP Address, page 6-7](#)
- [Setting Network Access Restrictions for a User, page 6-8](#)
- [Setting Max Sessions Options for a User, page 6-11](#)
- [Options for Setting User Usage Quotas, page 6-12](#)
- [Setting Options for User Account Disablement, page 6-13](#)
- [Assigning a Time Bound Alternate Group, page 6-14](#)
- [Assigning a Downloadable IP ACL to a User, page 6-14](#)

Adding a Basic User Account

This procedure details the minimum steps necessary to add a new user account to the ACS internal database.

To add a user account:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page opens.

Step 2 Type a name in the **User** box.



Note The username can contain up to 64 characters. Names cannot contain the pound sign (#), the question mark (?), the quote ("), the asterisk (*), the right angle bracket (>), or the left angle bracket (<). Leading and trailing spaces are not allowed.

Step 3 Click **Add/Edit**.

The User Setup Edit page opens. The username that you are adding appears at the top of the page.

Step 4 Ensure that you uncheck the **Account Disabled** check box.



Note Alternatively, you can check the **Account Disabled** check box to create a user account that is disabled, and enable the account at another time.

- Step 5** Under Password Authentication in the User Setup table, select the applicable authentication type from the list.



Tip The authentication types that appear reflect the databases that you have configured in the Database Configuration area of the External User Databases section.

- Step 6** Enter a single ACS Password Authentication Protocol (PAP) password by typing it in the first set of **Password** and **Confirm Password** boxes.



Note Up to 32 characters are allowed each for the **Password** box and the **Confirm Password** box.



Tip The ACS PAP password is also used for CHAP/MS-CHAP/ARAP if you do not check the **Separate CHAP/MS-CHAP/ARAP** check box.



Tip You can configure the AAA client to ask for a PAP password first and then a Challenge Authentication Handshake Protocol (CHAP) or Microsoft-Challenge Authentication Handshake Protocol (MS-CHAP) password; so that, when users dial in by using a PAP password, they will authenticate. For example, the following line in the AAA client configuration file causes the AAA client to enable CHAP after PAP: **ppp authentication pap chap**

- Step 7** Do one:
- Finish configuring the user account options and establish the user account, click **Submit**.
 - Continue to specify the user account options, perform other procedures in this chapter, as applicable.



Tip For lengthy account configurations, you can click **Submit** before continuing. This action will prevent loss of information that you already entered if an unforeseen problem occurs.

Setting Supplementary User Information

Supplementary User Information can contain up to five fields that you configure. The default configuration includes two fields: Real Name and Description. For information about how to display and configure these optional fields, see [Customizing User Data, page 2-5](#).

To enter optional information into the Supplementary User Information table:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Complete each box that appears in the Supplementary User Info table.



Note Up to 128 characters are allowed each for the **Real Name** and the **Description** boxes.

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.

Setting a Separate CHAP/MS-CHAP/ARAP Password

Setting a separate CHAP/MS-CHAP/ARAP password adds more security to ACS authentication. However, you must have an AAA client configured to support the separate password.

To allow the user to authenticate by using a CHAP, MS-CHAP, or AppleTalk Remote Access Protocol (ARAP) password, instead of the PAP password in the ACS internal database:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Select the **Separate CHAP/MS-CHAP/ARAP** check box in the User Setup table.
- Step 3** Enter the CHAP/MS-CHAP/ARAP password to use by typing it in each of the second set of **Password** or **Confirm** boxes under the **Separate (CHAP/MS-CHAP/ARAP)** check box.



Note Up to 32 characters are allowed each for the **Password** box and the **Confirm Password** box.



Note These **Password** and **Confirm Password** boxes are only required for authentication by the ACS database. Additionally, if you assign a user to a VoIP (null password) group, and the optional password is also included in the user profile, the password is not used until the user is remapped to a non-VoIP group.

- Step 4** Do one:
- If you are finished configuring the user account options, click **Submit** to record the options.
 - To continue to specify the user account options, perform procedures in this chapter, as applicable.


Assigning a User to a Group

A user can only belong to one group in ACS. The user inherits the attributes and operations that are assigned to his or her group. However, in the case of conflicting settings, the settings at the user level override the settings that you configure at the group level.

By default, users are assigned to the Default Group. Users who authenticate via the Unknown User method and who are not mapped to an existing ACS group are also assigned to the Default Group.

Alternatively, you can choose not to map a user to a particular group; but instead, to have the group mapped by an external authenticator. For external user databases from which ACS can derive group information, you can associate the group memberships—defined for the users in the external user database—to specific ACS groups. For more information, see [Chapter 16, “User Group Mapping and Specification.”](#)



To assign a user to a group:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** From the Group to which user is assigned list in the User Setup table, select the group to which to assign the user.
-  **Tip** Alternatively, you can scroll up in the list to select the **Mapped By External Authenticator** option.
-
- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting the User Callback Option

Callback is a command string that is passed to the access server. You can use a callback string to initiate a modem to call the user back on a specific number for added security or reversal of line charges.

To set the user callback option:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Under Callback in the User Setup table, select the applicable option. Choices include:
- **Use group setting**—Click if you want this user to use the setting for the group.
 - **No callback allowed**—Click to disable callback for this user.
 - **Callback using this number**—Click and type the complete number, including area code if necessary, on which to always call back this user.
-  **Note** The maximum length for the callback number is 199 characters.
-
- **Dialup client specifies callback number**—Click to enable the Windows dialup client to specify the callback number.
 - **Use Windows Database callback settings**—Click to use the settings specified for Windows callback. If a Windows account for a user resides in a remote domain, the domain in which ACS resides must have a two-way trust with that domain for the Microsoft Windows callback settings to operate for that user.
-  **Note** The dial-in user must have configured Windows software that supports callback.
-

**Note**

If you enable the Windows Database callback settings, the Windows Callback feature must also be enabled in the Windows Database Configuration Settings. See [Windows User Database Configuration Options, page 12-18](#).

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.

Assigning a User to a Client IP Address

To assign a user to a client IP address:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Under **Client IP Address Assignment** in the User Setup table, select the applicable option. Choices include:

**Note**

The IP address assignment in User Setup overrides the IP address assignment in Group Setup.

- **Use group settings**—Click this option to use the IP address group assignment.
- **No IP address assignment**—Click this option to override the group setting if you do not want an IP address returned by the client.
- **Assigned by dialup client**—Click this option to use the IP address dialup client assignment.
- **Assign static IP address**—Click this option and type the IP address in the box (up to 15 characters), if a specific IP address should be used for this user.

**Note**

If the IP address is being assigned from a pool of IP addresses or by the dialup client, leave the **Assign static IP address** box blank.

- **Assigned by AAA client pool**—Click this option and type the AAA client IP pool name in the box, if this user is to have the IP address assigned by an IP address pool that is configured on the AAA client.
 - **Assigned from AAA pool**—Click this option and type the applicable pool name in the box, if this user is to have the IP address that is assigned by an IP address pool configured on the AAA server. Select the AAA server IP pool name from the **Available Pools** list, and then click --> (right arrow button) to move the name into the **Selected Pools** list. If the **Selected Pools** list contains more than one pool, the users in this group are assigned to the first available pool in the order listed. To move the position of a pool in the list, select the pool name, and click **Up** or **Down** until the pool is in the position that you want.
- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.

Setting Network Access Restrictions for a User

You use the Network Access Restrictions table in the Advanced Settings area of User Setup to set NARs in three ways:

- Apply existing shared NARs by name.
- Define IP-based access restrictions to permit or deny user access to a specified AAA client or to specified ports on an AAA client when an IP connection has been established.
- Define calling line ID/Dialed Number Identification Service (CLI/DNIS)-based access restrictions to permit or deny user access based on the CLI/DNIS that is used.



Note

You can also use the CLI/DNIS-based access restrictions area to specify other values. For more information, see [Network Access Restrictions, page 4-18](#).

Typically, you define (shared) NARs from within the Shared Components section so that you can apply these restrictions to more than one group or user. For more information, see [Adding a Shared NAR, page 4-21](#). You must have selected the **User-Level Network Access Restrictions** check box on the Advanced Options page of the Interface Configuration section for this set of options to appear in the web interface.

However, you can also use ACS to define and apply a NAR for a single user from within the User Setup section. You must have enabled the **User-Level Network Access Restrictions** setting on the Advanced Options page of the Interface Configuration section for single user IP-based filter options and single user CLI/DNIS-based filter options to appear in the web interface.



Note

When an authentication request is forwarded by proxy to an ACS, any NARs for Terminal Access Controller Access Control System (TACACS+) requests are applied to the IP address of the forwarding AAA server, not to the IP address of the originating AAA client.

When you create access restrictions on a per-user basis, ACS does not enforce limits to the number of access restrictions nor does it enforce a limit to the length of each access restriction; however, there are strict limits:

- The combination of fields for each line item cannot exceed 1024 characters in length.
- The shared NAR cannot have more than 16 KB of characters. The number of line items supported depends on the length of each line item. For example, if you create a CLI/DNIS-based NAR where the AAA client names are 10 characters, the port numbers are 5 characters, the CLI entries are 15 characters, and the DNIS entries are 20 characters, you can add 450 line items before reaching the 16 KB limit.

To set NARs for a user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** To apply a previously configured shared NAR to this user:



Note To apply a shared NAR, you must configure it under Network Access Restrictions in the Shared Profile Components section. For more information, see [Adding a Shared NAR, page 4-21](#).

- a. Check the **Only Allow network access when** check box.
- b. To specify whether one or all shared NARs must apply for the user to be permitted access, select one, as applicable:
 - All selected NARS result in permit.
 - Any one selected NAR results in permit.
- c. Select a shared NAR name in the NARs list, and then click --> (right arrow button) to move the name into the Selected NARs list.



Tip To view the server details of the shared NARs you have selected to apply, you can click **View IP NAR** or **View CLID/DNIS NAR**, as applicable.

Step 3 To define and apply a NAR, for this particular user, that permits or denies this user access based on IP address, or IP address and port:



Tip You should define most NARs from within the Shared Components section so that you can apply them to more than one group or user. For more information, see [Adding a Shared NAR, page 4-21](#).

- a. In the Network Access Restrictions table, under Per User Defined Network Access Restrictions, check the **Define IP-based access restrictions** check box.
- b. To specify whether the subsequent listing specifies permitted or denied IP addresses, from the Table Defines list, select one:
 - **Permitted Calling/Point of Access Locations**
 - **Denied Calling/Point of Access Locations**
- c. Select or enter the information in the following boxes:
 - **AAA Client**—Select **All AAA Clients**, or the name of a network device group (NDG), or the name of the individual AAA client, to which to permit or deny access.
 - **Port**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports on the selected AAA client.
 - **Address**—Type the IP address or addresses to use when performing access restrictions. You can use the asterisk (*) as a wildcard.



Note The total number of characters in the AAA Client list, and the Port and Src IP Address boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

- d. Click **Enter**.

The specified AAA client, port, and address information appears in the table above the AAA Client list.

Step 4 To permit or deny this user access based on calling location or values other than an established IP address:

- a. Check the **Define CLI/DNIS based access restrictions** check box.
- b. To specify whether the subsequent listing specifies permitted or denied values, from the Table Defines list, select one:
 - **Permitted Calling/Point of Access Locations**
 - **Denied Calling/Point of Access Locations**
- c. Complete the following boxes:



Note You must make an entry in each box. You can use the asterisk (*) as a wildcard for all or part of a value. The format that you use must match the format of the string that you receive from your AAA client. You can determine this format from your RADIUS Accounting Log.

- **AAA Client**—Select **All AAA Clients**, or the name of the NDG, or the name of the individual AAA client, to which to permit or deny access.
- **PORT**—Type the number of the port to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access to all ports.
- **CLI**—Type the CLI number to which to permit or deny access. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number.



Tip Use the CLI entry if you want to restrict access based on other values such as a Cisco Aironet client MAC address. For more information, see [About Network Access Restrictions, page 4-18](#).

- **DNIS**—Type the DNIS number to which to permit or deny access. Use this entry to restrict access based on the number into which the user will be dialing. You can use the asterisk (*) as a wildcard to permit or deny access based on part of the number.



Tip Use the DNIS selection if you want to restrict access based on other values such as a Cisco Aironet AP MAC address. For more information, see [About Network Access Restrictions, page 4-18](#).



Note The total number of characters in the AAA Client list and the **Port**, **CLI**, and **DNIS** boxes must not exceed 1024. Although ACS accepts more than 1024 characters when you add a NAR, you cannot edit the NAR and ACS cannot accurately apply it to users.

- d. Click **enter**.

The information, specifying the AAA client, port, CLI, and DNIS, appears in the table above the AAA Client list.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting Max Sessions Options for a User

You use the Max Sessions feature to set the maximum number of simultaneous connections permitted for this user. For ACS purposes, a session is considered any type of user connection RADIUS or TACACS+ supports, for example Point-to-Point Protocol (PPP), or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for ACS to be aware of a session. All session counts are based on user and group names only. ACS does not support any differentiation by type of session—all sessions are counted as the same. To illustrate, a user with a Max Session count of 1 who is dialed in to an AAA client with a PPP session will be refused a connection if that user then tries to Telnet to a location whose access is controlled by the same ACS.



Note

Each ACS holds its own Max Sessions counts. There is no mechanism for ACS to share Max Sessions counts across multiple ACSs. Therefore, if two ACSs are set up as a mirror pair with the workload distributed between them, they will have completely independent views of the Max Sessions totals.



Tip

If the Max Sessions table does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Max Sessions** check box.

To set max sessions options for a user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** In the Max Sessions table, under Sessions available to user, select one:
 - **Unlimited**—Select to allow this user an unlimited number of simultaneous sessions. (This effectively disables Max Sessions.)
 - *n*—Select and then type the maximum number of simultaneous sessions to allow this user.
 - **Use group setting**—Select to use the Max Sessions value for the group.



Note

The default setting is Use group setting.



Note

User Max Sessions settings override the group Max Sessions settings. For example, if the group Sales has a Max Sessions value of only 10, but a user in the group Sales, John, has a User Max Sessions value of Unlimited, John is still allowed an unlimited number of sessions.

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.

Options for Setting User Usage Quotas

You can define usage quotas for individual users. You can limit users by the:

- Duration of sessions for the period selected.
- Number of sessions for the period selected.

For ACS purposes, a session is considered any type of user connection the RADIUS or TACACS+ supports, for example PPP, or Telnet, or ARAP. Note, however, that accounting must be enabled on the AAA client for ACS to be aware of a session. If you make no selections in the Session Quotas section for an individual user, ACS applies the session quotas of the group to which the user is assigned.



Note

If the User Usage Quotas feature does not appear, choose **Interface Configuration > Advanced Options**. Then check the **Usage Quotas** check box.



Tip

The Current Usage table under the User Usage Quotas table on the User Setup Edit page displays usage statistics for the current user. The Current Usage table lists online time and sessions used by the user, with columns for daily, weekly, monthly, and total usage. The Current Usage table appears only on user accounts that you have established; that is, it does not appear during initial user setup.

For a user who has exceeded his quota, ACS denies him access on his next attempt to start a session. If a quota is exceeded during a session, ACS allows the session to continue. If a user account has been disabled because the user has exceeded usage quotas, the User Setup Edit page displays a message stating that the account has been disabled for this reason.

You can reset the session quota counters on the User Setup page for a user. For more information about resetting usage quota counters, see [Resetting User Session Quota Counters, page 6-39](#).

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off. If the AAA client through which the user is accessing your network fails, the quota is not updated. In the case of multiple sessions, such as with ISDN, the quota is not updated until all sessions terminate, which means that a second channel will be accepted; even if the first channel has exhausted the quota that is allocated to the user.

To set usage quota options for a user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** In the Usage Quotas table, select **Use these settings**.
- Step 3** To define a usage quota based on duration of sessions for a user:
 - a. Check the **Limit user to x hours of online time** check box.
 - b. Type the number of hours to which you want to limit the user in the **Limit user to x hours of online time** box. Use decimal values to indicate minutes. For example, a value of 10.5 would equal 10 hours and 30 minutes. This field can contain up to 10 characters.
 - c. Select the period for which you want to enforce the time usage quota:
 - **per Day**—From 12:01 a.m. until midnight.
 - **per Week**—From 12:01 a.m. Sunday until midnight Saturday.

- **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
 - **Absolute**—A continuous, open-ended count of hours.
- Step 4** To define usage quotas based on the number of sessions for a user:
- a. Check the **Limit user to x sessions** check box.
 - b. Type the number of sessions to which you want to limit the user in the **Limit user to x sessions** box. Up to 10 characters are allowed for this field.
 - c. Select the period for which you want to enforce the session usage quota:
 - **per Day**—From 12:01 a.m. until midnight.
 - **per Week**—From 12:01 a.m. Sunday until midnight Saturday.
 - **per Month**—From 12:01 a.m. on the first of the month until midnight on the last day of the month.
 - **Absolute**—A continuous, open-ended count of hours.
- Step 5** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 6** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Options for User Account Disablement

The Account Disable feature defines the circumstances under which a user account is disabled.



Note

Do not confuse this feature with account expiration due to password aging. Password aging is defined for groups only, not for individual users. This feature is distinct from the **Account Disabled** check box. For instructions on how to disable a user account, see [Disabling a User Account, page 6-38](#).



Note

If the user is authenticated with a Windows user database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings configured in Windows.

To set options for user account disablement:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Do one:
- a. Select the **Never** option to keep the user account always enabled. This is the default.
 - b. Select the **Disable account if** option to disable the account under specific circumstances. Then, specify one or both of the circumstances under the following boxes:
 - **Date exceeds**—Check the **Date exceeds** check box. Then select the month and type the date (two characters) and year (four characters) on which to disable the account. The default is 30 days after the user is added.

- **Failed attempts exceed**—Check the **Failed attempts exceed** check box and then type the number of consecutive unsuccessful login attempts to allow before disabling the account. The default is 5.

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Assigning a Time Bound Alternate Group

This feature can be used to designate another user as an alternate administrator. The alternate administrator has administrative privileges within the boundaries set by a start date, end date, and time limits.

To configure an alternate administrator:

-
- Step 1** Check the **Enable Time Bound Alternate Group** check box.
- Step 2** Select the month and enter the date and year. for the **Start Date**
- Step 3** Enter the **Time** (hh:mm) at which the alternate administrator gains privilege.
- Step 4** Select the month and enter the date and year for the **End Date**.
- Step 5** Enter the time (hh:mm) at which the alternate administrator relinquishes administrative privileges.
- Step 6** Select the **Alternate Group** to which administrative privilege will be granted. from the drop down list.
- Step 7** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 8** If you are finished configuring the user account options, click **Submit** to record the options.
-

Assigning a Downloadable IP ACL to a User

You can use the Downloadable ACLs feature to assign an IP Access Control List (ACL) at the user level. You must configure one or more IP ACLs before you assign one. For instructions on how to configure a downloadable IP ACL by using the Shared Profile Components section of the ACS web interface, see [Adding a Downloadable IP ACL, page 4-15](#).



Note

The Downloadable ACLs table does not appear if it has not been enabled. To enable the Downloadable ACLs table, click **Interface Configuration > Advanced Options**, and then check the **User-Level Downloadable ACLs** check box.

To assign a downloadable IP ACL to a user account:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username being added and edited is at the top of the page.
- Step 2** Under the Downloadable ACLs section, click the **Assign IP ACL:** check box.

- Step 3** Select an IP ACL from the list.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Advanced User Authentication Settings

This section presents the activities that you perform to configure user-level TACACS+ and RADIUS enable parameters.

This section contains:

- [TACACS+ Settings \(User\), page 6-15](#)
 - [Configuring TACACS+ Settings for a User, page 6-16](#)
 - [Configuring a Shell Command Authorization Set for a User, page 6-17](#)
 - [Configuring a PIX Command Authorization Set for a User, page 6-19](#)
 - [Configuring Device-Management Command Authorization for a User, page 6-20](#)
 - [Configuring the Unknown Service Setting for a User, page 6-21](#)
- [Advanced TACACS+ Settings for a User, page 6-21](#)
 - [Setting Enable Privilege Options for a User, page 6-22](#)
 - [Setting TACACS+ Enable Password Options for a User, page 6-23](#)
 - [Setting TACACS+ Outbound Password for a User, page 6-24](#)
- [RADIUS Attributes, page 6-24](#)
 - [Setting IETF RADIUS Parameters for a User, page 6-25](#)
 - [Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User, page 6-26](#)
 - [Setting Cisco Airespace RADIUS Parameters for a User, page 6-27](#)
 - [Setting Cisco Aironet RADIUS Parameters for a User, page 6-27](#)
 - [Setting Ascend RADIUS Parameters for a User, page 6-29](#)
 - [Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User, page 6-29](#)
 - [Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 6-30](#)
 - [Setting Microsoft RADIUS Parameters for a User, page 6-31](#)
 - [Setting Nortel RADIUS Parameters for a User, page 6-33](#)
 - [Setting Juniper RADIUS Parameters for a User, page 6-33](#)
 - [Setting BBSM RADIUS Parameters for a User, page 6-35](#)
 - [Setting Custom RADIUS Attributes for a User, page 6-36](#)

TACACS+ Settings (User)

You can use TACACS+ Settings section to enable and configure the service and protocol parameters to apply for the authorization of a user.

This section contains:

- [Configuring TACACS+ Settings for a User, page 6-16](#)
- [Configuring a Shell Command Authorization Set for a User, page 6-17](#)
- [Configuring a PIX Command Authorization Set for a User, page 6-19](#)
- [Configuring Device-Management Command Authorization for a User, page 6-20](#)
- [Configuring the Unknown Service Setting for a User, page 6-21](#)

Configuring TACACS+ Settings for a User

You can use this procedure to configure TACACS+ settings at the user level for the following services and protocols:

- PPP IP
- PPP IPX
- PPP Multilink
- PPP Apple Talk
- PPP VPDN
- PPP LCP
- ARAP
- Shell (exec)
- Project Information Exchange (PIX) PIX Shell (pixShell)
- Serial Line Internet Protocol (SLIP)

You can also enable any *new* TACACS+ services that you configure. Because having all service/protocol settings appear within the User Setup section would be cumbersome, you choose what settings to hide or display at the user level when you configure the interface. For more information about setting up new or existing TACACS+ services in the ACS web interface, see [Displaying TACACS+ Configuration Options, page 2-6](#).

If you have configured ACS to interact with a Cisco device-management application, new TACACS+ services may appear automatically, as needed, to support the device-management application. For more information about ACS interaction with device-management applications, see [Support for Cisco Device-Management Applications, page 1-14](#).


For more information about attributes, see [Appendix A, “TACACS+ Attribute-Value Pairs,”](#) or your AAA client documentation. For information on assigning an IP ACL, see [Assigning a Downloadable IP ACL to a User, page 6-14](#).

Before You Begin

- For the TACACS+ service/protocol configuration to appear, you must configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.

To configure TACACS+ settings for a user:

-
- Step 1** Click **Interface Configuration > TACACS+ (Cisco IOS)**. In the TACACS+ Services table, under the heading User, ensure that the check box is selected for each service/protocol that you want to configure.

- Step 2** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 3** Scroll down to the TACACS+ Settings table and select the bold service name check box to enable that protocol; for example **PPP IP**.
- Step 4** To enable specific parameters within the selected service, Check the check box next to a specific parameter and then do one of the following, as applicable:
- Check the **Enabled** check box.
 - Enter a value in the corresponding attribute box.
- To specify ACLs and IP address pools, enter the name of the ACL or pool as defined on the AAA client. Leave the box blank if the default (as defined on the AAA client) should be used. For more information about attributes, see [Appendix A, “TACACS+ Attribute-Value Pairs,”](#) or your AAA client documentation. For information on assigning a IP ACL, see [Assigning a Downloadable IP ACL to a User, page 6-14](#).
-  **Tip** An ACL is a list of Cisco IOS commands that you use to restrict access to or from other devices and users on the network.
- Step 5** To employ custom attributes for a particular service, check the **Custom attributes** check box under that service, and then enter the attribute and value in the box below the check box.
- Step 6** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 7** If you are finished configuring the user account options, click **Submit** to record the options.

Configuring a Shell Command Authorization Set for a User

Use this procedure to specify the shell command-authorization set parameters for a user. You can choose:

- **None**—No authorization for shell commands.
- **Group**—The group-level shell command-authorization set applies for this user.
- **Assign a Shell Command Authorization Set for any network device**—One shell command-authorization set is assigned, and it applies all network devices.
- **Assign a Shell Command Authorization Set on a per Network Device Group Basis**—Particular shell command-authorization sets will be effective on particular NDGs. When you select this option, you create the table that lists what NDG associates with what shell command-authorization set.
- **Per User Command Authorization**—Permits or denies specific Cisco IOS commands and arguments at the user level.

Before You Begin

- Ensure that you configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In the TACACS+ (Cisco) section of Interface Configuration, ensure that the Shell (exec) option is selected in the User column.

- Ensure that you have already configured one or more shell command-authorization sets. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

To specify shell command-authorization set parameters for a user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Scroll down to the TACACS+ Settings table and to the Shell Command Authorization Set feature area within it.
- Step 3** To prevent the application of any shell command-authorization set, click (or accept the default of) the **None** option.
- Step 4** To assign the shell command-authorization set at the group level, select the **As Group** option.
- Step 5** To assign a particular shell command-authorization set to be effective on any configured network device:
- Select the **Assign a Shell Command Authorization Set for any network device** option.
 - Then, from the list directly below that option, select the shell command-authorization set that you want to apply to this user.
- Step 6** To create associations that assign a particular shell command-authorization set to be effective on a particular NDG, for each association:
- Select the **Assign a Shell Command Authorization Set on a per Network Device Group Basis** option.
 - Select a **Device Group** and an associated **Command Set**.
 - Click **Add Association**.



Tip You can also select which command set applies to network device groups that are not listed by associating that command set with the NDG *<default>* listing.

The NDG or NDGs and associated shell command-authorization set or sets are paired in the table.

- Step 7** To define the specific Cisco IOS commands and arguments to permit or deny for this user:



Caution

This step configures a powerful, advanced feature. Only an administrator who is skilled with Cisco IOS commands should use this feature. Correct syntax is the responsibility of the administrator. For information on how ACS uses pattern matching in command arguments, see [About Pattern Matching, page 4-28](#).

- Select the **Per User Command Authorization** option.
- Under Unmatched Cisco IOS commands, select **Permit** or **Deny**.
If you select **Permit**, the user can issue all commands that are not specifically listed. If you select **Deny**, the user can issue only those commands that are listed.
- To list particular commands to permit or deny, check the **Command** check box and then type the name of the command, define its arguments using standard permit or deny syntax, and select whether unlisted arguments are to be permitted or denied.

**Tip**

To enter several commands, you must click **Submit** after entering a command. A new command entry box appears below the box that you just completed.

- Step 8** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 9** If you are finished configuring the user account options, click **Submit** to record the options.

Configuring a PIX Command Authorization Set for a User

Use this procedure to specify the PIX command-authorization set parameters for a user. The options are:

- **None**—No authorization for PIX commands.
- **Group**—The group-level PIX command-authorization set applies for this user.
- **Assign a PIX Command Authorization Set for any network device**—One PIX command-authorization set is assigned, and it applies to all network devices.
- **Assign a PIX Command Authorization Set on a per Network Device Group Basis**—Particular PIX command-authorization sets will be effective on particular NDGs.

Before You Begin

- Ensure that you configure an AAA client to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In **Interface Configuration > TACACS+ (Cisco)**, ensure that the **PIX Shell (pixShell)** option is selected in the User column.
- Ensure that you have configured one or more PIX command-authorization sets. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

To specify PIX command-authorization set parameters for a user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Scroll down to the TACACS+ Settings table and to the PIX Command Authorization Set feature area within it.
- Step 3** To prevent the application of any PIX command-authorization set, select (or accept the default of) the **None** option.
- Step 4** To assign the PIX command-authorization set at the group level, select the **As Group** option.
- Step 5** To assign a particular PIX command-authorization set to be effective on any configured network device:
- Select the **Assign a PIX Command Authorization Set for any network device** option.
 - From the list directly below that option, select the PIX command-authorization set that you want to apply to this user.

- Step 6** To create associations that assign a particular PIX command-authorization set to be effective on a particular NDG, for each association:
- Select the **Assign a PIX Command Authorization Set on a per Network Device Group Basis** option.
 - Select a **Device Group** and an associated **Command Set**.
 - Click **Add Association**.
- The associated NDG and PIX command-authorization sets appear in the table.
- Step 7** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 8** If you are finished configuring the user account options, click **Submit** to record the options.
-

Configuring Device-Management Command Authorization for a User

Use this procedure to specify the device-management command-authorization set parameters for a user. Device-management command-authorization sets support the authorization of tasks in Cisco device-management applications that are configured to use ACS for authorization. You can choose:

- None**—No authorization is performed for commands that are issued in the applicable Cisco device-management application.
- Group**—For this user, the group-level command-authorization set applies for the applicable device-management application.
- Assign a <device-management application>** for any network device—For the applicable device-management application, one command-authorization set is assigned, and it applies to management tasks on all network devices.
- Assign a <device-management application> on a per Network Device Group Basis**—For the applicable device-management application, you use this option to apply command-authorization sets to specific NDGs, so that it affects all management tasks on the network devices that belong to the NDG.

Before You Begin

- Ensure that an AAA client is configured to use TACACS+ as the security control protocol.
- In **Interface Configuration > Advanced Options**, ensure that the **Per-user TACACS+/RADIUS Attributes** check box is selected.
- In **Interface Configuration > TACACS+ (Cisco)**, ensure that the new TACACS+ service corresponding to the applicable device-management application is selected under **New Services** in the User column.
- If you want to apply command-authorization sets, be certain that you have configured one or more device-management command-authorization sets. For detailed steps, see [Adding a Command Authorization Set, page 4-29](#).

To specify device-management application command authorization for a user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

- Step 2** Scroll down to the TACACS+ Settings table and to the applicable device-management command-authorization feature area within it.
- Step 3** To prevent the application of any command authorization for actions that are performed in the applicable device-management application, select (or accept the default of) the **None** option.
- Step 4** To assign command authorization for the applicable device-management application at the group level, select the **As Group** option.
- Step 5** To assign a particular command-authorization set that affects device-management application actions on any network device:
- Select the **Assign a <device-management application>** for any network device option.
 - Then, from the list directly below that option, select the command-authorization set that you want to apply to this user.
- Step 6** To create associations that assign a particular command-authorization set that affects device-management application actions on a particular NDG, for each association:
- Select the **Assign a <device-management application>** on a per Network Device Group Basis option.
 - Select a **Device Group** and an associated *<device-management application>*.
 - Click **Add Association**.
- The associated NDG and command-authorization sets appear in the table.
- Step 7** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 8** If you are finished configuring the user account options, click **Submit** to record the options.

Configuring the Unknown Service Setting for a User

If you want TACACS+ AAA clients to permit unknown services, you can check the Default (Undefined) Services check box. Checking this option will PERMIT all UNKNOWN Services.

To configure the Unknown Service setting for a user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Scroll down to the table under the heading PERMIT all UNKNOWN Services.
- Step 3** To allow TACACS+ AAA clients to permit unknown services for this user, select the **Default (Undefined) Services** check box.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.

Advanced TACACS+ Settings for a User

The information in this section applies when you have configured an AAA client with TACACS+.



Tip

If the Advanced TACACS+ Settings (User) table does not appear, choose **Interface Configuration > TACACS+ (Cisco IOS)**. Then, choose **Advanced TACACS+ Features**.

This section contains:

- [Setting Enable Privilege Options for a User, page 6-22](#)
- [Setting TACACS+ Enable Password Options for a User, page 6-23](#)
- [Setting TACACS+ Outbound Password for a User, page 6-24](#)

Setting Enable Privilege Options for a User

You use a TACACS+ Enable Control with Exec session to control administrator access. Typically, you use it for router-management control. Select and specify the user privilege level:

- **Use Group Level Setting**—Sets the privileges for this user identical to the privileges configured at the group level.
- **No Enable Privilege**—Disallows enable privileges for this user.



Note

No Enable Privilege is the default setting.

- **Max Privilege for any AAA Client**—You can select from a list the maximum privilege level that will apply to this user on any AAA client on which this user is authorized.
- **Define Max Privilege on a per-Network Device Group Basis**—You can associate maximum privilege levels for this user in one or more NDGs.



Note

For information about privilege levels, refer to your AAA client documentation.



Tip

You must configure NDGs from within Interface Configuration before you can assign user privilege levels to them.

To select and specify the privilege level for a user:

Step 1 Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Under TACACS+ Enable Control in the Advanced TACACS+ Settings table, select one of the four privilege options:

- **Use Group Level Setting**
- **No Enable Privilege**



Note

No Enable Privilege is the default setting; when setting up an new user account, this privilege should already be selected.

- **Max Privilege for Any Access Server**

- **Define Max Privilege on a per-Network Device Group Basis**

Step 3 If you selected **Max Privilege for Any Access Server** in Step 2, select the appropriate privilege level from the corresponding list.

Step 4 If you selected **Define Max Privilege on a per-Network Device Group Basis** in Step 2, perform the following steps to define the privilege levels on each NDG, as applicable:

- a. From the Device Group list, select a device group.



Note You must have already configured a device group for it to be listed.

- b. From the Privilege list, select a privilege level to associate with the selected device group.

- c. Click **Add Association**.

An entry appears in the table, which associates the device group with a particular privilege level.

- d. Repeat Step a through Step c for each device group that you want to associate to this user.



Tip To delete an entry, select the entry and then click **Remove Associate**.

Step 5 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 6 If you are finished configuring the user account options, click **Submit** to record the options.

Setting TACACS+ Enable Password Options for a User

When setting the TACACS+ Enable Password Options for a user, you can use:

- **ACS PAP password.**
- **External database password.**
- **A separate password.**

To set the options for the TACACS+ Enable password:

Step 1 Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Select a password option:

- To use the information that is configured in the Password Authentication section, select **Use Cisco Secure PAP password**.



Note For information about basic password setup, see [Adding a Basic User Account, page 6-3](#).

- To use an external database password, select **Use external database password**, and then choose the database that authenticates the enable password for this user.

**Note**

The list of databases displays only the databases that you have configured. For more information, see [About External User Databases, page 12-3](#).

- To use a separate password, click **Use separate password**, and then type and retype to confirm a control password for this user. This password is used in addition to the regular authentication.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

Setting TACACS+ Outbound Password for a User

The TACACS+ outbound password enables an AAA client to authenticate itself to another AAA client via outbound authentication. The outbound authentication can be PAP, CHAP, MS-CHAP, or ARAP, and results in the ACS password being given out. By default, the user ASCII/PAP or CHAP/MS-CHAP/ARAP password is used. To avoid compromising inbound passwords, you can configure a separate SENDAUTH password.

**Caution**

Use an outbound password only if you are familiar with the use of a TACACS+ SendAuth/OutBound password.

To set a TACACS+ outbound password for a user:

Step 1 Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).

The User Setup Edit page opens. The username that you add or edit appears at the top of the page.

Step 2 Type and retype to confirm a TACACS+ outbound password for this user.

Step 3 To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.

Step 4 If you are finished configuring the user account options, click **Submit** to record the options.

RADIUS Attributes

You can configure user attributes for RADIUS authentication generally, at the Internet Engineering Task Force (IETF) level, or for vendor-specific attributes (VSAs) on a vendor-by-vendor basis. For general attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#). ACS ships with many popular VSAs already loaded and available to configure and apply. For information about creating additional, custom RADIUS VSAs, see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#).

**Caution**

If you are using Shared Radius Authorization Components (SRACs), you should be aware of issues regarding attribute merging and overwriting RADIUS attributes on a user or group level. You should not assign RADIUS attributes to an individual user (only as a last resort). Use group or SRACs to assign RADIUS attributes in the user's group or profile levels.

This section contains:

- [Setting IETF RADIUS Parameters for a User, page 6-25](#)
- [Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User, page 6-26](#)
- [Setting Cisco Aironet RADIUS Parameters for a User, page 6-27](#)
- [Setting Ascend RADIUS Parameters for a User, page 6-29](#)
- [Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User, page 6-29](#)
- [Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User, page 6-30](#)
- [Setting Microsoft RADIUS Parameters for a User, page 6-31](#)
- [Setting Nortel RADIUS Parameters for a User, page 6-33](#)
- [Setting Juniper RADIUS Parameters for a User, page 6-33](#)
- [Setting BBSM RADIUS Parameters for a User, page 6-35](#)
- [Setting Custom RADIUS Attributes for a User, page 6-36](#)

Setting IETF RADIUS Parameters for a User

ACS sends the RADIUS attributes as a user profile to the requesting AAA client. These parameters appear only if:

- AAA clients (one or more) are using one of the RADIUS protocols in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level IETF RADIUS attributes are enabled under **Interface Configuration > RADIUS (IETF)**.

**Note**

To display or hide any of these attributes in the web interface, see [Displaying RADIUS Configuration Options, page 2-7](#).

**Note**

For a list and explanation of RADIUS attributes, see [Appendix B, "RADIUS Attributes,"](#) or the documentation for your particular network device that is using RADIUS.

To configure IETF RADIUS attribute settings to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** In the IETF RADIUS table, for each attribute that you need to authorize for the current user, check the check box next to the attribute and then further define the authorization for the attribute in the box or boxes next to it, as applicable.

- Step 3** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 4** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Cisco IOS/PIX 6.0 RADIUS Parameters for a User

The Cisco IOS RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco IOS/PIX 6.0)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco IOS/PIX 6.0)** attributes are enabled under **Interface Configuration > RADIUS (Cisco IOS/PIX 6.0)**.



Note

To hide or display the Cisco IOS RADIUS VSA, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

Cisco IOS RADIUS represents only the Cisco IOS VSAs. You must configure the IETF RADIUS and Cisco IOS RADIUS attributes.

To configure and enable Cisco IOS RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco IOS RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** If you want to use the [009\001] `cisco-av-pair` attribute to specify authorizations, check the check box next to the attribute and then type the attribute-value pairs in the text box. Separate each attribute-value pair by pressing **enter**.

For example, if the current user profile corresponds to a Network Admission Control (NAC) client to which ACS always assigns a `status-query-timeout` attribute value that must be different than a value that any applicable group profile contains, you could specify the value as:

`status-query-timeout=1200`
- Step 4** If you want to use other Cisco IOS/PIX 6.0 RADIUS attributes, select the corresponding check box and specify the required values in the adjacent text box.
- Step 5** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 6** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Cisco Airespace RADIUS Parameters for a User

The Cisco Airespace RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco Airespace)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco Airespace)** attributes that you want to apply are enabled under **Interface Configuration> RADIUS (Cisco Airespace)**.

Cisco Airespace RADIUS represents only the Cisco Airespace proprietary attributes. You must configure IETF RADIUS and Cisco Airespace RADIUS attributes that you want to use.



Note

To hide or display Cisco Airespace RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco Airespace RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco Airespace RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the Cisco Airespace RADIUS Attributes table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** Do one:
- If you are finished configuring the user account options, click **Submit** to record the options.
 - To continue to specify the user account options, perform other procedures in this chapter, as applicable.
-

Setting Cisco Aironet RADIUS Parameters for a User

The single Cisco Aironet RADIUS VSA, Cisco-Aironet-Session-Timeout, is a virtual VSA. This VSA acts as a specialized implementation (that is, a remapping) of the IETF RADIUS Session-Timeout attribute (27) to respond to a request from a Cisco Aironet Access Point. Use the Cisco-Aironet-Session-Timeout attribute to provide a different timeout value when a user must be able

to connect via wireless and wired devices. This capability to provide a second timeout value specifically for WLAN connections avoids the difficulties that would arise if you had to use a standard timeout value (typically measured in hours) for a WLAN connection (that is typically measured in minutes). You do not need to use `Cisco-Aironet-Session-Timeout` if the particular user will always connect only with a Cisco Aironet Access Point. Rather, use this setting when a user may connect via wired or wireless clients.

For example, imagine a user's **Cisco-Aironet-Session-Timeout** set to 600 seconds (10 minutes) and that same user's IETF RADIUS Session-Timeout set to 3 hours. When the user connects via a VPN, ACS uses 3 hours as the timeout value. However, if that same user connects via a Cisco Aironet Access Point, ACS responds to an authentication request from the Aironet AP by sending 600 seconds in the IETF RADIUS **Session-Timeout** attribute. Thus, with the **Cisco-Aironet-Session-Timeout** attribute configured, different session-timeout values can be sent depending on whether the end-user client is a wired device or a Cisco Aironet Access Point.

The Cisco Aironet RADIUS parameters appear on the User Setup page only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco Aironet)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco Aironet)** attribute is enabled under RADIUS (Cisco Aironet) in the **Interface Configuration > RADIUS (Cisco Aironet)**.



Note

To hide or display the Cisco Aironet RADIUS VSA, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable the Cisco Aironet RADIUS attribute to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco Aironet RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the Cisco Aironet RADIUS Attributes table, select the **[5842\001] Cisco-Aironet-Session-Timeout** check box.
- Step 4** In the **[5842\001] Cisco-Aironet-Session-Timeout** box, type the session-timeout value (in seconds) that ACS is to send in the IETF RADIUS Session-Timeout (27) attribute when the AAA client is configured in Network Configuration to use the RADIUS (Cisco Aironet) authentication option. The recommended value is 600 seconds.
For more information about the IETF RADIUS Session-Timeout attribute, see [Appendix B, "RADIUS Attributes,"](#) or your AAA client documentation.
- Step 5** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 6** If you are finished configuring the user account options, click **Submit** to record the options.

Setting Ascend RADIUS Parameters for a User

The Ascend RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Ascend)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Ascend)** attributes that you want to apply are enabled under in the **Interface Configuration > RADIUS (Ascend)**.

Ascend RADIUS represents only the Ascend proprietary attributes. You must configure the IETF RADIUS and Ascend RADIUS attributes. Proprietary attributes override IETF attributes.

The default attribute setting that appears for RADIUS is `Ascend-Remote-Addr`.



Note

To hide or display Ascend RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA that is applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Ascend RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Ascend RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the Ascend RADIUS Attributes table, to specify the attributes that should be authorized for the user:
 - a. Check the check box next to the particular attribute.
 - b. Further define the authorization for that attribute in the box next to it.
 - c. Continue to select and define attributes, as applicable.
For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.

Setting Cisco VPN 3000/ASA/PIX 7.x+ RADIUS Parameters for a User

To control Microsoft Point-to-Point Encryption (MPPE) settings for users who access the network through a Cisco VPN 3000-series concentrator, an Adaptive Security Appliance (ASA), or PIX Security Appliance version 7.x+, use the **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) attributes. Settings for **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft)

attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) attributes; regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attribute configurations appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.

Cisco VPN 3000/ASA/PIX 7.x+ RADIUS represents only the Cisco VPN 3000/ASA/PIX 7.x+ VSA. You must configure the IETF RADIUS and Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes.



Note

To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco VPN 3000/ASA/PIX 7.x+ RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly.
- For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the Cisco VPN 3000/ASA/PIX 7.x+ Attribute table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Cisco VPN 5000 Concentrator RADIUS Parameters for a User

The Cisco VPN 5000 Concentrator RADIUS attribute configurations appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Cisco VPN 5000)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level RADIUS (Cisco VPN 5000) attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Cisco VPN 5000)**.

Cisco VPN 5000 Concentrator RADIUS represents only the Cisco VPN 5000 Concentrator VSA. You must configure the IETF RADIUS and Cisco VPN 5000 Concentrator RADIUS attributes.



Note

To hide or display Cisco VPN 5000 Concentrator RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Cisco VPN 5000 Concentrator RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco VPN 5000 Concentrator RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the Cisco VPN 5000 Concentrator Attribute table, to specify the attributes that should be authorized for the user:
- a. Check the check box next to the particular attribute.
 - b. Further define the authorization for that attribute in the box next to it.
 - c. Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Microsoft RADIUS Parameters for a User

Microsoft RADIUS provides VSAs supporting Microsoft Point-to-Point Encryption (MPPE), which is an encryption technology developed by Microsoft to encrypt point-to-point (PPP) links. These PPP connections can be via a dial-in line, or over a Virtual Private Network (VPN) tunnel.

To control Microsoft MPPE settings for users who access the network through a Cisco VPN 3000-series concentrator, use the **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) attributes. Settings for **CVPN3000-PPTP-Encryption** (VSA 20) and **CVPN3000-L2TP-Encryption** (VSA 21) override Microsoft MPPE RADIUS settings. If either of these

attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the **RADIUS (Cisco VPN 3000)** attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

The Microsoft RADIUS attribute configurations appear only if the following are true:

- AAA clients (one or more) are configured in **Network Configuration** that use a RADIUS protocol that supports the Microsoft RADIUS VSA.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Microsoft)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Microsoft)**.

The following ACS RADIUS protocols support the Microsoft RADIUS VSA:

- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX 7.x+
- Cisco VPN 5000
- Ascend
- Cisco Airespace

Microsoft RADIUS represents only the Microsoft VSA. You must configure the IETF RADIUS and Microsoft RADIUS attributes.



Note

To hide or display Microsoft RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Microsoft RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Cisco IOS RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the Microsoft RADIUS Attributes table, to specify the attributes that should be authorized for the user:
 - a. Check the check box next to the particular attribute.
 - b. Further define the authorization for that attribute in the box next to it.
 - c. Continue to select and define attributes, as applicable.

For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.



Note

The **MS-CHAP-MPPE-Keys** attribute value is autogenerated by ACS; there is no value to set in the web interface.

- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Nortel RADIUS Parameters for a User

The Nortel RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Nortel)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Nortel)** attributes that you want to apply are enabled under in the **Interface Configuration > RADIUS (Nortel)**.

Nortel RADIUS represents only the Nortel proprietary attributes. You must configure the Internet Engineering Task Force (IETF) RADIUS and Nortel RADIUS attributes. Proprietary attributes override IETF attributes.



Note

To hide or display Nortel RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA that is applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Nortel RADIUS attributes to apply as an authorization for the current user:

- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Nortel RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the Nortel RADIUS Attributes table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Juniper RADIUS Parameters for a User

The Juniper RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (Juniper)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (Juniper)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (Juniper)**.

Juniper RADIUS represents only the Juniper proprietary attributes. You must configure the IETF RADIUS and Juniper RADIUS attributes. Proprietary attributes override IETF attributes.

**Note**

To hide or display Juniper RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable Juniper RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring Juniper RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the Juniper RADIUS Attributes table, to specify the attributes to authorize for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting 3COMUSR RADIUS Parameters for a User

The 3COMUSR RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (3COMUSR)** in **Network Configuration**.
- **Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (3COMUSR)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (3COMUSR)**.

3COMUSR RADIUS represents only the 3COMUSR proprietary attributes. You must configure the IETF RADIUS and 3COMUSR RADIUS attributes. Proprietary attributes override IETF attributes.

**Note**

To hide or display 3COMUSR RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable 3COMUSR RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring 3COMUSR RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the 3COMUSR RADIUS Attributes table, to specify the attributes to authorize for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting BBSM RADIUS Parameters for a User

The Building Broadband Services Manager (BBSM) RADIUS parameters appear only if all the following are true:

- AAA clients (one or more) are configured to use **RADIUS (BBSM)** in **Network Configuration**.
- Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level **RADIUS (BBSM)** attributes that you want to apply are enabled under **Interface Configuration > RADIUS (BBSM)**.

BBSM RADIUS represents only the BBSM proprietary attributes. You must configure the IETF RADIUS and BBSM RADIUS attributes. Proprietary attributes override IETF attributes.

**Note**

To hide or display BBSM RADIUS attributes, see [Specifying Display of RADIUS \(<vendor>\) Options, page 2-9](#). A VSA applied as an authorization to a particular user persists, even when you remove or replace the associated AAA client; however, if you have no AAA clients of this (vendor) type configured, the VSA settings do not appear in the user configuration interface.

To configure and enable BBSM RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).

- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring BBSM RADIUS attributes, ensure that your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the BBSM RADIUS Attributes table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it.
 - Continue to select and define attributes, as applicable.
- For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.
- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

Setting Custom RADIUS Attributes for a User

Custom RADIUS parameters appear only if all the following are true:

- You have defined and configured the custom RADIUS VSAs. (For information about creating user-defined RADIUS VSAs, see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#).)
- AAA clients (one or more) are configured in **Network Configuration** that use a RADIUS protocol that supports the custom VSA.
- Per-user TACACS+/RADIUS Attributes** check box is selected under **Interface Configuration > Advanced Options**.
- User-level RADIUS (*custom name*) attributes that you want to apply are enabled under RADIUS (*custom name*) in the **Interface Configuration** section.

You must configure the IETF RADIUS and the custom RADIUS attributes. Proprietary attributes override IETF attributes.

To configure and enable custom RADIUS attributes to apply as an authorization for the current user:

-
- Step 1** Perform Step 1 through Step 3 of [Adding a Basic User Account, page 6-3](#).
- The User Setup Edit page opens. The username that you add or edit appears at the top of the page.
- Step 2** Before configuring custom RADIUS attributes, be certain your IETF RADIUS attributes are configured properly. For more information about setting IETF RADIUS attributes, see [Setting IETF RADIUS Parameters for a User, page 6-25](#).
- Step 3** In the RADIUS *custom name* Attributes table, to specify the attributes that should be authorized for the user:
- Check the check box next to the particular attribute.
 - Further define the authorization for that attribute in the box next to it, as required.
 - Continue to select and define attributes, as applicable.

For more information about attributes, see [Appendix B, “RADIUS Attributes,”](#) or your AAA client documentation.

- Step 4** To continue to specify other user account options, perform the required steps. See the other procedures in this section, as applicable.
- Step 5** If you are finished configuring the user account options, click **Submit** to record the options.
-

User Management

This section describes how to use the User Setup section to perform a variety of user account-management tasks.

This section contains:

- [Listing All Users, page 6-37](#)
- [Finding a User, page 6-37](#)
- [Disabling a User Account, page 6-38](#)
- [Deleting a User Account, page 6-39](#)
- [Resetting User Session Quota Counters, page 6-39](#)
- [Resetting a User Account after Login Failure, page 6-40](#)
- [Removing Dynamic Users, page 6-41](#)
- [Saving User Settings, page 6-41](#)

Listing All Users

The User List displays all user accounts (enabled and disabled). The list includes, for each user, the username, status, and the group to which the user belongs.

Usernames appear in the order in which they were entered into the database. This list cannot be sorted.

To view a list of all user accounts:

-
- Step 1** In the navigation bar, click **User Setup**.
The User Setup Select page opens.
- Step 2** Click **List All Users**.
In the display area on the right, the User List appears.
- Step 3** To view or edit the information for an individual user, click the username in the right window.
The user account information appears.
-

Finding a User

To find a user:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page opens.

Step 2 Type the name in the **User** box, and then click **Find**.



Tip You can use an asterisk (*) as a wildcard in this box.



Tip To display a list of usernames that begin with a particular letter or number, click the letter or number in the alphanumeric list. A list of users, whose names begin with that letter or number, opens in the display area on the right.

The username, status (enabled or disabled), and group to which the user belongs appear in the display area on the right.

Step 3 To view or edit the information for the user, click the username in the display area on the right.

The user account information appears.

Disabling a User Account

To manually disable a user account in the ACS internal database:



Note

To configure the conditions by which a user account will automatically be disabled, see [Setting Options for User Account Disablement, page 6-13](#).



Note

Do not confuse this procedure with account expiration due to password aging. Password aging is defined for groups only, not for individual users.

To disable a user account:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page opens.

Step 2 In the **User** box, type the name of the user whose account is to be disabled.

Step 3 Click **Add/Edit**.

The User Setup Edit page opens. The username being edited is at the top of the page.

Step 4 Select the **Account Disabled** check box.

Step 5 Click **Submit** at the bottom of the page.

The specified user account is disabled.

Deleting a User Account

You can delete user accounts one at a time by using the web interface.

**Note**

If you are authenticating using the Unknown User policy and you want deny a user access by deleting the user account, you must also delete the user account from the external user database. This action prevents the username from being automatically added to the ACS internal database the next time the user attempts to log in.

**Tip**

For deleting batches of user accounts, use the Relational Database Management System (RDBMS) Synchronization feature with action code 101 (see [RDBMS Synchronization, page 8-17](#), for more information.).

To delete a user account:

Step 1 Click **User Setup**.

The User Setup Select page of the web interface opens.

Step 2 In the **User** box, type the complete username to be deleted.

**Note**

Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 At the bottom of the User Setup page, click **Delete**.

**Note**

The Delete button appears only when you are editing user information, not when you are adding a username.

A popup window appears and prompts you to confirm the user deletion.

Step 5 Click **OK**.

The user account is removed from the ACS internal database.

Resetting User Session Quota Counters

You can reset the session quota counters for a user before or after the user exceeds a quota.

To reset user usage quota counters:

Step 1 Click **User Setup**.

The Select page of the web interface opens.

Step 2 In the **User** box, type the complete username of the user whose session quota counters that you are going to reset.



Note Alternatively, you can click **List All Users** and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 In the Session Quotas section, select the **Reset All Counters on submit** check box.

Step 5 Click **Submit** at the bottom of the browser page.

The session quota counters are reset for this user. The User Setup Select page appears.

Resetting a User Account after Login Failure

Perform this procedure when an account is disabled because the failed attempts count has been exceeded during an unsuccessful user attempt to log in.

To reset a user account after login failure:

Step 1 Click **User Setup**.

The User Setup Select page of the web interface opens.

Step 2 In the **User** box, type the complete username of the account to be reset.



Note Alternatively, you can click List All Users and then select the user from the list that appears.

Step 3 Click **Add/Edit**.

Step 4 In the Account Disable table, select the **Reset current failed attempts count on submit** check box, and then click **Submit**.

The **Failed attempts since last successful login**: counter resets to zero (0) and the system reenables the account.



Note This counter shows the number of unsuccessful login attempts since the last time this user logged in successfully.



Note If the user authenticates with a Windows user database, this expiration information is in addition to the information in the Windows user account. Changes here do not alter settings that you configured in Windows.

Removing Dynamic Users

External sources can manage dynamic users, their identities and other related properties. Dynamic users are created in the ACS internal database after they are successfully authenticated against the external sources. Dynamic users are created for optimization, and removing them does not effect ACS functionality.

You can remove dynamic users in user groups that are cached.



Note

All CSAuth activities will be suspended while dynamic users are being removed from the database.

To remove dynamic users:

Step 1 In the navigation bar, click **User Setup**.

The User Setup Select page appears.

Step 2 Click **Remove Dynamic Users**.

A message appears in the right pane, indicating the number of dynamic users removed or whether any errors occurred.



Note

Dynamically mapped users *are not* saved when you perform replication, upgrade or overinstall ACS. Dynamically mapped users *are* saved when you back up or restore ACS.



Note

You can configure ACS to omit creating dynamic users while authenticating against external databases. For more information, see [Unknown User Policy Options, page 15-6](#).

Saving User Settings

After you have completed configuration for a user you must save your work.

To save the configuration for the current user:

Step 1 To save the user account configuration, click **Submit**.

Step 2 To verify that your changes were applied, type the username in the **User** box and click **Add/Edit**, and then review the settings.



CHAPTER 7

System Configuration: Basic

This chapter addresses the basic features in the System Configuration section of the web interface for the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

This chapter contains:

- [Service Control, page 7-1](#)
- [Logging, page 7-3](#)
- [Date and Time Format Control, page 7-3](#)
- [Local Password Management, page 7-4](#)
- [ACS Backup, page 7-8](#)
- [ACS System Restore, page 7-14](#)
- [ACS Active Service Management, page 7-18](#)
- [VoIP Accounting Configuration, page 7-21](#)
- [Support Page, page 7-25](#)
- [Appliance Upgrade Mechanism \(ACS SE Only\), page 7-27](#)

Service Control

ACS uses several services. The Service Control page provides basic status information about the services. You use this page to configure the service log files, and to stop or restart the services. For more information about ACS services, see [Chapter 1, “Overview.”](#)



Tip

You can configure ACS service logs. For more information, see [Configuring Service Logs, page 10-29](#).

This section contains:

- [Determining the Status of ACS Services, page 7-2](#)
- [Stopping, Starting, or Restarting Services, page 7-2](#)
- [Setting Service Log File Parameters, page 7-2](#)

Determining the Status of ACS Services

You can determine whether ACS services are running or stopped by accessing the Service Control page. To determine the status of ACS services:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Service Control**.

The status of the services appears in ACS on *hostname* table, where *hostname* is the name of the ACS.

Stopping, Starting, or Restarting Services

You can stop, start, or restart ACS services as needed. The following procedure stops, starts, or restarts most ACS services.



Tip

You should use the web interface to control services, due to dependencies in the order in which ACS starts services. If you need to restart the **CSAdmin** service, you can use the Windows Control Panel (ACS for Windows) or the **stop** and **start** commands on the serial console (ACS SE).



Note

(ACS SE only) You cannot control the **CSAgent** service from the Service Control page. For information, see [Enabling or Disabling CSAgent, page 7-22](#).

To stop, start, or restart most ACS services:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Service Control**.

The status of the services appears in ACS on *hostname* table, where *hostname* is the name of the ACS.

If the services are running, the Restart and Stop buttons appear at the bottom of the page.

If the services are stopped, the Start button appears at the bottom of the page.

Step 3 Click **Stop**, **Start**, or **Restart**, as applicable.

The status of ACS services changes to the state according to which button that you clicked.

Setting Service Log File Parameters

To configure the parameters for the service log file and directory management, use this page. For detailed option descriptions, see [Configuring Service Logs, page 10-29](#).

Step 1 Complete the following:

Field	From the List, Select:
Level of detail	The level of detail.
Generate new file	The schedule to generate log files.
Manage directory	How long to keep log files.

Step 2 Click **Restart**.

ACS restarts its services and implements the service log settings that you specified.



Note Ensure that you have enough disk space in which to store your log files. Consult the logs if any problems occur.

Logging

You can configure ACS to generate logs for administrative and accounting events, depending on the protocols and options that you enable. Log files are stored in the *drive:\install_dir\service_name\Logs* directory. For example, in *C:\CiscoSecureACS\CSAuth\Logs*. For details on service logs and gathering information for troubleshooting, see [Service Logs, page 10-12](#).

Date and Time Format Control

ACS supports two possible date formats in its logs, reports, and administrative interface. You can choose a month/day/year format or a day/month/year format.

When ACS sends a log to the syslog server, the syslog server displays and records the time. ACS supports two possible time formats in its logs, reports, and administrative interface. You can choose the local time zone or the GMT display.

Setting the Date and Time Formats



Note If you have reports that were generated before you changed the date format, you must move or rename them to avoid conflicts. For example, if you are using the month/day/year format, ACS assigns the name *2007-07-12.csv* to a report that was generated on July 12, 2007. If you subsequently change to the day/month/year format, on December 7, 2001, ACS creates a file also named *2007-07-12.csv* and overwrites the existing file.

To set the date and time formats:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Date Format Control**.

ACS displays the Date Format Control page.

- Step 3** Chose a date format.
- Step 4** Chose a time zone for the syslog server display.
- Step 5** Click **Submit & Restart**.

ACS restarts its services and implements the date and time format that you chose.



Note For the new date or time format to be visible in the web interface reports, you must restart the connection to the ACS. Click the **X** in the upper-right corner of the browser window to close it.

Local Password Management

Use the Local Password Management page to configure settings that manage user passwords that were in the ACS internal database.



Note

ACS stores user accounts, username, and password authentication information separately from ACS administrator account information. ACS stores accounts that were created for authentication of network service requests and ACS administrative access in separate internal databases. For information on administrator accounts, see [Chapter 11, “Administrators and Administrative Policy.”](#)

The Local Password Management page contains these sections:

- **Password Validation Options**—You use these settings to configure validation parameters for user passwords. ACS enforces these rules when an administrator changes a user password in the ACS internal database and when a user attempts to change passwords by using the Authentication Agent applet.



Note

Password validation options apply only to user passwords that are stored in the ACS internal database. They do not apply to passwords in user records in external user databases; nor do they apply to enable or **admin** passwords for Cisco IOS network devices.

The password validation options are:

- **Password length between X and Y characters**—Enforces that password lengths adhere to the values specified in the X and Y boxes, inclusive. ACS supports passwords up to 32 characters long.
- **Password may not contain the username**—Requires that a user password does not contain the username.
- **Password is different from the previous value**—Requires that a new user password to be different from the previous password.
- **Password must be alphanumeric**—Requires that a user password contain letters and numbers.
- **Remote Change Password**—You use these settings to configure whether a TELNET password change is enabled and, if so, whether ACS immediately sends the updated user data to its replication partners.

The remote change password options are:

- **Disable TELNET Change Password against this ACS and return the following message to the users TELNET session**—ACS supports password change from a device that uses TACACS+. Check to disable the password change. When checked, this option disables the ability to perform password changes during a TELNET session that a TACACS+ AAA client hosts. Users who submit a password change receive the text message that you enter in the corresponding box. For more information, see [Changing a User Password from a Device Using TACACS+, page 7-5](#).
- **Upon remote user password change, immediately propagate the change to selected replication partners**—This setting determines whether ACS sends its replication partners any passwords that are changed during a TELNET session, that is hosted by a TACACS+ AAA client, the Authentication Agent, or the User-Changeable Passwords web interface. The ACSs that were configured as the replication partners of this ACS appear below this check box.

This feature depends on the Database Replication feature being configured properly; however, replication scheduling does not apply to propagation of changed password information. ACS sends changed password information immediately, regardless of replication scheduling.

Changed password information is replicated only to ACSs that are properly configured to receive replication data from this ACS. The automatically triggered cascade setting for the Database Replication feature does not cause ACSs that receive changed password information to send it to their replication partners.

For more information about Database Replication, see [ACS Internal Database Replication, page 8-1](#).

The log file management options for the User Password Changes Log are:

- **Generate New File**—You can specify the frequency at which ACS creates a *User Password Changes Log* file: daily, weekly, monthly; or, after the log reaches a size in kilobytes that you specify.
- **Manage Directory**—You can specify whether ACS controls the retention of log files. You can use this feature to specify the maximum number of files to retain or the maximum age of files to retain. If the maximum number of files is exceeded, ACS deletes the oldest log file. If the maximum age of a file is exceeded, ACS deletes the file.

Changing a User Password from a Device Using TACACS+

You can configure ACS to control whether network administrators can change passwords during TELNET sessions that are hosted by TACACS+ AAA clients. Some Cisco devices support a TACACS+ facility for users to change their passwords when connecting for an administration session. The changes made by the user are communicated to ACS over TACACS+ using a routine known as **chpass**.

On an ACS on which **chpass** is enabled (**chpass** should be enabled on a top-level replication master for the installation) the **chpass** sequence is as follows:

Enable **chpass** on a top-level replication master for the installation. On an ACS on which you enable **chpass**, the sequence is described here.

To enable **chpass** from a device:

-
- Step 1** When prompted for your password, press **Return**.
 - Step 2** When prompted for your current password, enter you current password and then press **Return**.

- Step 3** When prompted for a new password, enter the new password and then press **Return**.
-

When a user tries to change a password on a ACS on which **chpass** is enabled, ACS performs an immediate and automatic propagation of the event to its replication slave partners (all those configured in its GUI as replication slave partners). This process mitigates any possible change propagation issues that may have relied on a timed replication propagation.

You can also use **chpass** after a password was intentionally changed due to password aging. ACS initiates **chpass** so that you can reset or change your password in the ACS internal database.

The password aging feature in ACS requires you to change your password. When a password expires, the administrator must intentionally reset the user password. You will then only be able to log in to the AAA client via TELNET using the password that the administrator assigned, namely the reset password. When **chpass** is initiated, you will be asked to change your password according to the method described in this section.

An alternative method for allowing users to change their passwords is to use the Web-based User Changeable Password (UCP) utility supplied with ACS. For more information see the *Installation and User Guide for Cisco Secure ACS User-Changeable Passwords*.

An ACS receiving TACACS+ authentication traffic from a particular device, may not have yet received the password change update and so may still be operating with the older password. This is a well-known problem with many distributed password control systems. You can disable ACS **chpass** from its TACACS+ clients. When a user on a TACACS+ client device attempts the **chpass** procedure against ACS, on which support for **chpass** is disabled, ACS sends a configurable message back to the device, and to the user, explaining that the **chpass** functionality is not supported on this device. This configurable message can be used to direct device administrators to perform a TELNET to a device that uses a TACACS+ server that allows **chpass**.

Configuring Local Password Management

To configure password validation options for user account passwords:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Local Password Management**.
- The Local Password Management page appears.
- Step 3** Under Password Validation Options:
- In **Password length between X and Y characters**, enter the *minimum* valid number of characters for a password in the X box. While the X box accepts two characters, passwords can only be between 1 and 32 characters in length.
 - In **Password length between X and Y characters**, enter the *maximum* valid number of characters for a password in the Y box. While the Y box accepts two characters, passwords can only be between 1 and 32 characters in length.
 - If you want to disallow passwords that contain the username, check the **Password may not contain the username** check box.
 - If you want to require that a user password be different than the previous user password, check the **Password is different from the previous value** check box.
 - If you want to require that passwords must contain letters and numbers, check the **Password must be alphanumeric** check box.

Step 4 Under Remote Change Password:

- a. If you want to enable user password changes in TELNET sessions, uncheck the **Disable TELNET Change Password against this ACS and return the following message to the users TELNET session** check box.
- b. If you want to disable user password changes in TELNET sessions, check the **Disable TELNET Change Password against this ACS and return the following message to the users TELNET session** check box.
- c. In the box below the **Disable TELNET Change Password against this ACS and return the following message to the users TELNET session** check box, enter a message that users should see when attempting to change a password in a TELNET session and when the TELNET password change feature has been disabled (Step b).
- d. If you want ACS to send changed password information immediately after a user has changed a password, check the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.



Tip

The ACSs that receive the changed password information appear below the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.

Step 5 Click **Submit**.

ACS restarts its services and implements the settings that you specified.

Configuring Intervals for Generating a New Password (ACS for Windows Only)

If you want ACS to generate a User Password Changes log file at a regular interval:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

The Logging Configuration page appears.

Step 3 In the User Password Changes CSV column, click **Configure**.

The CSV User Password Changes File Configuration appears.

Step 4 In the Log File Management section, chose one of the following:

- **Every day**—ACS generates a new User Password Changes log file at the start of each day.
- **Every week**—ACS generates a new User Password Changes log file at the start of each week.
- **Every month**—ACS generates a new User Password Changes log file at the start of each month.

Step 5 If you want ACS to generate a new *User Password Changes* log file when the current file reaches a specific size, select the **When size is greater than X KB** option and type the file size threshold, in kilobytes, in the X box.

Step 6 If you want to manage which *User Password Changes* log files that ACS keeps:

- a. Check the **Manage Directory** check box.
- b. If you want to limit the number of User Password Changes log files that ACS retains, select the **Keep only the last X files** option and type the number of files that you want ACS to retain in the X box.

- c. If you want to limit the age of User Password Changes log files that ACS retains, select the **Delete files older than X days** option and type the number of days for which ACS should retain a User Password Changes log file before deleting it.

Step 7 Click **Submit**.

ACS restarts its services and implements the settings that you specified.

ACS Backup

This section provides information about the ACS Backup feature, including procedures for implementing this feature.



Caution

As with previous versions of ACS, you cannot perform replication between different versions of ACS.

This section contains:

- [About ACS Backup, page 7-8](#)
- [Backup File Locations \(ACS for Windows Only\), page 7-9](#)
- [Directory Management \(ACS for Windows Only\), page 7-9](#)
- [Components Backed Up, page 7-9](#)
- [Reports of ACS Backups, page 7-10](#)
- [Backup Options, page 7-10](#)
- [Performing a Manual ACS Backup, page 7-11](#)
- [Scheduling ACS Backups, page 7-12](#)
- [Disabling Scheduled ACS Backups, page 7-14](#)

About ACS Backup

Maintaining backup files can minimize downtime if system information becomes corrupt or is misconfigured. You can manually back up the ACS system. You can also establish automated backups that occur at regular intervals, or at selected days of the week and times.

ACS for Windows

The ACS Backup feature provides the option to back up your user and group databases, and your ACS system configuration information to a file on the local hard drive. We recommend that you copy the files to the hard drive on another computer in case the hardware fails on the primary system.

ACS SE

The ACS Backup feature backs up ACS system information to a file that ACS sends to an FTP server that you specify. We recommend that you copy the files from the FTP server to another computer in case the hardware fails on the FTP server.

**Note**

ACS determines the filename given to a backup. For more information about filenames that are assigned to backup files generated by ACS, see [Filenames and Locations, page 7-15](#).

Both Platforms

For information about using a backup file to restore ACS, see [ACS System Restore, page 7-14](#).

**Note**

We do not support backup and restore features between different versions of ACS.

Backup File Locations (ACS for Windows Only)

The default directory for backup files is:

drive: \ *path* \CSAuth\System Backups

where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory. For example, if you installed ACS version 4.2 in the default location, the default backup location would be:

c:\Program Files\CiscoSecure ACS v4.2\CSAuth\System Backups

ACS determines the filename that is assigned to a backup. For more information about filenames that ACS assigns to backup files, see [Filenames and Locations, page 7-15](#).

Directory Management (ACS for Windows Only)

You can configure the number of backup files to keep and the number of days after which backup files are deleted. The more complex your configuration and the more often you back up the system, the more diligent you should be about clearing out old databases from the ACS hard drive.

Components Backed Up

The ACS System Backup feature backs up the ACS user database that is relevant to ACS. The user database backup includes all user information, such as username, password, and other authentication information, including server certificates and the certificate trust list.

If your ACS for Windows logs information to a remote ACS server, both ACS versions must have identical release, build, and patch numbers; or the logging might fail.

**Caution**

As with previous versions of ACS, you must not perform replication between different versions of ACS.

**Note**

The cert7.db file is not backed up. If you use this certificate file with an LDAP database, we recommend that you back it up on a remote machine for disaster recovery.

Reports of ACS Backups

When a system backup occurs, whether it was manually generated or scheduled, the event is logged in the Administration Audit report, and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of ACS.

For more information about ACS reports, see [Chapter 1, “Overview.”](#)

Backup Options

The ACS System Backup Setup page contains:

- **Manually**—ACS does not perform automatic backups. When this option is selected, you can only perform a backup by following the steps in [Performing a Manual ACS Backup, page 7-11](#).
- **Every X minutes**—ACS performs automatic backups on a set frequency. The unit of measurement is minutes, with a default backup frequency of 60 minutes.
- **At specific times**—ACS performs automatic backups at the time that is specified in the day-and-hour graph. The minimum interval is one hour, and the backup occurs on the hour that you selected.

ACS for Windows

- **Directory**—The directory to which ACS writes the backup file. You must specify the directory by its full path on the Windows server that runs ACS, such as `c:\acs-bups`.
- **Manage Directory**—Defines whether ACS deletes older backup files. Using the following options, you can specify how ACS determines which log files to delete:
 - **Keep only the last X files**—ACS retains the most recent backup files, up to the number of files that you specified. When the number of files that you specified is exceeded, ACS deletes the oldest files.
 - **Delete files older than X days**—ACS deletes backup files that are older than the number of days that you specified. When a backup file grows older than the number of days that you specified, ACS deletes it.
- **Add Hostname**—Backup file names can include the ACS server host name. Click **Add Hostname** to add the hostname to backup file names. Adding a hostname provides a way to identify which backup file corresponds to which ACS server in distributed deployments with multiple ACS servers.

ACS SE

- **FTP Server**—The IP address or hostname of the FTP server to which you want to send the backup files. If you specify a hostname, you must enable DNS on your network.
- **Login**—A valid username that enables ACS to access the FTP server.
- **Password**—The password for the username provided in the Login box.
- **Directory**—The directory to which ACS writes the backup file. You must specify the directory relative to the FTP root directory. To specify the FTP root directory, enter a single period (.).
- **Encrypt Backup File**—Determines whether ACS encrypts the backup file.
- **Encryption Password**—The password used to encrypt the backup file. If the you click the Encrypt backup file option, you must provide a password.

**Note**

If you use an encrypted backup file to restore ACS data, you must provide the exact password that you entered in the Encryption Password box when the you created the backup.

Performing a Manual ACS Backup

You can back up ACS whenever you want, without scheduling the backup.

To perform an immediate backup of ACS:

ACS for Windows

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Backup**.
The ACS System Backup Setup page appears.
- Step 3** In the **Directory** box under Backup Location, enter the drive and path to the directory on a local hard drive to which you want to write the backup file.
- Step 4** Click **Backup Now**.
ACS immediately begins a backup.
-

ACS SE

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Backup**.
The ACS System Backup Setup page appears. At the top of the page, information about the last backup appears, including:
- Whether the last backup succeeded.
 - The IP address of the FTP server used for the backup.
 - The directory used to store the backup.
 - The filename of the backup file that was created.
- Step 3** In the **FTP Server** box under FTP Setup, enter the IP address or hostname of the FTP server to which you want ACS to send the backup file.
- Step 4** In the **Login** box under FTP Setup, enter a valid username to enable ACS to access the FTP server.
- Step 5** In the **Password** box under FTP Setup, enter the password for the username that you provided in the Login box.
- Step 6** In the **Directory** box under FTP Setup, enter the relative path to the directory on the FTP server to which you want to send the backup file.
- Step 7** If you want to encrypt the backup file:
- a. Check the **Encrypt backup file** check box.
 - b. In the **Encryption Password** box, enter the password that you want to use for encryption of the backup file.

**Note**

If you use an encrypted backup file to restore ACS data, you must provide the exact password that you entered in the Encryption Password box when the backup was created.

Step 8 Click **Backup Now**.

ACS immediately begins a backup.

**Note**

ACS determines the backup filename. For more information about filenames assigned to backup files generated by ACS, see [Filenames and Locations, page 7-15](#).

Scheduling ACS Backups

You can schedule ACS backups to occur at regular intervals, or on selected days of the week and times.

To schedule the times at which ACS performs a backup:

ACS for Windows

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

The ACS System Backup Setup page appears.

Step 3 To schedule backups at regular intervals, under ACS Backup Scheduling, select the **Every X minutes** option and, in the **X** box, enter the length of the interval at which ACS should perform backups.

**Note**

Because ACS is momentarily shut down during backup, if the backup interval is too frequent (that is, the setting is too low), users might be unable to authenticate.

Step 4 To schedule backups at specific times:

- a. Under ACS Backup Scheduling, select the **At specific times** option.
- b. In the day-and-hour graph, click the times at which you want ACS to perform a backup.

**Tip**

Clicking times of day on the graph selects those times; clicking again clears them. At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 5 To change the location where ACS writes backup files, type the drive letter and path in the **Directory** box.

Step 6 To manage which backup files ACS keeps:

- a. Check the **Manage Directory** check box.
- b. To limit the number of backup files that ACS retains, select the **Keep only the last X files** option and type in the **X** box the number of files that you want ACS to retain.

- c. To limit the age of backup files that ACS retains, select the **Delete files older than X days** option and type the number of days for which ACS should retain a backup file before deleting it.

Step 7 Click **Submit**.

ACS implements the backup schedule that you configured.

ACS SE

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

The ACS System Backup Setup page appears.

Step 3 To schedule backups at regular intervals, under ACS Backup Scheduling, select the **Every X minutes** option and, in the *X* box, enter the length of the interval at which ACS should perform backups.



Note Because ACS is momentarily shut down during backup, if the backup interval is too frequent (that is, the setting is too low), users might be unable to authenticate.

Step 4 To schedule backups at specific times:

- a. Under ACS Backup Scheduling, click the **At specific times** option.
- b. In the day-and-hour graph, click the times at which you want ACS to perform a backup.



Tip Clicking times of day on the graph selects those times; clicking again clears them. At any time, you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 5 In the **FTP** box under FTP Setup, enter the IP address or hostname of the FTP server to which you want ACS to send the backup file.

Step 6 In the **Login** box under FTP Setup, enter a valid username to enable ACS to access the FTP server.

Step 7 In the **Password** box under FTP Setup, enter the password for the username that you provided in the Login box.

Step 8 In the **Directory** box under FTP Setup, enter the relative path to the directory on the FTP server to which you want to write the backup file.

Step 9 If you want to encrypt the backup file:

- a. Check the **Encrypt backup file** check box.
- b. In the **Encryption Password** box, enter the password that you want to use to encrypt the backup file.



Note If you use an encrypted backup file to restore ACS data, you must provide the exact password that you entered in the Encryption Password box when the backup was created.

Step 10 Click **Submit**.

ACS implements the backup schedule that you configured.

Disabling Scheduled ACS Backups

You can disable scheduled ACS backups without losing the schedule itself. You can use this method to end scheduled backups and resume them later without having to recreate the schedule.

To disable a scheduled backup:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Backup**.

The ACS System Backup Setup page appears.

Step 3 Under ACS Backup Scheduling, select the **Manual** option.

Step 4 Click **Submit**.

ACS does not continue any scheduled backups. You can still perform manual backups as needed.

ACS System Restore

This section provides information about the ACS System Restore feature, including procedures for restoring your ACS from a backup file.



Caution

As with previous versions of ACS, you must not perform replication between different versions of ACS.

This section contains:

- [About ACS System Restore, page 7-14](#)
- [Filenames and Locations, page 7-15](#)
- [Components Restored, page 7-16](#)
- [Reports of ACS Restorations, page 7-16](#)
- [Restoring ACS from a Backup File, page 7-16](#)

About ACS System Restore

You use the ACS System Restore feature to restore your user and group databases, and your ACS system configuration information from backup files that the ACS Backup feature generates. This feature helps you to minimize downtime if ACS system information becomes corrupted or is misconfigured.

The ACS System Restore feature only works with backup files that ACS generates when running an identical ACS version and patch level.

If you restore onto a physically different server, it must have the same IP address as the original server; otherwise, replication will not work correctly because the network configuration has a hidden record that contains details of the ACS server.

Filenames and Locations

The ACS System Restore feature restores the ACS user database and other ACS configuration data from a backup file and location that was created by the ACS Backup feature. You can restore your system from the latest backup file; or, if you suspect that the latest backup was incorrect, you can restore from an earlier backup file.

ACS for Windows

The ACS System Restore feature restores the ACS user database and ACS Windows Registry information. ACS writes the backup files to the local hard drive. When you schedule backups or perform a manual backup, you select the backup directory. The default directory for backup files is:

drive: \path\CSAuth\System Backups

where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory. For example, if you installed ACS version 4.2 in the default location, the default backup location would be:

c:\Program Files\CiscoSecure ACS v4.2\CSAuth\System Backups

ACS SE

The ACS System Restore feature restores the ACS user database and other ACS configuration data from a backup file and location that the ACS Backup feature created. ACS sends backup files to an FTP server that you specify on the ACS System Backup Setup page. On the FTP server, backup files are written to the directory that you specify when you schedule backups or perform a manual backup. The FTP server uses the following locations. For:

- Windows FTP servers, `FTPROOT dir/user_specified_dir`
- Unix FTP servers, the FTP user home directory is `FTPROOT` by default

Both Platforms

ACS creates backup files by using the date and time format:

dd-mmm-yyyy hh-nn-ss.dmp

where:

- *dd* is the date the backup started
- *mmm* is the month, abbreviated in alphabetic characters
- *yyyy* is the year
- *hh* is the hour, in 24-hour format
- *nn* is the minute
- *ss* is the second at which the backup started

For example, if ACS started a backup on October 13, 1999, 11:41:35 a.m., ACS would generate a backup file named:

13-Oct-1999 11-41-35.dmp

ACS for Windows

If you are uncertain of the location of the latest backup file, check your scheduled backup configuration on the ACS Backup page.

ACS SE

If you chose to encrypt the backup file, the backup filename includes the lowercase letter *e* just before the *.dmp* file extension. If the previous example was an encrypted backup file, the file name becomes:

13-Oct-2005 11-41-35e.dmp

If you are uncertain which FTP server and directory was used to create the latest backup file, check the ACS System Restore Setup page. Information about the most recent backup and restore, if any, appears at the top of the page.

Components Restored

You can select the components to restore: user and group databases, system configuration, or both.

Reports of ACS Restorations

When an ACS system restoration occurs, the event is logged in the Administration Audit report, and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of ACS.

For more information about ACS reports, see [Chapter 10, “Logs and Reports.”](#)

Restoring ACS from a Backup File

You can perform a system restoration of ACS whenever needed.

**Note**

Using the ACS System Restore feature restarts all ACS services and logs out all administrators.

To restore ACS from a backup file that the ACS Backup feature generated:

ACS for Windows

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **ACS Restore**.
The **ACS System Restore Setup** page appears.
The Directory box displays the drive and path to the backup directory that is most recently configured in the Directory box on the ACS Backup page.
Beneath the Directory box, ACS displays the backup files in the current backup directory. If no backup files exist, <No Matching Files> appears in place of filenames.
 - Step 3** To change the backup directory, type the new drive and path to the backup directory in the **Directory** box, and then click **OK**.
ACS displays the backup files, if any, in the backup directory that you specified.
 - Step 4** In the list below the **Directory** box, select the backup file that you want to use to restore ACS.
 - Step 5** To restore user and group database information, check the **User and Group Database** check box.
 - Step 6** To restore system configuration information, check the **Cisco Secure ACS System Configuration** check box.

- Step 7** To upgrade to ACS 4.2 using the ACS 4.1 backup file check the **Restore from 4.1 backup file to ACS 4.2** check box. You use this option to upgrade to ACS 4.2 using the ACS 4.1 backup file. The upgrade functionality is then implemented, and the user and group databases and the system configuration will be restored.
- Step 8** Click **Restore Now**.
- ACS displays a confirmation dialog box indicating that performing the restoration will restart ACS services and log out all administrators.
- Step 9** To continue with the restoration, click **OK**.
- ACS restores the system components that you specified by using the backup file that you selected. The restoration should require several minutes to finish, depending on the components that you selected to restore and the size of your database.
- When the restoration is complete, you can log in to ACS again.

ACS SE

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Restore**.
- The **ACS System Restore Setup** page appears.
- With the exception of the Decryption Password box, the boxes under Select Backup To Restore From contain the values that were used for the most recent successful backup, as configured on the ACS System Backup Setup page.
- Step 3** If you want to accept the default values for the FTP Server, Login, Password, Directory, and File boxes, proceed to step 5.
- Step 4** If you want to change any of the values in the FTP Server, Login, Password, Directory, and File boxes:
- In the **FTP Server** box under FTP Setup, enter the IP address or hostname of the FTP server from which you want ACS to get the backup file.
 - In the **Login** box under FTP Setup, enter a valid username to enable ACS to access the FTP server.
 - In the **Password** box under FTP Setup, enter the password for the username that you provided in the Login box.
 - In the **Directory** box under FTP Setup, enter the relative path to the directory on the FTP server that contains the backup file.
 - Click **Browse**.
- After a pause to retrieve a file list from the FTP server, a dialog box lists the ACS backup files found in the specified directory. Encrypted backup files include the lowercase letter *e* before the *.dmp* filename extension (*<filename>e.dmp*).



Tip If no files are found or the FTP server could not be accessed, click **Cancel** to close the dialog box, and repeat Step 4.

- Click the filename of the backup file that you want to use to restore ACS.
- The filename that you select appears in the File box, and the dialog box closes.

- Step 5** If the backup file specified that the File box is encrypted, enter the same password that was used to encrypt the backup file in the **Decryption Password** box.



Note The decryption password must exactly match the password that you specified in the Encryption Password box on the ACS System Backup Setup page.

- Step 6** To restore user and group database information, check the **User and Group Database** check box.
- Step 7** To restore system configuration information, check the **ACS System Configuration** check box.
- Step 8** To upgrade to ACS 4.2 using the ACS 4.1 backup file check the **Restore from 4.1 backup file to ACS 4.2**.
- Step 9** Click **Restore Now**.

ACS displays a confirmation dialog box indicating that performing the restoration will restart ACS services and log out all administrators.

- Step 10** To continue with the restoration, click **OK**.

ACS restores the system components that you specified by using the backup file that you selected. The restoration should require several minutes to finish, depending on the components that you selected to restore and the size of your database.

When the restoration is complete, you can log in to ACS again.

ACS Active Service Management

ACS Active Service Management is an application-specific service-monitoring tool that is tightly integrated with ACS. The two features that comprise ACS Active Service Management are described in this section.

This section contains:

- [System Monitoring, page 7-18](#)
- [Event Logging, page 7-20](#)

System Monitoring

You use ACS system monitoring to determine how often ACS tests its authentication and accounting processes, and to determine what automated actions to take if the tests detect a failure of these processes. ACS performs system monitoring with the CSMon service. For more information about the CSMon service, see [CSMon, page F-10](#).

System Monitoring Options

The options for configuring system monitoring are:

- **Test login process every X minutes**—Controls whether ACS tests its login process. The value in the X box defines, in minutes, how often ACS tests its login process. The default frequency is once per minute, which is also the most frequent testing interval possible.

When you enable this option, at the interval defined, ACS tests authentication and accounting. If the test fails, after four unsuccessful retries ACS performs the action identified in the **If no successful authentications are recorded** list and logs the event.



Note You can also create scripts in the *CSMon\Scripts* folder to run in case the test login fails.

- **If no successful authentications are recorded**—Specifies what action ACS takes if it detects that its test login process failed. This list contains several built-in actions and actions that you define. The items beginning with asterisks (*) are predefined actions:
 - ***Restart All**—Restart all ACS services.
 - ***Restart RADIUS/TACACS+**—Restart only the Proxy Remote Access Dial-In User Service (RADIUS) and TACACS+ services.
 - ***Reboot**—Reboot ACS.
 - **Custom actions** (ACS for Windows)—You can define other actions for ACS to take if failure of the login process occurs. ACS can execute a batch file or executable on the failure of the login process. To make a batch or executable file available in the on failure list, place the file in:

drive:\path\CSMon\Scripts

where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory.



Tip Restart CSAdmin to see the new batch file or executable in the list.

- **Take No Action** (both platforms)—Leave ACS operating as is.
- **Generate event when an attempt is made to log in to a disabled account**—Specifies whether ACS generates a log entry when a user attempts to log in to your network by using a disabled account.



Note You can also create scripts in the *CSMon\Scripts* folder to run in case the test login fails.

- **Log all events to the NT Event log** (ACS for Windows)—Specifies whether ACS generates a Windows event log entry for each exception event.
- **Email notification of event** (both platforms)—Specifies whether ACS sends an e-mail notification for each event.
 - **To**—The e-mail address to which a notification is sent; for example, *joeadmin@company.com*.
 - **SMTP Mail Server**—The simple mail transfer protocol (SMTP) server that ACS should use to send notification e-mail. You can identify the SMTP server by its hostname or IP address.

Setting Up System Monitoring

To set up ACS System Monitoring:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Service Management**.

The ACS Active Service Management Setup page appears.

- Step 3** To have ACS test the login process:
- Check the **Test login process every X minutes** check box.
 - Use the **X** box to enter the interval (up to 3 characters) between each login process test.
 - From the **If no successful authentications are recorded** list, select the action that ACS should take when the login test fails five successive times.
- Step 4** To generate a Windows event when a user tries to log in to your network by using a disabled account, check the **Generate event when an attempt is made to log in to a disabled account** check box.
- Step 5** If you want to set up event logging, see [Setting Up Event Logging, page 7-20](#).
- Step 6** If you are finished setting up ACS Service Management, click **Submit**.
- ACS implements the service-management settings that you made.
-

Event Logging

You use the Event Logging feature to configure whether ACS logs events to the Windows event log and ACS generates an e-mail when an event occurs. ACS uses the System Monitoring feature to detect the events to be logged. For more information about system monitoring, see [System Monitoring Options, page 7-18](#).

Setting Up Event Logging

To set up ACS event logging:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Service Management**.
- The ACS Active Service Management Setup page appears.
- Step 3** (ACS for Windows only) To have ACS send all events to the Windows event log, select **Log all events to the Windows Event log**.



Note

To view the Windows event log, choose **Start > Programs > Administrative Tools > Event Viewer**. For more information about the Windows event log or Event Viewer, refer to your Microsoft Windows documentation.

- Step 4** (Both platforms) To have ACS send an e-mail when an event occurs:
- Check the **Email notification of event** check box.
 - In the **To** box, enter the e-mail address (up to 200 characters) to which ACS should send event notification e-mail.



Note

Do not use underscores (_) in the e-mail addresses that you enter in this box.

- In the **SMTP Mail Server** box, enter the hostname (up to 200 characters) of the sending e-mail server.

**Note**

The SMTP mail server must be operational and must be available from the ACS.

- Step 5** If you want to set up system monitoring, see [Setting Up System Monitoring, page 7-19](#).
- Step 6** If you are finished setting up ACS Service Management, click **Submit**.
ACS implements the service-management settings that you made.

VoIP Accounting Configuration

You use the voice over IP (VoIP) Accounting Configuration feature to specify which accounting logs receive VoIP accounting data. The options for VoIP accounting are:

- **Send to RADIUS and VoIP Accounting Log Targets**—ACS appends VoIP accounting data to the RADIUS accounting data and logs it separately to a CSV file. To view the data, you can use RADIUS Accounting or VoIP Accounting under **Reports** and **Activity**.
- **Send only to VoIP Accounting Log Targets**—ACS only logs VoIP accounting data to a CSV file. To view the data, you can use VoIP Accounting under Reports and Activity.
- **Send only to RADIUS Accounting Log Targets**—ACS only appends VoIP accounting data to the RADIUS accounting data. To view the data, you can use RADIUS Accounting under Reports and Activity.

Configuring VoIP Accounting

**Note**

If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Voice-over-IP (VoIP) Accounting Configuration** check box. See [Chapter 2, “Advanced Options \(for Interface Configuration\)”](#) for more information.

To configure VoIP accounting:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **VoIP Accounting Configuration**.
The VoIP Accounting Configuration page appears. The Voice-over-IP (VoIP) Accounting Configuration table displays the options for VoIP accounting.
- Step 3** Select the VoIP accounting option that you want.
- Step 4** Click **Submit**.
ACS implements the VoIP accounting configuration that you specified.

Appliance Configuration (ACS SE Only)

You use the Appliance Configuration page to set the ACS hostname, domain names, system date, and time. If you are using an appliance base image that incorporates the CSA or have applied a CSA update to ACS, you can use the Appliance Configuration page to enable and disable the **CSAgent** service.

This section contains:

- [Enabling or Disabling CSAgent, page 7-22](#)
- [Configuring SNMP Support, page 7-23](#)
- [Configuring SNMP Support, page 7-23](#)
- [Setting System Time and Date, page 7-23](#)
- [Setting the ACS Host and Domain Names, page 7-24](#)
- [Enabling or Disabling CSAgent, page 7-22](#)

Enabling or Disabling CSAgent



Note

The CSA section appears only if you are using appliance base image 3.3.1.3 or later or if you have applied the CSA update to the appliance.

You enable or disable the protection and restrictions imposed by the CSA on an appliance by enabling or disabling **CSAgent**. Disabling **CSAgent** is necessary for:

- Upgrading or applying patches to ACS.
- Allowing the appliance to respond to ping requests.



Note

When **CSAgent** is disabled, the CSA no longer protects the appliance. For information on CSA protection, see [Cisco Security Agent Policies, page 1-18](#).

When you disable **CSAgent**, it remains disabled until you explicitly re-enable it. Rebooting the appliance does not restart a disabled **CSAgent** service.

To enable or disable **CSAgent** on the appliance:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Appliance Configuration**.

ACS displays the Appliance Configuration page.



Note

If the system does not display the Appliance Configuration page, check connectivity to the ACS.

Step 3 Check or clear the **CSA Enabled** check box, as applicable.

Step 4 Click **Submit**.


ACS enables or disables **CSAgent**.

Configuring SNMP Support

You use the SNMP support in ACS SE to monitor information for the appliance, such as, processes, memory, CPU utilization, version of the appliance and ACS software version, ethernet interface status, and so on.

To configure the SNMP Agent, choose **System Configuration > Appliance Configuration** from the navigation bar.

To configure SNMP Agent settings:

-
- Step 1** Check the **SNMP Agent Enabled** check box. The default is enabled.
- Step 2** In the **SNMP Communities** box, enter the community strings for SNMP. With the exception of the comma(,), all characters are valid. You must use a comma (,) separator between community strings.
-  **Note** An SNMP client cannot retrieve information from ACS SE if the SNMP Communities field is empty.
-
- Step 3** In the **SNMP Port** box, enter the connectivity port number.
- Step 4** In the **Contact** box, enter the name of the network administrator.
- Step 5** In the **Location** box, enter the location of the device.
- Step 6** Check the **Accept SNMP packets from select hosts** check box if you want to restrict the requests that the SNMP agent accepts to a list of specific SNMP client host addresses.
- Step 7** In the **Host Addresses** box, enter the specific SNMP client host addresses. You must use a comma (,) delimiter between host addresses.
-

Setting System Time and Date

Use this procedure to set the system time and date from the web interface. In addition, you can use this procedure to maintain the system time and date by using a network time protocol (NTP) server that the system can use to automatically synchronize time and date.



Tip

You can also use the serial console to perform this procedure. For details, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

To set the system date and time:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Appliance Configuration**.
- ACS displays the Appliance Configuration page.



Note If the system does not display the Appliance Configuration page, check connectivity to ACS.

- Step 3** From the **Time Zone** list, select the system time zone.

- Step 4** In the **Time** box, enter the system time in the format hh:mm:ss.
- Step 5** From the **Day** list, select the day of the month.
- Step 6** From the **Month** list, select the month.
- Step 7** From the **Year** list, select the year.
- Step 8** Perform the following substeps only if you want to set up the NTP server to automatically synchronize time and date.
- Check the **NTP Synchronization Enabled** check box.
 - In the **NTP Server(s) box**, enter the IP address or addresses of the NTP server(s) that you want the system to use. If you enter more than one, separate the IP addresses with a space.

**Note**

Be sure that the IP addresses that you specify belong to valid NTP servers. Incorrect IP addresses or incorrectly operating NTP servers can greatly slow the NTP synchronization process.

- Step 9** Click **Submit**.
- The system time and date are set.


Setting the ACS Host and Domain Names

Use this procedure to configure ACS host and domain names.

**Note**

This procedure requires that you reboot the ACS. You should perform this procedure during off hours to minimize disruption of users.

To set the ACS host and domain names:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Appliance Configuration**.
- ACS displays the Appliance Configuration page.
-  **Note** If the system does not display the Appliance Configuration page, check connectivity to ACS.
- Step 3** In the **Host Name** box, enter the hostname.
- Step 4** In the **Domain Name** box, enter the domain name.
- Step 5** At the bottom of the page, click **Submit** and then click **Reboot**.

Support Page

You use the Support page for two purposes:

- To package system state information into a file that can be forwarded to the Cisco Technical Assistance Center.
- To monitor the state of ACS services.

Each of these activities is detailed in the following sections:

- [Running Support, page 7-25](#)
- [Monitoring System Information, page 7-26](#)

This section contains:

- [Running Support, page 7-25](#)
- [Monitoring System Information, page 7-26](#)

Running Support

You can use the Support page to package system information for forwarding to your Technical Assistance Center (TAC) representative. When you perform this procedure, ACS automatically packages all current logs.

You also have the options to package:

- The user database.
- System logs for the number of preceding days that you specify.
- Diagnostic logs

Support information is packaged in a cabinet file, which has the file extension `.cab`. Cabinet files are compressed so that you can more easily send the support information.



Note AAA services are briefly suspended when you run the **Support** procedure. We recommend that you perform this procedure during periods of least AAA activity to minimize user impact.

To package system state information into a file for the Cisco Technical Assistance Center:

-
- | | |
|---------------|---|
| Step 1 | In the navigation bar, click System Configuration . |
| Step 2 | Click Support .
The Support page appears. |
| Step 3 | If you want to download diagnostic log information, check the Collect Log Files check box. If you select this option, ACS services are not restarted during the generation of package.cab. See Viewing or Downloading Diagnostic Logs (ACS SE Only), page 7-27 for more information about diagnostic log information for the appliance only. |
| Step 4 | If you want to include the ACS internal database in the support file, check the Collect User Database check box in the Details to collect table. |
| Step 5 | If you want to include archived system logs:
a. Check the Collect Previous X Days logs check box. |

**Note**

If you want the support information to be downloaded to include service log files that are older than the current log files, check the **Collect Previous X Days logs** check box and type the number of days of log files to be included. For example, if you want an archived copy of the *Backup and Restore.csv* log to be included, type the number of days prior to today that you want ACS to look for *Backup and Restore.csv* files. The current log file may not be today's date. It is the current one, which may be several days older than today's date.

- b. In the *X* box, enter the number of preceding days for which you want logs collected. The maximum number of preceding days is 9999.

Step 6 Click **Run Support Now**.

The File Download dialog box appears.

Step 7 On the **File Download** dialog box, click **Save**.

The Save As dialog box appears.

Step 8 Use the **Save As** dialog box to specify the path and filename for the cabinet file. Then click **Save**.

ACS briefly suspends normal services while a support file is generated and saved. When the download is complete, a ACS displays the Download Complete dialog box.

Step 9 You should make note of the name and location of the support file, and then click **Close**.

A current cabinet file of support information is written to the location that you specified. You can forward it as needed to a TAC representative or other Cisco support personnel.

Monitoring System Information

You use this procedure to monitor the status and distribution of ACS resources. The top row in the Resource Usage table displays CPU idle resource percentage and available memory space. The remainder of the Resource Usage table shows the following allocations for each service:

- **CPU**—The percentage of CPU cycles being used. In the System category, ACS numbers the CPUs, starting with zero (0). If there is more than one CPU, the System category displays CPU information for each CPU.
- **Memory**—The amount of memory allocated by each service.
- **Handle count**—The number of system handles (that is, resources) allocated by each service.
- **Thread count**—The number of threads spawned by each service.

To monitor the status of the ACS services:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Support**.

ACS displays the Support page.

Step 3 Read system information in the Resource Usage table.

**Tip**

The first row of the Resource Usage table, marked System, displays the percentage of CPU cycles that are idle. Other rows indicate the percentage of CPU cycles used by each service. The total is 100 percent.

Viewing or Downloading Diagnostic Logs (ACS SE Only)

ACS records diagnostic logs whenever you apply upgrades or patches to the software that is running on the appliance. ACS also creates a diagnostic log if you use the recovery CD to restore the appliance to its original state.

In addition, if you are using an appliance base image that incorporates the CSA or have applied a CSA update to ACS, the View Diagnostic Logs page provides access to two logs that the CSA creates.

To view or download an appliance diagnostic log:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **View Diagnostic Logs**.

ACS displays the View Diagnostic Logs page:

- In the Log File column, the log files are listed by name.
- In the File Size column, the size of each log file appears (in kilobytes).

If ACS failed to create an expected log file, a `Log file is not created` message appears in the File Size column.

Step 3 If you want to download a diagnostic log, right click on the log filename and use the applicable browser feature to save the log.

A copy of the log file is now available for viewing in a third-party application, such as Microsoft Excel or a text editor. If requested, you can also send the diagnostic log file to Cisco support technicians.

Step 4 If you want to view a diagnostic log, click on the log filename.

ACS displays the contents of the diagnostic log.

Appliance Upgrade Mechanism (ACS SE Only)

This section contains:

- [About Appliance Upgrades and Patches, page 7-28](#)
- [Distribution Server Requirements, page 7-29](#)
- [Upgrading an Appliance, page 7-29](#)
- [Transferring an Upgrade Package to an Appliance, page 7-30](#)
- [Applying an Upgrade to an Appliance, page 7-33](#)

About Appliance Upgrades and Patches

All upgrades and patches for ACS are packaged using the upgrade mechanism. For more information about installing ACS 4.2, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.



Note

To upgrade to the ACS 4.2 release, you will need to reimage the appliance with the 4.2 recovery CD and then restore the ACS 4.1 database. The upgrade to ACS 4.2 includes the Windows 2003 Operating System upgrade.

Use the following three-phase process to upgrade or patch your existing ACS.

- **Phase one**—Obtain an upgrade package and load it onto a computer designated as a distribution server for ACS upgrade distribution. You can obtain the upgrade package as a CD-ROM or as a file that you download from Cisco.com.
- **Phase two**—Transfer installation package files from the distribution server to the appliance. The HTTP server, which is part of the installation package, performs file transfer. The upgrade files are signed and the signature is verified after uploading to ensure that the files have not been corrupted.
- **Phase three**—Apply the upgrade to the appliance. Before the upgrade files are applied to the appliance, ACS verifies the digital signature on the files to ensure their authenticity and to verify that they are not corrupt.

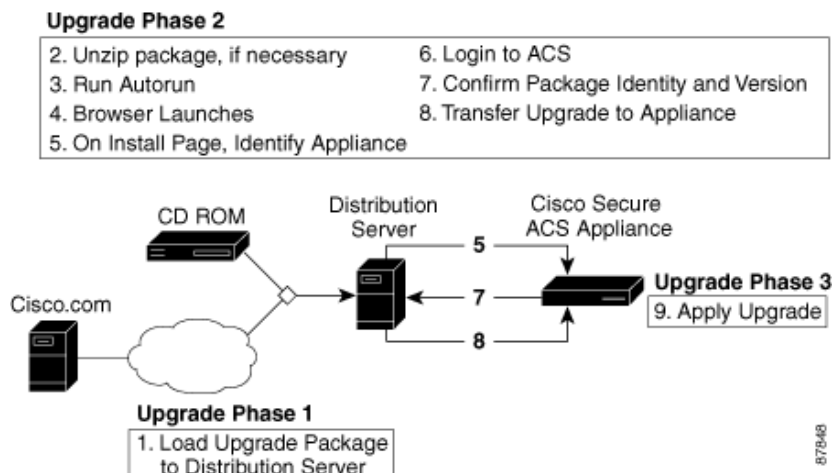


Note

While you apply the upgrade, ACS cannot provide AAA services. If it is not critical to immediately apply an upgrade package, you should consider performing this phase when ACS downtime will have the least impact on users. For example, when you apply the upgrade, it will stop the AAA servers, apply the new patch, and then restart the AAA servers again.

Figure 7-1 summarizes the process.

Figure 7-1 Appliance Upgrade Process



Distribution Server Requirements

The distribution server must meet the following requirements:

- For support, the distribution server must use an English-language version of one of the following operating systems:
 - Windows Server 2003 R2, Enterprise Edition
 - Windows 2000 Server with Service Pack 3 installed
 - Windows XP Professional with Service Pack 1 installed
 - Solaris 2.8

**Note**

While the upgrade process may succeed by using an unsupported operating system, the list reflects the operating systems that we used to test the upgrade process. We do not support upgrades from distribution servers that use untested operating systems.

- If you acquire the upgrade package on CD, the distribution server must have a CD-ROM drive or must be able to use the CD-ROM drive on another computer that you can access.
- TCP port 8080 should not be in use on the distribution server. The upgrade process requires exclusive control of port 8080.

**Tip**

We recommend that no other web server runs on the distribution server.

- A supported web browser should be available on the distribution server. If necessary, you can use a web browser on a different computer than the distribution server. For a list of supported browsers, see the *Release Notes for Cisco Secure ACS Release 4.2*. The most recent revision to the Release Notes is posted on Cisco.com.

Gateway devices between the distribution server and any appliance that you want to upgrade must permit HTTP traffic to the distribution server on port 8080. They must also permit an ACS remote administrative session; therefore, they must permit HTTP traffic to the appliance on port 2002 and the range of ports allowed for administrative sessions. For more information, see [HTTP Port Allocation for Administrative Sessions, page 1-19](#).

Upgrading an Appliance

Use the information in this section to upgrade the appliance software.

Before You Begin

Always back up ACS before upgrading. For information on backing up ACS, see [ACS Backup, page 7-8](#).

To upgrade an appliance:

Step 1

Acquire the upgrade package. Acquisition of an upgrade package differs depending on the type of upgrade package and service agreement. For:

- **Commercial upgrade packages**—Contact your Cisco sales representative.
- **Maintenance contracts**—You may be able to download upgrade packages from Cisco.com. Contact your Cisco sales representative.

- **Upgrade packages that apply patches for specific issues**—Contact your TAC representative.

- Step 2** Choose a computer to use as the distribution server. The distribution server must meet the requirements discussed in [Distribution Server Requirements, page 7-29](#).
- Step 3** If you have acquired the upgrade package in a compressed file format, such as a *.zip* or *.gz*:
- If you have not already done so, copy the upgrade package file to a directory on the distribution server.
 - Use the appropriate file decompression utility to extract the upgrade package.

**Tip**

Consider extracting the upgrade package in a new directory that you create for the contents of the upgrade package.

- Step 4** If you have acquired the upgrade package on CD, do not insert the CD in a CD-ROM drive until instructed to do so. The CD contains *autorun* files, and if the distribution server uses Microsoft Windows, the CD-ROM drive can prematurely start the *autorun* process.
- Step 5** Transfer the upgrade package to an appliance. For detailed steps, see [Transferring an Upgrade Package to an Appliance, page 7-30](#).
- The upgrade package is now on the appliance and ready to be applied.
- Step 6** If the CSA is running on the appliance, disable the CSA. For detailed steps, see [Enabling or Disabling CSAgent, page 7-22](#).
- Step 7** Apply the upgrade package to the appliance. For detailed steps, see [Applying an Upgrade to an Appliance, page 7-33](#).
- ACS applies the upgrade and runs using the upgraded software.
- Step 8** If you want the CSA to protect the appliance, enable it. For detailed steps, see [Enabling or Disabling CSAgent, page 7-22](#).

**Note**

System restarts performed during the upgrade do not re-enable **CSAgent**.

Transferring an Upgrade Package to an Appliance

Use this procedure to transfer an upgrade package from a distribution server to an appliance.

**Note**

After you have performed this procedure, you must still apply the upgrade for it to become effective. For information on applying the upgrade, see [Applying an Upgrade to an Appliance, page 7-33](#). For more general information about the upgrade process, see [About Appliance Upgrades and Patches, page 7-28](#).

Before You Begin

You must have acquired the upgrade package and selected a distribution server. For more information, see [Upgrading an Appliance, page 7-29](#).

To transfer an upgrade to your appliance:

Step 1 If the distribution server uses Solaris, go to Step 2. If the distribution server uses Microsoft Windows:

- a. If you have acquired the upgrade package on CD, insert the CD in a CD-ROM drive on the distribution server.



Tip

You can also use a shared CD drive on a different computer. If you do so and *autorun* is enabled on the shared CD drive, the HTTP server included in the upgrade package starts on the other computer. For example, if computer A and computer B share a CD drive, and you use the CD drive on computer B where *autorun* is also enabled, the HTTP server starts on computer B.

- b. If either of the following conditions is true:
 - You have acquired the upgrade package as a compressed file.
 - *autorun* is not enabled on the CD-ROM drive.

Locate the *autorun.bat* file on the CD or in the directory to which you extracted the compressed upgrade package, and start the *autorun*.

- c. The HTTP server starts, messages from *autorun.bat* appear in a console window, and ACS displays the following two browser windows:
 - Use **Appliance Upgrade** to enter the appliance hostname or IP address.
 - Use **New Desktop** to start transfers to other appliances.

Step 2 If the distribution server uses Sun Solaris:

- a. If you have acquired the upgrade package on CD, insert the CD in a CD-ROM drive on the distribution server.
- b. Locate the *autorun.sh* file on the CD or in the directory to which you extracted the compressed upgrade package.
- c. Run *autorun.sh*.



Tip

If *autorun.sh* has insufficient permissions, enter `chmod +x autorun.sh` and repeat Step c.

- d. The HTTP server starts, messages from *autorun.bat* appear in a console window, and the following two browser windows appear:
 - Use **Appliance Upgrade** to enter the appliance hostname or IP address.
 - Use **New Desktop** to start transfers to other appliances.

Step 3 If no web browser opens after you have run the *autorun* file, start a web browser on the distribution server and open the following URL:

`http://127.0.0.1:8080/install/index.html`



Tip

You can access the HTTP server on the distribution server from a web browser on a different computer using the following URL: `http://IP address:8080/install/index.html`, where *IP address* is the IP address of the distribution server.

Step 4 In the Appliance Upgrade browser window, enter the appliance IP address or hostname in the **Enter appliance hostname or IP address** box, and click **Install**.

The ACS login page for the specified appliance appears.

Step 5 Log in to the ACS web interface:

- a. In the **Username** box, enter a valid ACS administrator name.
- b. In the **Password** box, enter the password for the ACS administrator.
- c. Click **Login**.

Step 6 In the navigation bar, click **System Configuration**.

Step 7 Click **Appliance Upgrade Status**.

ACS displays the Appliance Upgrade page.

Step 8 Click **Download**.

ACS displays the Appliance Upgrade Form page. This page contains the Transfer Setup table, which you use to identify the distribution server.

Step 9 In the **Install Server** box, enter the hostname or IP address of the distribution server.

Step 10 Click **Connect**.

The Appliance Upgrade Form page displays the Software Install table, which details the version and name of the upgrade available from the distribution server.

Step 11 Examine the Software Install table to confirm that the version, name, and condition of the upgrade is satisfactory, and click **Download Now**.

ACS displays the Appliance Upgrade page and the upgrade file is downloaded from the distribution server to the appliance. ACS displays the status of the download below the Appliance Versions table.



Tip

On the Appliance Upgrade page, the system displays the message *Distribution Download in Progress*, followed by the number of downloaded kilobytes.

Step 12 If you want to update the transfer status message, click **Refresh**. **Refresh** exhibits the following behavior:



Tip

During the transfer, you can click **Refresh** as often as necessary to update the status message.

- If you click **Refresh**

While the transfer is in progress, ACS displays the number of downloaded kilobytes.

After the transfer is complete, ACS displays the Apply Upgrade button and the transfer progress text is replaced with a message indicating that an upgrade package is available on the appliance.

Step 13 To ensure that the download was successful and the upgrade is ready to be applied, confirm that the following message appears on the Appliance Upgrade page: *Ready to Upgrade to version*, where *version* is the version of the upgrade package you have transferred to the appliance.

The upgrade package is now successfully transferred to the appliance.

Step 14 If you want to transfer the upgrade package to another appliance, access the browser window titled **New Desktop**, click **Install Next**, and return to Step 4.



Tip

If you know the URL for the web interface of another appliance, you can enter it in the browser location box and return to Step 5 to transfer the upgrade package to that appliance.

- Step 15** If you are finished transferring upgrade packages to appliances, access the browser window titled **New Desktop** and click **Stop Distribution Server**.
- The HTTP server stops and the distribution server releases the resources that the HTTP server used.
- Step 16** If you want to apply the upgrade, perform the steps in [Applying an Upgrade to an Appliance, page 7-33](#). Alternatively, you can use the **upgrade** command by using the serial console. For more information about the **upgrade** command, see *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.
-

Applying an Upgrade to an Appliance

You use this procedure to apply an upgrade package to an ACS.



Note

As an alternative, you can apply an upgrade package by using the **upgrade** command on the serial console. For more information, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Before You Begin

Before you apply the upgrade:

- Transfer the upgrade package to the appliance. For detailed steps, see [Transferring an Upgrade Package to an Appliance, page 7-30](#). For the steps required to upgrade an appliance, see [Upgrading an Appliance, page 7-29](#).
- Back up ACS. For information about backing up ACS, see [ACS Backup, page 7-8](#).
- Disable the **CSAgent** service. Application of the upgrade will fail if **CSAgent** is running. For detailed steps, see [Enabling or Disabling CSAgent, page 7-22](#).



Note

During the upgrade, ACS cannot provide AAA services. If it is not critical to immediately apply an upgrade package, consider performing this procedure when ACS downtime will have the least impact on users.

To apply an upgrade to an ACS:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Appliance Upgrade Status**.
- ACS displays the Appliance Upgrade page.
- Step 3** Verify that the message *Ready to Upgrade to version* appears, where *version* is the version of the upgrade package that is available on the appliance.
- Step 4** Click **Apply Upgrade**.
- ACS displays the Apply Upgrade Message table. This table displays messages about the upgrade process.
- Step 5** For each message that ACS displays, you should carefully read the message and click the appropriate button.

**Caution**

You might receive a warning message that an upgrade package is not verified. Before applying an upgrade or patch, ACS attempts to verify that the upgrade or patch is Cisco certified. Some valid upgrade packages might not pass this verification, such as patches distributed for an urgent fix. Do not apply an upgrade package if you have unresolved concerns about the validity of the upgrade package.

After you have answered all confirmation prompts, ACS applies the upgrade. Be aware that:

- During an upgrade, ACS services and the web interface are not available. When the upgrade is complete, the ACS services and the web interface become available.
- Application of an upgrade can take several minutes. A full upgrade of ACS takes longer if the ACS internal database contains a large number of user profiles.
- Upgrade of ACS usually requires the appliance to restart itself once or twice. Smaller patches might not require restarts.
- If the browser window is open and the web interface is not available, wait for the appliance to resume normal operation. Then close the original browser window, open a new browser window, and log in to ACS.

**Caution**

Do not reset the appliance during application of an upgrade unless the TAC directs you to do so.

Step 6

After application of the upgrade, go to the Appliance Upgrade page and verify the versions of the software on the appliance. The Appliance Versions table lists the versions of software running on the appliance. Table entries should reflect the upgrade package that you applied.

**Note**

If the browser window is open and the web interface is not available, wait for the appliance to resume normal operation. Then close the original browser window, open a new browser window, and log in to ACS.



CHAPTER 8

System Configuration: Advanced

This chapter addresses the ACS internal database replication and RDBMS synchronization features in the System Configuration section of the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

This chapter contains the following sections:

- [ACS Internal Database Replication, page 8-1](#)
- [RDBMS Synchronization, page 8-17](#)
- [IP Pools Server, page 8-39](#)
- [IP Pools Address Recovery, page 8-44](#)
- [NAC Attribute Management \(ACS SE Only\), page 8-44](#)

ACS Internal Database Replication

This section provides information about the ACS internal database replication feature, including procedures for implementing this feature and configuring the ACSs involved.



Note

ACS does not support distributed deployments in a NAT environment. If a Primary or Secondary address is NAT-configured, the database replication file will indicate shared secret mismatch.

This section contains:

- [About ACS Internal Database Replication, page 8-2](#)
 - [Replication Process, page 8-3](#)
 - [Replication Frequency, page 8-5](#)
- [Important Implementation Considerations, page 8-5](#)
- [Database Replication Versus Database Backup, page 8-6](#)
- [Database Replication Logging, page 8-7](#)
- [Replication Options, page 8-7](#)
 - [Replication Components Options, page 8-7](#)
 - [Outbound Replication Options, page 8-9](#)
 - [Inbound Replication Options, page 8-10](#)

- [Implementing Primary and Secondary Replication Setups on ACSs, page 8-10](#)
- [Configuring a Secondary ACS, page 8-11](#)
- [Replicating Immediately, page 8-13](#)
- [Scheduling Replication, page 8-14](#)
- [Disabling ACS Database Replication, page 8-16](#)
- [Configuring Automatic Change Password Replication, page 8-16](#)
- [Database Replication Event Errors, page 8-17](#)

About ACS Internal Database Replication

Database replication creates mirror systems of ACSs by duplicating parts of the primary ACS setup to one or more secondary ACSs. You can configure your AAA clients to use these secondary ACSs if the primary ACS fails or is unreachable. With a secondary ACS whose ACS internal database is a replica of the ACS internal database on the primary ACS, if the primary ACS goes out of service, incoming requests are authenticated without network downtime, provided that your AAA clients are configured to fail over to the secondary ACS.

You can use database replication to:

- Select the parts of the primary ACS configuration to be replicated.
- Control the timing of the replication process, including creating schedules.
- Export selected configuration items from the primary ACS.
- Securely transport selected configuration data from the primary ACS to one or more secondary ACSs.
- Update the secondary ACSs to create matching configurations.

The following items cannot be replicated:

- IP pool definitions (for more information, see [About IP Pools Server, page 8-39](#)).
- ACS certificate and private key files.
- Unknown user group mapping configuration.
- Dynamically-mapped users.
- Settings on the ACS Service Management page in the System Configuration section.
- RDBMS Synchronization settings.



Tip

For a list of the various components and what database replication encompasses, see [Replication Components Options, page 8-7](#).

With regard to database replication, we make the following distinctions about ACSs:

- **Primary ACS**—An ACS that sends replicated ACS internal database components to other ACSs.
- **Secondary ACS**—An ACS that receives replicated ACS internal database components from a primary ACS. In the web interface, these are identified as replication partners.

An ACS can be a primary ACS and a secondary ACS, provided that it is not configured to be a secondary ACS to an ACS for which it performs as a primary ACS.

**Note**

Bidirectional replication, wherein an ACS sends database components to and receives database components from the same remote ACS, is not supported. Replication fails if an ACS is configured to replicate to and from the same ACS.

**Note**

All ACSs that are involved in replication must run the same release of the ACS software. For example, if the primary ACS is running ACS version 3.2, all secondary ACSs should be running ACS version 3.2. Because patch releases can introduce significant changes to the ACS internal database, we strongly recommend that ACSs involved in replication use the same patch level.

Replication Process

This topic describes the process of database replication, including the interaction between a primary ACS and each of its secondary ACSs. The following steps occur in database replication:

1. The primary ACS determines if its database has changed since the last successful replication. If it has, replication proceeds. If it has not, replication is aborted. No attempt is made to compare the databases of the primary and secondary ACSs.

**Tip**

You can force replication to occur by making one change to a user or group profile, such as changing a password or modifying a RADIUS attribute.

2. The primary ACS contacts the secondary ACS. In this initial connection, the following four events occur:
 - a. The two ACSs perform mutual authentication based on the shared secret of the primary ACS. If authentication fails, replication fails.

**Note**

On the secondary ACS, the AAA Servers table entry for the primary ACS must have the same shared secret that the primary ACS has for itself in its own AAA Servers table entry. The shared secret of the secondary ACS is irrelevant.

- b. The secondary ACS verifies that it is not configured to replicate to the primary ACS. If it is, replication is aborted. ACS does not support bidirectional replication, wherein an ACS can act as a primary and a secondary ACS to the same remote ACS.
 - c. The primary ACS verifies that the version of ACS that the secondary ACS is running is the same as its own version of ACS. If not, replication fails.
 - d. The primary ACS compares the list of database components that it is configured to send with the list of database components that the secondary ACS is configured to receive. If the secondary ACS is not configured to receive any of the components that the primary ACS is configured to send, the database replication fails.
3. After the primary ACS has determined which components to send to the secondary ACS, the replication process continues on the primary ACS:
 - a. The primary ACS stops its authentication and creates a copy of the ACS internal database components that it is configured to replicate. During this step, if AAA clients are configured properly, those that usually use the primary ACS fail over to another ACS.

- b. The primary ACS resumes its authentication service. It also compresses and encrypts the copy of its database components for transmission to the secondary ACS.
 - c. The primary ACS transmits the compressed, encrypted copy of its database components to the secondary ACS. This transmission occurs over a TCP connection by using port 2000. The TCP session uses a 128-bit encrypted, Cisco-proprietary protocol.
4. After the preceding events on the primary ACS, the database replication process continues on the secondary ACS:
 - a. The secondary ACS receives the compressed, encrypted copy of the ACS internal database components from the primary ACS. After transmission of the database components is complete, the secondary ACS decompresses the database components.
 - b. The secondary ACS stops its authentication service and replaces its database components with the database components that it received from the primary ACS. During this step, if AAA clients are configured properly, those that usually use the secondary ACS fail over to another ACS.
 - c. The secondary ACS resumes its authentication service.

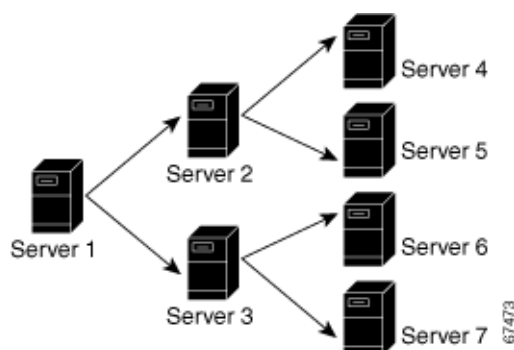
ACS can act as a primary ACS and a secondary ACS. [Figure 8-1](#) shows a cascading replication scenario. Server 1 acts only as a primary ACS, replicating to servers 2 and 3, which act as secondary ACSs. After replication from server 1 to server 2 has completed, server 2 acts as a primary ACS while replicating to servers 4 and 5. Similarly, server 3 acts as a primary ACS while replicating to servers 6 and 7.

**Note**

If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary ACS. In [Figure 8-1](#), server 1 must have an entry in its AAA Servers table for each of the other six ACSs. If this is not done, after replication, servers 2 and 3 do not have servers 4 through 7 in their AAA Servers tables and replication will fail.

If server 2 were configured to replicate to server 1 in addition to receiving replication from server 1, replication to server 2 would fail. ACS cannot support such a configuration, known as bidirectional replication. To safeguard against this, a secondary ACS aborts replication when its primary ACS appears on its Replication list.

Figure 8-1 Cascading Database Replication



Replication Frequency

The frequency with which your ACSs replicate can have important implications for overall AAA performance. With shorter replication frequencies, a secondary ACS is more up to date with the primary ACS. This frequency produces a more current secondary ACS if the primary ACS fails.

Frequent replications incur a cost. The more frequent the replication, the higher the load on a multi-ACS architecture and your network environment. If you schedule frequent replications, network traffic is much higher. Also, processing load on the replicating systems is increased. Replication consumes system resources and briefly interrupts authentication; thus the more often replication occurs, the greater the impact on the AAA performance of the ACS. And because service is momentarily interrupted on both servers, NAS failovers can occur.

**Note**

Regardless of how frequently replication is scheduled to occur, it only occurs when the database of the primary ACS has changed since the last successful replication.

This issue is more apparent with databases that are large or frequently change. Database replication is a nonincremental, destructive backup. In other words, it completely replaces the database and configuration on the secondary ACS every time it runs. Therefore, a large database results in substantial amounts of data being transferred, and the processing overhead can also be large.

Important Implementation Considerations

Several important points to consider when you implement the ACS Database Replication feature are:

- ACS only supports database replication to other ACSs. All ACSs participating in ACS internal database replication must run the same version of ACS. We strongly recommend that ACSs that are involved in replication use the same patch level, too.
- You must ensure correct configuration of the AAA Servers table in all ACSs that are involved in replication.
 - In its AAA Servers table, a primary ACS must have an accurately configured entry for each secondary ACS.

**Note**

If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from that primary ACS. For example, if the primary ACS replicates to two secondary ACSs, which, in turn, each replicate to two more ACSs, the primary ACS must have AAA server configurations for all six ACSs that will receive replicated database components.

- In its AAA Servers table, a secondary ACS must have an accurately configured entry for each of its primary ACSs.
- On a primary ACS and all its secondary ACSs, the AAA Servers table entries for the primary ACS must have identical shared secrets.
- Only suitably configured, valid ACSs can be secondary ACSs. To configure a secondary ACS for database replication, see [Configuring a Secondary ACS, page 8-11](#).

- Replication only occurs when the database of the primary ACS has changed since the last successful replication, regardless of how frequently replication is scheduled to occur. When a scheduled or manually started replication begins, the primary ACS automatically aborts replication if its database has not changed since the last successful replication.

**Tip**

You can force replication to occur by making one change to a user or group profile, such as changing a password or modifying a RADIUS attribute.

- Replication to secondary ACSs occurs sequentially in the order listed in the Replication list under Replication Partners on the ACS Database Replication page.
- You must configure a secondary ACS that is receiving replicated components to accept database replication from the primary ACS. To configure a secondary ACS for database replication, see [Configuring a Secondary ACS, page 8-11](#).
- ACS does not support bidirectional database replication. The secondary ACS that receives the replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it rejects the components.
- For all components (except for Network Access Profiles), if you replicate user accounts, ensure that you name external database configurations identically on primary and secondary ACSs. A replicated user account retains its association with the database that is assigned to provide authentication or posture validation service, regardless of whether a database configuration of the same name exists on the secondary ACS. For example, if user account is associated with a database named **WestCoast LDAP**; on the primary ACS, the replicated user account on all secondary ACSs remains associated with an external user database named **WestCoast LDAP** even if you have not configured an LDAP database instance of that name.
- For all components (except for Network Access Profiles), in order to replicate user and group settings that use user-defined RADIUS vendor and VSAs, you must manually add the user-defined RADIUS vendor and VSA definitions on primary and secondary ACSs, ensuring that the RADIUS vendor slots that the user-defined RADIUS vendors occupy are identical on each ACS. After you have done so, replication of settings by using user-defined RADIUS vendors and VSAs is supported. For more information about user-defined RADIUS vendors and VSAs, see [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#).

Database Replication Versus Database Backup

Do not confuse database replication with system backup. Database replication does *not* replace System Backup. While both features protect against partial or complete server loss, each feature addresses the issue in a different way:

- System Backup archives data into a format that you can later use to restore the configuration if the system fails or the data becomes corrupted. The backup data is stored on the local hard drive, and can be copied and removed from the system for long-term storage. You can store several generations of database backup files.
- You use ACS Database Replication to copy various components of the ACS internal database to other ACSs. This method can help you plan a failover AAA architecture, and reduce the complexity of your configuration and maintenance tasks. While unlikely, it is possible that ACS Database Replication can propagate a corrupted database to the ACSs that generate your backup files.

**Caution**

Because the possibility of replicating a corrupted database always exists, we strongly recommend that you implement a backup plan, especially in mission-critical environments. For more information about backing up the ACS internal database, see [ACS Backup, page 7-8](#). For additional information (ACS for Windows), see [Appendix C, “CSUtil Database Utility.”](#)

Database Replication Logging

ACS logs all replication events—regardless of whether they are successful—in two files. The:

- Windows Event Log
- Database Replication report

To view the Windows Event Log, use the Windows administration utilities. You can view recent reports in the Reports and Activity section of ACS.

For more information about ACS reports, see [Chapter 1, “Overview.”](#)

Replication Options

The ACS web interface provides three sets of options for configuring ACS Database Replication.

This section contains:

- [Replication Components Options, page 8-7](#)
- [Outbound Replication Options, page 8-9](#)
- [Inbound Replication Options, page 8-10](#)

Replication Components Options

You can specify the ACS internal database components that an ACS sends as a primary ACS and the components that it receives as a secondary ACS.

For increased security, you might want to have one ACS always be the sender and the other ACSs always be the receivers. You can use this method to ensure that all your ACSs are configured identically.

**Note**

The ACS internal database components that a secondary ACS receives *overwrite* the ACS internal database components on the secondary ACS. Any information that is unique to the overwritten database component is lost. For example, if the Receive check box is selected for the User and Group Database, any existing user or group records are lost on replication when the new ACS internal database is received.

[Table 8-1](#) describes the Replication Components table on the ACS Database Replication page and describes the component options that are replicated.

Table 8-1 Replication Component Descriptions

Component	What Gets Replicated?
User and group database	Groups and users. Excludes the use of the Group database only option.
Group database only	Groups, but not for users. Excludes the use of the User and group database option.
Network Configuration Device tables ¹	AAA Servers tables, the AAA Clients tables, in the Network Configuration section, Key Wrap keys as part of host configuration or Network Device Groups (NDG) and Remote Agents configuration. This option also controls whether NDGs are replicated.
Distribution table	Proxy Distribution Table in the Network Configuration section.
Interface configuration	Advanced Options settings, RADIUS settings, and TACACS+ settings from the Interface Configuration section.
Interface security settings	Administrators and security information for the ACS web interface, password policy, including the password history and the parts of the global system configuration that configures the history.
Password validation settings	Password validation settings.
EAP-FAST master keys and policies	Active and retired master keys and policies for EAP-FAST.
Network Access Profiles ²	A collaboration of configuration settings. These include: Network Access Profiles, Posture Validation settings, AAA clients and hosts, external user database configuration, global authentication configuration, NDGs, user-defined RADIUS dictionaries, shared profile components, logging configuration ³ , GAME Group Feed back configuration, databases for MAC Authentication Bypass, EAP-TLS for PEAP configuration, EAP-TLS configuration, and Key Wrap allowed configuration.
Logging Configuration (Enable/Disable Settings)	Logging configuration settings from the System Configuration section.

1. If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary ACS. For example, if the primary ACS replicates to two secondary ACSs that, in turn, each replicate to two more ACSs, the primary ACS must have AAA server configurations for all six ACSs that will receive replicated database components.
2. Replication of Network Access Profiles contradicts the replication of Network Configuration Device tables; therefore, do not check both of these components at the same time. NAP settings will override all other settings. Dynamically mapped users are not replicated, only statically added users are replicated.
3. When you replicate logging configurations between ACS for Windows and ACS SE, only the logger configurations that the receiving ACS supports are replicated. For example, ODBC logging configurations will not be replicated on an ACS SE.

**Note**

For interface security settings configuration replication: the activity limitation and locking as well as timezone are specified and evaluated on the master ACS and replicated. This replication may lead to unexpected behavior on the replica.

If mirroring the entire database might send confidential information to the secondary ACS, such as the Proxy Distribution Table, you can configure the primary ACS to send only a specific category of database information.

Outbound Replication Options

In the Outbound Replication table on the ACS Database Replication page, you can schedule outbound replication and specify the secondary ACSs for this primary ACS.

Table 8-2 Outbound Replication Options

Option	Description
Scheduling Options	
Manually	ACS does not perform automatic database replication.
Automatically Triggered Cascade¹	ACS performs database replication to the configured list of secondary ACSs when database replication from a primary ACS completes. You use this option to build a propagation hierarchy of ACS, relieving a primary ACS from the burden of propagating the replicated components to every other ACS. For an illustration of cascade replication, see Figure 8-1 .
Every X minutes	ACS performs, on a set frequency, database replication to the configured list of secondary ACSs. The unit of measurement is minutes, with a default update frequency of 60 minutes.
At specific times	ACS performs, at the time that is specified in the day and hour graph, database replication to the configured list of secondary ACSs. The minimum interval is one hour, and the replication occurs on the hour selected.
Partner Options	You can specify the secondary ACSs for this primary ACS. The options that control the secondary ACSs to which a primary ACS replicates appear in the Partners section of the Outbound Replication table.
AAA Server	Represents the secondary ACSs that this primary ACS <i>does not</i> send replicated components to.
Replication	Represents the secondary ACSs that this primary ACS <i>does</i> send replicated components to.
Replication Timeout	Specifies the number of minutes that this primary ACS continues replicating to a secondary ACS. When the timeout value is exceeded, ACS terminates replication to the secondary ACS it was attempting to replicate to and then it restarts the CSAuth service. The replication timeout feature helps prevent loss of AAA services due to stalled replication communication, which can occur when the network connection between the primary and secondary ACS is abnormally slow or when a fault occurs within either ACS. The default value is five minutes.

1. If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary ACS. For example, if the primary ACS replicates to two secondary ACSs which, in turn, each replicate to two more ACSs, the primary ACS must have AAA server configurations for all six ACSs that will receive replicated database components.

The items in the AAA Server and Replication lists reflect the AAA servers configured in the AAA Servers table in Network Configuration. To make a particular ACS available as a secondary ACS, you must first add that ACS to the AAA Servers table of the primary ACS.

**Tip**

The size of the components replicated affects the time required for replication. For example, replicating a database containing 80,000 user profiles takes more time than replicating a database containing 500 user profiles. You may need to monitor successful replication events to determine a reasonable timeout value for your implementation.

ACS does not support bidirectional database replication. A secondary ACS receiving replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it rejects the components.

When replicating three nodes or more, the master should have all the AAA servers configured on network devices and the partners should also be configured. For example, if there is a cascade A-->B-->C, then in A, C should be configured in the AAA server column and B should be configured in the replication column. In B, A should be configured in the AAA server column and C in the replication column. In C, B should be configured in the AAA server column. Otherwise the cascade replication fails.

Inbound Replication Options

You can specify the primary ACSs from which a secondary ACS accepts replication. This option appears in the Inbound Replication table on the ACS Database Replication page.

The **Accept replication from** list controls which ACSs the current ACS does accept replicated components from. The list contains:

- **Any Known ACS Server**—If this option is selected, ACS accepts replicated components from any ACS configured in the AAA Servers table in Network Configuration.
- **Other AAA servers**—The list displays all the AAA servers configured in the AAA Servers table in Network Configuration. If a specific AAA server name is selected, ACS accepts replicated components only from the ACS specified.

**Note**

ACS does not support bidirectional database replication. A secondary ACS receiving replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it rejects the components.

For more information about the AAA Servers table in Network Configuration, see [Configuring AAA Servers](#), page 3-15.

Implementing Primary and Secondary Replication Setups on ACSs

If you implement a replication scheme that uses cascading replication, the ACS configured to replicate only when it has received replicated components from another ACS acts as a primary ACS and as a secondary ACS. First, it acts as a secondary ACS while it receives replicated components, and then it acts as a primary ACS while it replicates components to other ACSs. For an illustration of cascade replication, see [Figure 8-1](#).

To implement primary and secondary replication setups on ACSs:

-
- Step 1** On each secondary ACS:
- In the Network Configuration section, add the primary ACS to the AAA Servers table.
For more information about adding entries to the AAA Servers table, see [Configuring AAA Servers, page 3-15](#).
 - Configure the secondary ACS to receive replicated components. For instructions, see [Configuring a Secondary ACS, page 8-11](#).
- Step 2** On the primary ACS:
- In the Network Configuration section, add each secondary ACS to the AAA Servers table.



Note If you intend to use cascading replication to replicate network configuration device tables, you must configure the primary ACS with all ACSs that will receive replicated database components, regardless of whether they receive replication directly or indirectly from the primary ACS. For example, if the primary ACS replicates to two secondary ACSs which, in turn, each replicate to two more ACSs, the primary ACS must have AAA server configurations for all six ACSs that will receive replicated database components.

For more information about adding entries to the AAA Servers table, see [Configuring AAA Servers, page 3-15](#).

- If you want to replicate according to a schedule, at intervals, or whenever the primary ACS has received replicated components from another ACS, see [Scheduling Replication, page 8-14](#).
 - If you want to initiate replication immediately, see [Replicating Immediately, page 8-13](#).
-

Configuring a Secondary ACS



Note

If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **ACS Database Replication** check box. Check the **Distributed System Settings** check box if it is not already checked.

The ACS Database Replication feature requires that you configure specific ACSs to act as secondary ACSs. The components that a secondary ACS is to receive must be explicitly specified, as must be its primary ACS.

Replication is always initiated by the primary ACS. For more information about sending replication components, see [Replicating Immediately, page 8-13](#) or [Scheduling Replication, page 8-14](#).



Caution

The ACS internal database components received by a secondary ACS *overwrite* the ACS internal database components on the secondary ACS. Any information unique to the overwritten database component is lost.

Before You Begin

Ensure correct configuration of the AAA Servers table in the secondary ACS. This secondary ACS must have an entry in its AAA Servers table for each of its primary ACSs. Also, the AAA Servers table entry for each primary ACS must have the same shared secret that the primary ACS has for its own entry in its AAA Servers table. For more information about the AAA Servers table, see [Configuring AAA Servers, page 3-15](#).

To configure an ACS to be a secondary ACS:

Step 1 Log in to the web interface on the secondary ACS.

Step 2 In the navigation bar, click **System Configuration**.

Step 3 Click **Database Replication**.

The Database Replication Setup page appears.

Step 4 In the Replication Components table, check the **Receive** check box for each database component to be received from a primary ACS.

For more information about replication components, see [Replication Components Options, page 8-7](#).

Step 5 Make sure that no ACS that the secondary ACS is to receive replicated components from is included in the Replication list. If so, select the primary ACS in the Replication list and click the <-- (left arrow) to move it to the AAA Servers list.



Note ACS does not support bidirectional database replication. A secondary ACS receiving replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it aborts replication.

Step 6 If the secondary ACS is to receive replication components from *only one* primary ACS, from the Accept replication from list, select the name of the primary ACS.

The primary ACSs available in the Accept replication from list are determined by the AAA Servers table in the Network Configuration section. For more information about the AAA Servers table, see [Configuring AAA Servers, page 3-15](#).



Note On the primary ACS and all secondary ACSs, the AAA Servers table entries for the primary ACS must have identical shared secrets.

Step 7 If the secondary ACS is to receive replication components from *more than one* primary ACS, from the Accept replication from list, select **Any Known ACS Server**.

The Any Known ACS Server option is limited to the ACSs listed in the AAA Servers table in Network Configuration.



Note For each primary ACS for this secondary ACS, on the primary and secondary ACS, the AAA Servers table entries for the primary ACS must have identical shared secrets.

Step 8 Click **Submit**.

ACS saves the replication configuration, and at the frequency or times that you specified, ACS begins accepting the replicated components from the other ACSs you specified.

Replicating Immediately

You can manually start database replication.



Note

Replication cannot occur until you have configured at least one secondary ACS. For more information about configuring a secondary ACS, see [Configuring a Secondary ACS, page 8-11](#).

Before You Begin

Ensure correct configuration of the primary and secondary ACSs. For detailed steps, see [Implementing Primary and Secondary Replication Setups on ACSs, page 8-10](#).

For each secondary ACS that this ACS is to send replicated components to, make sure that you have completed the steps in [Configuring a Secondary ACS, page 8-11](#).

To initiate database replication immediately:

-
- Step 1** Log in to the web interface on the primary ACS.
 - Step 2** In the navigation bar, click **System Configuration**.
 - Step 3** Click **Database Replication**.



Note

If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **ACS Database Replication** check box. Check the **Distributed System Settings** check box if it is not already checked.

The Database Replication Setup page appears.

- Step 4** For each ACS internal database component you want to replicate to a secondary ACS, under Replication Components, select the corresponding **Send** check box.
- Step 5** For each secondary ACS that you want the primary ACS to replicate its select components to, select the secondary ACS from the AAA Servers list, and then click --> (right arrow button).



Tip

If you want to remove a secondary ACSs from the Replication list, select the secondary ACS in the Replication list, and then click <-- (left arrow button).



Note

ACS does not support bidirectional database replication. A secondary ACS receiving replicated components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated components. If so, it rejects the components.

- Step 6** In the **Replication timeout** text box, specify how long this ACS will perform replication to each of its secondary ACS before terminating the replication attempt and restarting the CSAuth service.
- Step 7** At the bottom of the browser window, click **Replicate Now**.

ACS saves the replication configuration. ACS immediately begins sending replicated database components to the secondary ACSs you specified.

**Note**

Replication only occurs when the database of the primary ACS has changed since the last successful replication. You can force replication to occur by making one change to a user or group profile, such as changing a password or RADIUS attribute.

Scheduling Replication

You can schedule when a primary ACS sends its replicated database components to a secondary ACS. For more information about replication scheduling options, see [Outbound Replication Options, page 8-9](#).

**Note**

Replication cannot occur until the secondary ACSs are configured properly. For more information, see [Configuring a Secondary ACS, page 8-11](#).

Before You Begin

Ensure correct configuration of the primary and secondary ACSs. For detailed steps, see [Implementing Primary and Secondary Replication Setups on ACSs, page 8-10](#).

For each secondary ACS of this primary ACS, ensure that you have completed the steps in [Configuring a Secondary ACS, page 8-11](#).

To schedule when a primary ACS replicates to its secondary ACSs:

-
- Step 1** Log in to the web interface on the primary ACS.
 - Step 2** In the navigation bar, click **System Configuration**.
 - Step 3** Click **ACS Database Replication**.

**Note**

If this feature does not appear, choose **Interface Configuration > click Advanced Options**. Then, check the **ACS Database Replication** check box. Check the **Distributed System Settings** check box if not already selected.

The Database Replication Setup page appears.

- Step 4** To specify which ACS internal database components the primary ACS should send to its secondary ACSs, under Replication Components, select the corresponding **Send** check box for each database component to be sent.

For more information about replicated database components, see [Replication Components Options, page 8-7](#).
- Step 5** To have the primary ACS send replicated database components to its secondary ACSs at regular intervals, under Replication Scheduling, select the Every X minutes option and in the X box enter the length of the interval at which ACS should perform replication (up to 7 characters).

**Note**

Because ACS is momentarily shut down during replication, a short replication interval may cause frequent failover of your AAA clients to other ACSs. If AAA clients are not configured to failover to other ACSs, the brief interruption in authentication service may prevent users from authenticating. For more information, see [Replication Frequency, page 8-5](#).

Step 6 If you want to schedule times at which the primary ACS sends its replicated database components to its secondary ACSs:

- a. In the Outbound Replication table, select the **At specific times** option.
- b. In the day and hour graph, click the times at which you want ACS to perform replication.

**Tip**

Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 7 If you want to have this ACS send replicated database components immediately on receiving replicated database components from another ACS, select the **Automatically triggered cascade** option.

**Note**

If you specify the Automatically triggered cascade option, you must configure another ACS to act as a primary ACS to this ACS; otherwise, this ACS never replicates to its secondary ACSs.

Step 8 You must specify the secondary ACSs that this ACS should replicate to. To do so:

**Note**

ACS does not support bidirectional database replication. A secondary ACS receiving replicated database components verifies that the primary ACS is not on its Replication list. If not, the secondary ACS accepts the replicated database components. If so, it rejects the components. For more information about replication partners, see [Inbound Replication Options, page 8-10](#).

- a. In the Outbound Replication table, from the AAA Servers list, select the name of a secondary ACS to which you want the primary ACS to send its selected replicated database components.

**Note**

The AAA Servers table in Network Configuration determines which secondary ACSs are available in the AAA Servers list. For more information about the AAA Servers table, see [Configuring AAA Servers, page 3-15](#).

- b. Click --> (right arrow button).
The selected secondary ACS moves to the Replication list.
- c. Repeat Step a and Step b for each secondary ACS to which you want the primary ACS to send its selected replicated database components.

Step 9 In the **Replication timeout** text box, specify how long this ACS will perform replication to each of its secondary ACS before terminating the replication attempt and restarting the CSAuth service.

Step 10 Click **Submit**.

ACS saves the replication configuration that you created.

Disabling ACS Database Replication

You can disable scheduled ACS database replications without losing the schedule itself. This allows you to cease scheduled replications temporarily and later resume them without having to re-enter the schedule information.

To disable ACS database replication:

-
- Step 1** Log in to the web interface on the primary ACS.
- Step 2** In the navigation bar, click **System Configuration**.
- Step 3** Click **Database Replication**.
The Database Replication Setup page appears.
- Step 4** In the Replication Components table, clear all check boxes.
- Step 5** In the Outbound Replication table, select the **Manually** option.
- Step 6** Click **Submit**.
ACS does not permit any replication to or from this ACS server.
-

Configuring Automatic Change Password Replication

To configure automatic change password replication and other local password management options:

-
- Step 1** Log in to the web interface on the primary ACS.
- Step 2** In the navigation bar, click **System Configuration**.
- Step 3** Click **Local Password Management**.
- Step 4** Select the options to configure:

Field	Description
Password Validation Options	<ul style="list-style-type: none"> Character length May not contain username Different from previous value Alphanumeric
Remote Change Password	<ul style="list-style-type: none"> Disable Telnet password on this ACS and return desired message to users Telnet session. Upon remote password change, immediately propagate the change to selected replication partners.

- Step 5** Click **Submit**.
-

Database Replication Event Errors

The Database Replication report contains messages indicating errors that occur during replication. For more information about the Database Replication report, see [ACS Audit Logs, page 10-5](#).



Tip

Brief descriptions of errors are reported to the replication report, however sometimes more detailed errors are written to the CSAuth service log file, *auth.log*.

RDBMS Synchronization

This section provides information about the RDBMS Synchronization feature, including procedures for implementing this feature, within ACS and the external data source involved.

This section contains:

- [About RDBMS Synchronization, page 8-17](#)
- [Invoking RDBMS Synchronization, page 8-19](#)
- [RDBMS Synchronization Functionality, page 8-20](#)
- [RDBMS Synchronization Components, page 8-27](#)
- [ACS Database Recovery Using the accountActions Table, page 8-30](#)
- [Reports and Event \(Error\) Handling, page 8-30](#)
- [Preparing to Use RDBMS Synchronization, page 8-30](#)
- [Configuring a System DSN for RDBMS Synchronization \(ACS for Windows\), page 8-32](#)
- [RDBMS Synchronization Options, page 8-33](#)
- [Performing RDBMS Synchronization, page 8-35](#)
- [Scheduling RDBMS Synchronization, page 8-36](#)
- [Disabling Scheduled RDBMS Synchronizations, page 8-37](#)
- [RDBMS Synchronization Failure Codes, page 8-38](#)

About RDBMS Synchronization

You can regard RDBMS Synchronization as an API—much of what you can configure for a user, group, or device through the ACS web interface, you can alternatively maintain through this feature. RDBMS Synchronization supports the creation, addition, modification, and deletion for all data items that it can access.

You can configure the synchronization to occur on a regular schedule. You can also perform synchronizations manually, updating the ACS internal database on demand. For more information about configuring RDBMS Synchronization, see the *Configuration Guide for Cisco Secure ACS 4.2*.

Synchronization that a single ACS performs can update the internal databases of other ACSs, so that you only need to configure RDBMS Synchronization on one ACS. ACSs listen on TCP port 2000 for synchronization data. RDBMS Synchronization communication between ACSs is encrypted using a 128-bit encrypted, proprietary algorithm.

RDBMS Synchronization is available for manipulating ACS database objects effectively. You can invoke RDBMS synchronization using a CSV account actions file.

**Note**

ACS cannot use the *accountactions.csv* file at:
C:/Program_Files/CiscoSecureACSV4.2/CSDBSync/Databases/CSV/accountactions.csv.

The process differs for the ACS Windows and ACS SE platforms. ACS SE requires a command-line-interface-like utility to invoke RDBMS synchronization. You can invoke RDBMS synchronization using the SSH server implementation and using the command **csdbsync -syncnow**. When you specify a CSV file location on an FTP server, the ACS SE creates a Data Source Name (DSN) and performs RDBMS synchronization. The ACS Windows version provides two options. You can enable the **Use Local CSV** option, and the DSN is automatically created and synchronization occurs, or you must create a DSN manually to perform RDBMS synchronization. ACS for Windows uses a local CSV file that you specify when you configure RDBMS synchronization.

You can also run the **csdbsync** command from the Windows command line, similar to as you run it on the SSH remote shell with the SE. You can code a text file to specify dACLs that you use as input to a CREATE_DACL (account action code 385) entry in the CSV file.

RDBMS synchronization includes a support mechanism to configure downloadable ACLs, assign dACLs's to users, and AAA client configuration management. You can create, update and delete downloadable ACLs for users using the account action codes, 380, 381, and 382, respectively.

You can also create, read, update, and delete single or multiple AAA clients through RDBMS Synchronization. You can use the account codes 224 and 255, respectively, to update or read the AAA clients. With the capability of reading the AAA clients, you can export the AAA client list for a particular NDG, or a AAA client list with a specified IP range, or the list of all AAA clients.

ACS for Windows

You use the RDBMS Synchronization feature to update the ACS internal database with information from an ODBC-compliant data source. The ODBC-compliant data source can be the RDBMS database of a third-party application. It can also be an intermediate file or database that a third-party system updates. Regardless of where the file or database resides, ACS reads the file or database via the ODBC connection.

The RDBMS Synchronization feature provides the ability to update the ACS internal database with information from a local CSV file.

ACS SE

The RDBMS Synchronization feature provides the ability to update the ACS internal database with information from a text file on an FTP server.

The *accountActions.csv* file is uploaded to ACS and is used to read the action codes for the RDBMS Synchronization operations. A third-party application may generate the text file. ACS gets the file from the FTP server, reads the file, and performs the configuration actions that the file specifies.

You specify the actions in a relational database table (ACS for Windows only) or text file, named *accountActions*. For more information about the *accountActions* table, see [About the accountActions Table \(ACS for Windows\)](#), page 8-28. For more information about the *accountActions* file, see [About the accountActions File \(ACS SE\)](#), page 8-29. For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, "RDBMS Synchronization Import Definitions."](#)

Invoking RDBMS Synchronization

To invoke RDBMS Synchronization:



Note

Enter **net stop csdbsync** and a **net start csdbsync** before you run **csdbsync -syncnow** or **cydbsync -run**.

Use the *accountActions.CSV* file and then run the **csdbsync -syncnow** command. This method is applicable for Windows and the SE versions of ACS.

Configuring RDBMS for the ACS SE

To configure RDBMS Synchronization for the SE:

- Step 1** Connect to the ACS SE via the SSH client, to invoke the **csdbsync -syncnow** command.
Use the scriptable interface that the SSH service supports, that is added to the ACS SE.
- Step 2** Check the connectivity between the SSH client and the SSH server.
- Step 3** Find the location of the *accountActions.csv* file on the FTP server.
The ACS SE requires the *accountActions.csv* file to invoke RDBMS synchronization.
- Step 4** Check the connectivity between the ACS SE and the FTP server and be certain that you have write permissions to the FTP server directory.
ACS gets the CSV file from the FTP server and automatically creates the DSN. The uploaded CSV files should be in a valid format and the values in the CSV file for RDBMS Synchronization must be valid.
- Step 5** Run the **csdbsync -syncnow** command to invoke RDBMS Synchronization.
This command operates identically to the **CSDBSync** command without stopping or starting the RDBMS Synchronization command.
ACS SE fetches the CSV file from the database, reads the action codes in the file, and performs the RDBMS Synchronization operations specified in the file. For more information on the steps to perform the RDBMS Synchronization, see [Performing RDBMS Synchronization, page 8-35](#)

Configuring for RDBMS Synchronization for ACS for Windows

To configure RDBMS Synchronization for ACS for Windows:



Note

Enter **net stop csdbsync** and a **net start csdbsync** before you run **csdbsync -syncnow** or **cydbsync -run**.

- Step 1** In Windows, use the command line interface to invoke the **csdbsync -run** or **csdbsync -syncnow** command, if you do not use the **Synchronize Now** option.



Note

The invocation of RDBMS Synchronization is slightly different when compared to the ACS SE because you must manually create the DNS.

- Step 2** Create a DSN to perform the RDBMS Synchronization with one of two methods:

- a. You can enable the **Use Local CSV File** option in the GUI, which enables ACS to accept a local csv filename and location.

**Note**

The local csv file should not be
`C:\ProgramFiles\CiscoSecureACSV4.2\CSDBSync\Databases\CSV\accountactions.csv.`

- b. Manually create the DSN.

ACS uses the Microsoft Text Driver to create a default DSN called *Cisco Secure DBSync* that processes the local csv files. ACS extracts the contents from the csv file at the specified location, processes the file and then renames the file with a *.done* extension.

**Note**

The default DSN *CiscoSecure DBSync* must be present.

Step 3 When you click the **Synchronize Now** option, ACS will fetch the csv file from the database.

ACS reads the action codes in the csv file and performs the RDBMS synchronization operations that the file specifies.

For more detailed information on the steps to perform the RDBMS Synchronization, see [Performing RDBMS Synchronization, page 8-35](#)

RDBMS Synchronization Functionality

This section provides an overview of the different kinds of configuration that RDBMS Synchronization can automate:

- [User Related Actions for RDBMS Synchronization, page 8-20](#)
- [User Groups Related Actions for RDBMS Synchronization, page 8-21](#)
- [Creating, Reading, Updating and Deleting Actions for AAA clients, page 8-22](#)

User Related Actions for RDBMS Synchronization

Among the user-related configuration actions that RDBMS Synchronization can perform are:

- Adding users.
- Deleting users.
- Setting passwords.
- Setting user group memberships.
- Setting Max Sessions parameters.
- Setting network usage quota parameters.
- Configuring command authorizations.
- Configuring network access restrictions.
- Configuring time-of-day/day-of-week access restrictions.
- Assigning IP addresses.
- Specifying outbound RADIUS attribute values.
- Specifying outbound TACACS+ attribute values.

**Note**

For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, “RDBMS Synchronization Import Definitions.”](#)

User Groups Related Actions for RDBMS Synchronization

Among the group-related configuration actions that RDBMS Synchronization can perform are:

- Setting Max Sessions parameters.
- Setting network usage quota parameters.
- Configuring command authorizations.
- Configuring network access restrictions.
- Configuring time-of-day/day-of-week access restrictions.
- Specifying outbound RADIUS attribute values.
- Specifying outbound TACACS+ attribute values.

**Note**

For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, “RDBMS Synchronization Import Definitions.”](#)

Creating, Updating and Deleting dACLs for User and User Groups

This section describes the various RDBMS Synchronization tasks that you can perform for users and user groups.

To perform these tasks:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

The RDBMS Synchronization Setup page appears.

**Note**

If this feature does not appear, click **Interface Configuration > Advanced Options**, then check **RDBMS Synchronization**.

Step 3 Click the **User-Level Downloadable ACLs** option to enable the functionality of the action codes.

Step 4 click the **Group-Level Downloadable ACLs** option to specify the Group Name to which the dACL needs to be assigned.

Step 5 Run the **csdbsync -syncnow** command or click **Synchronize Now** option to invoke RDBMS Synchronization.

**Note**

Before invoking RDBMS Synchronization, the Account Action Codes must be specified in the CSV file or ODBC database.

ACS processes the action codes that are specified in the CSV file and performs RDBMS Synchronization. See [Action Codes for dACL Attributes, page E-27](#) for more information.

The following are descriptions of the new action codes.

Action Code 380 - Create dACL for User

This action code enables you to Assign IP ACLs and assigns the specific dACL to the specified User or Group. The dACL name that you specify should be valid and present in ACS.

Action Code 381 - Update dACL for User

This action code updates the dACL for a specified User or Group. The dACL name specified should be valid and present in ACS.

Action Code 382 - Delete dACL for User

This action code disables the Assign IP ACL for a specified User or Group.

Network Configuration

Among the network device-related configuration actions that RDBMS Synchronization can perform are:

- Adding AAA clients.
- Deleting AAA clients.
- Setting AAA client configuration details.
- Adding AAA servers.
- Deleting AAA servers.
- Setting AAA server configuration details.
- Adding and configuring Proxy Distribution Table entries.



Note

For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, “RDBMS Synchronization Import Definitions.”](#)

Creating, Reading, Updating and Deleting Actions for AAA clients

The RDBMS Synchronization feature supports creating and deleting single or multiple AAA clients. In addition, the account actions codes 224 and 225 enable reading and updating AAA client information. This section describes the various RDBMS Synchronization tasks that you can perform on single or multiple AAA clients.

[Table 8-3](#) lists the account action codes that are used to read and update single or multiple AAA clients.

Table 8-3 Account Action Codes to Create, Read, Update, Delete for AAA Clients

Action Code	Name	Required	Description
224	UPDATE_NAS	VN, V1, V2, V3	Use this action code to update AAA clients. VN = AAA Client Name V1 = IP-Address V2 = Shared Secret Key V3 = Vendor
225	READ_NAS	VN, V1 (optional)	Use this action code to export an AAA client list to an output file that can be used to associate the list with members of a particular NDG or with all AAA clients. You can use this output file as input for CSUtil , to import NASs. VN = <output_file_name> where <i>output_file_name</i> specifies the filename for the FTP server used with the ACS SE. If nothing is specified, the default name <i>DumpNAS.txt</i> is used. For the ACS for Windows platform, you can specify the absolute file path, for example: <i>C:\MyNAS\dump.txt</i> . If no value is specified, the AAA client lists is written to the <i>\ACS\bin\DumpNAS.txt</i> file. V1 = NDG name (optional) V1 should contain a valid NDG name.

Action Code 224 - Update dACL for AAA Client

This action code is used to update the AAA clients.

Action Code 225 - Read dACL for AAA Client

This action code is used to export AAA clients list at a particular NDG or all AAA clients. The exported file can be used as input to import NAS via **CSUtil**.

**Note**

Export mechanism requires write permission for the FTP directory.

Creating, Reading, Updating, and Deleting dACL Attributes

This section describes the various RDBMS Synchronization tasks that you can perform for dACL attributes.

To perform these tasks:

- Step 1** In the navigation bar, click **Interface Configuration**.
- Step 2** Click **Advanced Options**.

The Advanced Options page opens.

- Step 3** Click the **User-Level Downloadable ACLs** option to enable the functionality of the action codes.
- Step 4** Click the **Group-Level Downloadable ACLs** option so that you can specify the Group Name to which to assign the dACL.
- Step 5** Invoke the **csdbsync -syncnow** command to perform RDBMS Synchronization.



Note For the create and update functions, you must specify the dACL name, description, dACL content name, and definition fields. You also have the option of specifying the Network Access Filter (NAF) name, to which to apply the dACL content. By default, this dACL content will be applied to all AAA clients.

- Step 6** You can specify the operation that you want RDBMS Synchronization to perform by specifying the account action codes.



Note You must add the new account action codes to RDBMS Synchronization.

Table 8-4 lists the account action codes that you can use to create, read, update, and delete dACLs for users.

Table 8-4 Account Action Codes for Creating, Reading, Updating, or Deleting a dACL

Action Code	Name	Required	Description
385	CREATE_DACL	VN	<p>VN = <i><input_file_name></i></p> <p><i>input_file_name</i> contains definition for dACL.</p> <p>Specifies the filename present in the FTP server for ACS SE.</p> <p>Absolute path (for example <i>C:\DACL\dump.txt</i>) for ACS for Windows.</p> <p>The dACL definition is ignored in case it already present.</p> <p>The dACL definition is ignored if it contains an invalid definition, content name, content definition or NAF name.</p>
386	READ_DACL	VN, V1 (optional)	<p>Use this action code to read dACL attributes and save them in a file for later use.</p> <p>VN = contains dACL name or * for all dACLs.</p> <p>V1 = <i><output_file_name></i></p> <p>where <i>output_file_name</i> contains the exported dACLs definition.</p> <p>On the ACS SE, <i>output_file_name</i> specifies the file in the FTP server for the ACS SE. If not is specified the default filename <i>DumpDACL.txt</i> is used.</p> <p>On ACS for Windows, you can specify the absolute file path, for example, <i>C:\temp\DACL.txt</i> for ACS for Windows. If you do not specify the file path and filename, ACS writes the data to a file in the <i>ACS\bin</i> directory.</p>

Table 8-4 Account Action Codes for Creating, Reading, Updating, or Deleting a dACL

Action Code	Name	Required	Description
387	UPDATE_DACL	VN, V1(optional)	<p>Use this action code to update dACL attributes.</p> <p>VN = <i><input_file_name></i></p> <p>where <i>input_file_name</i> specifies the file that contains the definition for the dACL to be updated.</p> <p>On the ACS SE platform, <i>input_file_name</i> specifies the file name present in the FTP server for ACS SE.</p> <p>You can specify the absolute file path, for example: <i>C:\DACL\dump.txt</i> for ACS for Windows.</p> <p>V1=DACL_REPLACE or DACL_APPEND</p> <p>The default option is:</p> <p>DACL_REPLACE</p> <p>The DACL_REPLACE option replaces the existing dACL with the new one.</p> <p>DACL_APPEND appends the new dACL content and it's definition to the existing dACL.</p> <p>If the dACL has not been defined, the new dACL is added to the existing list.</p> <p>The dACL definition is ignored if it contains an invalid definition, content name, content definition or NAF name.</p>
388	DELETE_DACL	VN	<p>Use this action code to delete a dACL.</p> <p>VN = The name of the dACL to delete. To delete all dACLs, code an asterisk (*).</p> <p>By default, all the dACLs are deleted.</p> <p>Users and Groups associated with this dACL will be dereferenced after deleting the dACL.</p>

Action Code 385 - Create dACL Attribute

This action code is used to create dACL attributes.

Action Code 386 - Read dACL Attribute

This action code is used to read dACL attributes.

Action Code 387 - Update dACL for Attribute

This actions code is used to update dACL attributes.

Action Code 388 - Delete dACL for Attribute

This action code is used to delete dACL attributes.

Custom RADIUS Vendors and VSAs

You use RDBMS Synchronization to configure custom RADIUS vendors and VSAs. In addition to supporting a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), ACS supports RADIUS vendors and VSAs that you define. Vendors you add must be IETF-compliant; therefore, all VSAs that you add must be sub-attributes of IETF RADIUS attribute number 26.

You can define up to ten custom RADIUS vendors. ACS allows only one instance of any given vendor, as defined by the unique vendor IETF ID number and by the vendor name.

**Note**

If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary ACSs, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see [ACS Internal Database Replication, page 8-1](#).

For specific information about all actions that RDBMS Synchronization can perform, see [Appendix E, “RDBMS Synchronization Import Definitions.”](#)

RDBMS Synchronization Components

The RDBMS Synchronization feature comprises:

- **CSDBSync**—A dedicated Windows service that performs automated user and group account management services for ACS.
- **(ACS for Windows) accountActions Table**—The data object that holds information that **CSDBSync** uses to update the ACS internal database.
- **(ACS SE) accountActions File**—The file that holds information that **CSDBSync** uses to update the ACS internal database.

These topics describe RDBMS synchronization components:

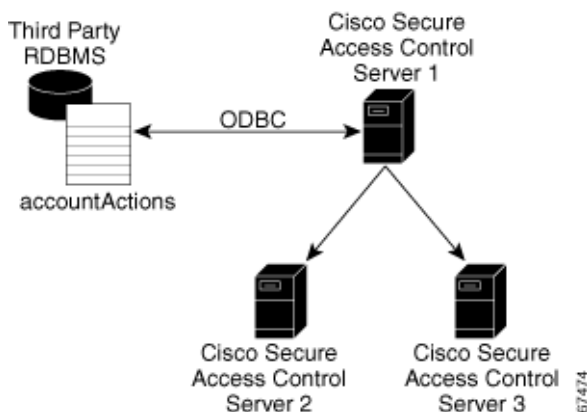
- [About CSDBSync, page 8-27](#)
- [About the accountActions Table \(ACS for Windows\), page 8-28](#)
- [About the accountActions File \(ACS SE\), page 8-29](#)

About CSDBSync

This section describes the CSDBSync service.

ACS for Windows

The CSDBSync service uses the Microsoft Text driver as the default system DSN that looks for the *accountactions.csv* file. See [Figure 8-2](#). This service looks specifically for *accountActions.csv* file. Synchronization events fail if **CSDBSync** cannot access the *accountActions.csv* file.

Figure 8-2 RDBMS Synchronization

CSDBSync reads each record from the `accountActions` table and updates the ACS internal database as specified by the action code in the record. For example, a record could instruct **CSDBSync** to add a user or change a user password. In a distributed environment, a single ACS, known as the senior synchronization partner, accesses the `accountActions` table and sends synchronization commands to its synchronization partners. In [Figure 8-2](#), Access Control Server 1 is the senior synchronization partner and the other two ACSs are its synchronization partners.

CSDBSync reads and writes (deletes records) in the `accountActions` table. After **CSDBSync** processes each record, it deletes the record from the table. To perform this action, the database user account that you configure the system DSN to use must have read and write privileges.

ACS SE

The **CSDBSync** service reads the `accountActions` file. While `accountActions.csv` is the default name for the `accountActions` file, you can name the file however you like. Synchronization events fail if **CSDBSync** cannot access the `accountActions` file.

CSDBSync reads each record from the `accountActions` file and updates the ACS internal database as specified by the action code in the record. For example, a record could instruct **CSDBSync** to add a user or change a user password. In a distributed environment, a single ACS, known as the senior synchronization partner, accesses the `accountActions` table and sends synchronization commands to its synchronization partners.



Note

The senior synchronization partner must have AAA configurations for each ACS that is a synchronization partners. In turn, each of the synchronization partners must have a AAA server configuration for the senior partner. Synchronization commands from the senior partner are ignored if the ACS receiving the synchronization commands does not have a AAA server configuration for the senior partner.

For more information about **CSDBSync** or other Windows services used by ACS, see [Appendix F, “Windows Services.”](#)

About the `accountActions` Table (ACS for Windows)

The `accountActions` table contains a set of rows that define actions that **CSDBSync** is to perform in the ACS internal database. Each row in the `accountActions` table holds user, user group, or AAA client information. Each row also contains an action field and several other fields. These fields provide

CSDBSync with the information it needs to update the ACS internal database. For details of the `accountActions` table format and available actions, see [Appendix E, “RDBMS Synchronization Import Definitions.”](#)

The database containing the `accountActions` table must support a multi-user ODBC driver. This is required to prevent problems if ACS and the third-party system attempt to access the `accountActions` table simultaneously.

ACS includes files to help you create your `accountActions` table for several common formats. You can find these files on the ACS in the following location, assuming a default installation of ACS:

C:\Program Files\CiscoSecure ACS vx.x\CSDBSync\Databases

The `Databases` directory contains the following subdirectories:

- **Access**—Contains the file *CiscoSecure Transactions.mdb*.

The *CiscoSecure Transactions.mdb* database contains a preconfigured `accountActions` table.



Note By default, the username and password for the *CiscoSecure Transactions.mdb* database are set to **null**. To increase the security of RDBMS synchronizations performed using this database, change the username and password, in the *CiscoSecure Transactions.mdb* database and in ACS. Any other processes that access the *CiscoSecure Transactions.mdb* database should be changed to use the new username and password, too.

- **CSV**—Contains the files *accountactions* and *schema.ini*.

The *accountactions* file is the `accountActions` table in a csv file. The *schema.ini* file provides the Microsoft ODBC text file driver with the information it needs to access the *accountactions* file.

- **Oracle 7**—Contains the files *accountActions.sql* and *testData.sql*.

The *accountActions.sql* file contains the Oracle 7 SQL procedure needed to generate an `accountActions` table. The *testData.sql* file contains Oracle 7 SQL procedures for updating the `accountActions` table with sample transactions that **CSDBSync** can process.

- **Oracle 8**—Contains the files *accountActions.sql* and *testData.sql*.

The *accountActions.sql* file contains the Oracle 8 SQL procedure needed to generate an `accountActions` table. The *testData.sql* file contains Oracle 8 SQL procedures for updating the `accountActions` table with sample transactions that **CSDBSync** can process.

- **SQL Server 6.5**—Contains the files *accountActions.sql* and *testData.sql*.

The *accountActions.sql* file contains the Microsoft SQL Server 6.5 SQL procedure needed to generate an `accountActions` table. The *testData.sql* file contains Microsoft SQL Server 6.5 SQL procedures for updating the `accountActions` table with sample transactions that **CSDBSync** can process.

About the `accountActions` File (ACS SE)

The *accountActions* file contains a set of rows that define actions **CSDBSync** is to perform in the ACS internal database. Each row in the *accountActions* file holds user, user group, or AAA client information. Except for the first row (which is used for field headers and thus is ignored during synchronization), each row also contains an action field and several other fields. These fields provide **CSDBSync** with the information it requires to update the ACS internal database.

For full details of the *accountActions* file format and available actions, see [Appendix E, “RDBMS Synchronization Import Definitions.”](#)

ACS Database Recovery Using the accountActions Table

The RDBMS Synchronization feature, in effect, produces a transaction queue:

- (ACS for Windows) The RDBMS Synchronization feature deletes each record in the accountActions table after processing the record; therefore, the accountActions table can be considered a transaction queue.
- (ACS SE) Combining all instances of *accountActions* files in the order that the RDBMS Synchronization produces processes them, in effect, a transaction queue.

The RDBMS Synchronization feature does not maintain a transaction log, or audit, trail. If a log is required, the external system that adds records to the accountActions table must create it. Unless the external system can recreate the entire transaction history in the accountActions table, we recommend that you construct a transaction log file for recovery purposes.

To do this:

ACS for Windows

Create a second table that is stored in a safe location and backed up regularly. In that second table, mirror all the additions and updates to records in the accountActions table.

ACS SE

Create a transaction log file that is stored in a safe location and backed up on a regular basis. In that second file, mirror all the additions and updates to records in the *accountActions* file. The transaction log file would therefore be a concatenation of all actions recorded in the many instances of the *accountActions* file processed by RDBMS Synchronization.

If the database is large, it is not practical to replay all transaction logs to synchronize the ACS internal database with the third-party system. Instead, you should create regular backups of the ACS internal database and replay the transaction logs from the time of most recent backup to resynchronize the ACS internal database with the third-party system. For information on creating backup files, see [Appendix E, “RDBMS Synchronization Import Definitions.”](#)

Replaying transaction logs that slightly predate the checkpoint does not damage the ACS internal database, although some transactions might be invalid and reported as errors. As long as the entire transaction log is replayed, the ACS internal database is consistent with the database of the external RDBMS application.

Reports and Event (Error) Handling

The **CSDBSync** service provides event and error logging. For more information about the RDBMS Synchronization log, see [ACS Audit Logs, page 10-5](#). For more information about the **CSDBSync** service log, see [Service Logs, page 10-12](#).

During manual synchronizations, ACS provides visual alerts to notify you of problems that occurred during synchronization.

Preparing to Use RDBMS Synchronization

Synchronizing the ACS internal database by using data from the accountActions table requires that you complete several steps that are external to ACS before you configure the RDBMS Synchronization feature within ACS. If you are planning to use a CSV file as your accountActions table, also see [Configuring a System DSN for RDBMS Synchronization \(ACS for Windows\), page 8-32](#).

**Note**

The *schema.ini* file must be located in the same folder as the *accountactions.csv* file.

To prepare to use RDBMS Synchronization:

Step 1 Determine the following:

ACS for Windows

Where you want to create the *accountActions* table and in what format. For more information about the *accountActions* table, see [About the accountActions Table \(ACS for Windows\)](#), page 8-28.

ACS SE

- How to create the *accountActions* file. For more information about the *accountActions* file, see [About the accountActions File \(ACS SE\)](#), page 8-29.
- The FTP server that you want to use to make the *accountActions* file accessible to ACS.

For details on the format and content of the *accountActions* table, see [Appendix E, “RDBMS Synchronization Import Definitions.”](#)

Step 2 Create your *accountActions* table.

Step 3 Configure your third-party system to generate records and update the *accountActions* table with them. This effort will most likely involve creating stored procedures that write to the *accountActions* table at a triggered event; however, the mechanism for maintaining your *accountActions* table is unique to your implementation. If the third-party system that you are using to update the *accountActions* table is a commercial product, for assistance, refer to the documentation from your third-party system vendor.

Step 4 (ACS SE) If needed, configure the mechanism that is to copy the *accountActions* file from where it is generated to the applicable directory on the FTP server.

Step 5 Validate that your third-party system updates the *accountActions* table properly. Rows that are generated in the *accountActions* table must be valid.

**Note**

After testing that the third-party system updates the *accountActions* table properly, discontinue updating the *accountActions* table until after you have completed [Step 7](#) and [Step 8](#).

Step 6 If you have a distributed AAA environment and want to synchronize multiple ACSs:

- Determine which ACS you want to use to communicate with the third-party system. This ACS is the senior synchronization partner, which you will later configure to send synchronization data to its synchronization partners, which are the other ACSs needing synchronization.
- On the senior synchronization partner, verify that there is a AAA server configuration for each synchronization partner. Add a AAA server configuration for each missing synchronization partner. For detailed steps about adding a AAA server, see [Adding AAA Servers](#), page 3-17.
- On all the other synchronization partners, verify that a AAA server configuration exists for the senior synchronization partner. If no AAA server configuration for the senior synchronization partner exists, create one. For detailed steps about adding a AAA server, see [Adding AAA Servers](#), page 3-17.

Synchronization between the senior synchronization partner and the other synchronization partners is enabled.

- Step 7** (ACS for Windows) Set up a system DSN on the senior synchronization partner (the ACS that will communicate with the third-party system). For steps, see [Configuring a System DSN for RDBMS Synchronization \(ACS for Windows\)](#), page 8-32.
- Step 8** Schedule RDBMS synchronization on the senior synchronization partner. For steps, see [Scheduling RDBMS Synchronization](#), page 8-36.
- Step 9** Configure your third-party system to begin updating the `accountActions` table with information that will be imported into the ACS internal database.
- (ACS SE) If needed, activate the mechanism that is to copy the `accountActions` file to the applicable directory on the FTP server.
- Step 10** Confirm that RDBMS synchronization is operating properly by monitoring the RDBMS Synchronization report in the Reports and Activity section. For more information about the RDBMS Synchronization log, see [ACS Audit Logs](#), page 10-5.
- Also, monitor the **CSDBSync** service log. For more information about the **CSDBSync** service log, see [Service Logs](#), page 10-12.
-

Configuring a System DSN for RDBMS Synchronization (ACS for Windows)

On the ACS, a system DSN must exist for ACS to access the `accountActions` table. You can use a local `AccountActions` CSV file to obtain a DSN for RDBMS Synchronization. ACS creates a default DSN *CiscoSecure DBSync* using a Microsoft Text Driver to process the local CSV files. ACS extracts the contents from the CSV file at the specified location, process the contents and renames the file with *.done* extension. If the **Use local CSV file** option is disabled, ACS performs RDBMS Synchronization as usual.



Tip

Everything ACS does with ODBC requires System DSNs. User DSNs will not work. Confusing the two DSNs is an easy mistake to make when configuring the datasources in the ODBC control panel applet. Ensure your System DSN is set properly.

For more information about the *CiscoSecure Transactions.mdb* file, see [Preparing to Use RDBMS Synchronization](#), page 8-30.

To create a system DSN for use with RDBMS synchronization:

- Step 1** From Windows Control Panel, open the ODBC Data Source Administrator window.



Tip

In Windows 2000 and new Microsoft operating systems, the ODBC Data Sources icon is located in the Administrative Tools folder.

- Step 2** In the ODBC Data Source Administrator window, click the **System DSN** tab.
- Step 3** Click **Add**.
- Step 4** Select the driver to use with your new DSN, and then click **Finish**.
- A dialog box displays fields requiring information that is specific to the selected ODBC driver.
- Step 5** In the **Data Source Name** box, enter a descriptive name for the DSN.
- Step 6** Complete the other fields that the selected ODBC. These fields may include information such as the IP address of the server on which the ODBC-compliant database runs.

Step 7 Click **OK**.

The name that you assigned to the DSN appears in the System Data Sources list.

Step 8 Close the **ODBC** window and **Windows Control Panel**.

On your ACS, you create the system that ACS uses to access your accountActions table.

RDBMS Synchronization Options

The RDBMS Synchronization Setup page, which is available from System Configuration, provides control of the RDBMS Synchronization feature. It contains three tables whose options are described in this section.

This section contains:

- [RDBMS Setup Options, page 8-33](#)
- [RDBMS Synchronization Setup For the accountActions File for Windows, page 8-33](#)
- [FTP Setup Options for RDBMS Synchronization for SE, page 8-34](#)
- [Synchronization Scheduling Options, page 8-34](#)
- [Synchronization Partners Options, page 8-34](#)

RDBMS Setup Options

The RDBMS Setup table defines how ACS accesses the accountActions table and contains the following options:

- **Data Source**—Specifies which of all the system DSNs that are available on ACS that can be used to access the accountActions table.
- **Username**—Specifies the username that ACS should use to access the database that contains the accountActions table.



Note

The database user account that the username specifies must have sufficient privileges to read and write to the accountActions table.

- **Password**—Specifies the password that ACS uses to access the database that contains the accountActions table.

RDBMS Synchronization Setup For the accountActions File for Windows

You can increase the usability of RDBMS synchronization with CSV files in ACS by providing information about the *accountActions* file such as:

- **Actions File**—The name of the *accountActions* file.
- **Directory**—Enter the path of the file in the local machine.

FTP Setup Options for RDBMS Synchronization for SE

The FTP Setup For Account Actions Download table defines how ACS accesses the `accountActions` table. It contains:

- **Actions File**—The name of the `accountActions` file. The default name is `actions.csv`. The filename provided must match the name of the `accountActions` file on the FTP server.
- **FTP Server**—The IP address or hostname of the FTP server from which ACS receives the `accountActions` file. If you specify a hostname, DNS must be enabled on your network.
- **Directory**—The relative path from the FTP server root directory to the directory where the `accountActions` file is. To specify the FTP root directory, enter a single period (.).
- **Username**—A valid username to enable ACS to access the FTP server.
- **Password**—The password for the username provided in the Login box.

Scriptable Interface for RDBM Synchronization

ACS for SE

You can change ACS configuration via remote systems using a command line utility for RDBMS Synchronization that includes SSH support. With the mechanism that starts the SSH server, you can add Administrator privileges and invoke the `csdbsync -syncnow` command. The `csdbsync -syncnow` command works just as the `csdbsync -run` command does without stopping or starting RDBMSync service.

Synchronization Scheduling Options

The Synchronization Scheduling table defines when synchronization occurs. It contains:

- **Manually**—ACS does not perform automatic RDBMS synchronization.
- **Every X minutes**—ACS performs synchronization on a set frequency. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times**—ACS performs synchronization at the time that is specified in the day and hour graph. The minimum interval is one hour, and the synchronization occurs on the hour that you selected.

Synchronization Partners Options

The Synchronization Partners table defines which ACSs are synchronized with data from the `accountActions` table. It provides:

- **AAA Server**—This list represents the AAA servers that are configured in the AAA Servers table in Network Configuration for which the ACS *does not* perform RDBMS synchronization.
- **Synchronize**—This list represents the AAA servers that are configured in the AAA Servers table in Network Configuration for which the ACS *does* perform RDBMS synchronization. The AAA servers on this list are the synchronization partners of this ACS. During synchronization, communication between this ACS and its synchronization partners is 128-bit encrypted with a Cisco-proprietary protocol. The synchronization partners receive synchronization data on TCP port 2000.

**Note**

Each synchronization partner *must* have a AAA server configuration in its Network Configuration section that corresponds to this ACS; otherwise, the synchronization commands this ACS sends to it are ignored.

For more information about the AAA Servers table in Network Configuration, see [Configuring AAA Servers, page 3-15](#).

Performing RDBMS Synchronization

You can manually start an RDBMS synchronization event.

To perform manual RDBMS synchronization:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

The RDBMS Synchronization Setup page appears.

**Note**

If this feature does not appear, click **Interface Configuration > Advanced Options**, then check **RDBMS Synchronization**.

Step 3 (ACS for Windows) To specify options in the RDBMS Synchronization using the local CSV file:

- a. **Use Local CSV File** —Check to activate ACS to take the CSV file from your local machine. ACS creates a default DSN *CiscoSecure DBSync* to process the local CSV files. ACS extracts the contents from the CSV file at the specified location, processes the contents and renames the file with “.done” extension.
- b. In the **AccountActions File** box, enter the name of the CSV file of configuration actions. The default is *accountactions.csv*.
- c. In the **Directory** box, enter the path name where the accountActions file is located in your local machine.

Step 4 (ACS for Windows) To specify options in the RDBMS Synchronization using the **CDBSync** system DSN:

- a. From the Data Source list, chose the system DSN that you configured to communicate with the database that contains your accountActions table.

For more information about configuring a system DSN for use with RDBMS Synchronization, see [Configuring a System DSN for RDBMS Synchronization \(ACS for Windows\), page 8-32](#).

- b. In the **Username** box, enter the username for a database user account that has read-write access to the accountActions table.
- c. In the **Password** box, enter the password for the username that was specified in the Step b.

**Note**

For more information about RDBMS setup, see [RDBMS Setup Options, page 8-33](#).

ACS has the information with which to access the accountActions table.



Note You do *not* have to select **Manually** under **Replication Scheduling**. For more information, see [Disabling Scheduled RDBMS Synchronizations, page 8-37](#).

- Step 5** (ACS SE) To specify options in the **FTP Setup For Account Actions Download** table:
- In the **Actions Files** box, type the name of the *accountActions* file that you want to use to update ACS.
 - In the **FTP Server** box, type the IP address or hostname of the FTP server from which you want ACS to get the *accountActions* file.
 - In the **Directory** box, type the relative path to the directory on the FTP server where the *accountActions* file resides.
 - In the **Username** box, type a valid username to enable ACS to access the FTP server.
 - In the **Password** box, type the password for the username provided in the **Login** box.



Note For more information about FTP setup, see [FTP Setup Options for RDBMS Synchronization for SE, page 8-34](#).

ACS has the information necessary to get the *accountActions* file from the FTP server.



Note You do *not* have to select **Manually** under **Replication Scheduling**. For more information, see [Disabling Scheduled RDBMS Synchronizations, page 8-37](#).

- Step 6** For each ACS that you want this ACS to update with data from the *accountActions* table, select the ACS in the **AAA Servers** list, and then click the right arrow button on the interface.
- The selected ACS appears in the **Synchronize** list.
- Step 7** To remove ACSs from the **Synchronize** list, select the ACS in the **Synchronize** list, and then click <-- (left arrow button).
- The selected ACS appears in the **Synchronize** list.
- Step 8** At the bottom of the browser window, click **Synchronize Now**.
- ACS immediately begins a synchronization event. To check the status of the synchronization, view the RDBMS Synchronization report in **Reports and Activity**.

Scheduling RDBMS Synchronization

You can schedule when ACS performs RDBMS synchronization.

To schedule when ACS performs RDBMS synchronization:

- Step 1** Perform RDBMS Synchronization. See [Performing RDBMS Synchronization, page 8-35](#).
- To have this ACS perform RDBMS synchronization at regular intervals, under **Synchronization Scheduling**, check the **Every X minutes** option and in the X box, enter the length of the interval in minutes at which ACS should perform synchronization (up to 7 characters).

- To schedule times at which this ACS performs RDBMS synchronization:
 - a. Under Synchronization Scheduling, check the **At specific times** option.
 - b. In the day and hour graph, click the times at which you want ACS to perform replication.

**Tip**

Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

Step 2 For each ACS that you want to synchronize with data from the accountActions table:

**Note**

For more information about synchronization targets, see [Inbound Replication Options, page 8-10](#).

- a. In the Synchronization Partners table, from the AAA Servers list, select the name of an ACS that you want this ACS to update with data from the accountActions table.

**Note**

The AAA Servers table in Network Configuration determines which ACSs are available in the AAA Servers list, with the addition of the name of the current ACS server. For more information about the AAA Servers table, see [Configuring AAA Servers, page 3-15](#).

- b. Click --> (right arrow button).

The selected ACS moves to the Synchronize list.

**Note**

At least one ACS must be in the Synchronize list. This includes the server on which you are configuring RDBMS Synchronization. RDBMS Synchronization does not automatically include the internal database of the current server.

Step 3 Click **Submit**.

ACS saves the RDBMS synchronization schedule that you created.

Disabling Scheduled RDBMS Synchronizations

You can disable scheduled RDBMS synchronization events without losing the schedule itself. You can use this ability to end scheduled synchronizations and resume them later without having to recreate the schedule.

To disable scheduled RDBMS synchronizations:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

The RDBMS Synchronization Setup page appears.

Step 3 Under Synchronization Scheduling, select the **Manually** option.

Step 4 Click **Submit**.

ACS does not perform scheduled RDBMS synchronizations.

RDBMS Synchronization Failure Codes

Fatal as well as nonfatal RDBMS synchronization errors can occur during a single transaction. When a nonfatal error message is written to the RDBMS synchronization audit log, and processing continues as if it is a successful transaction, the record is deleted from the action table. When a fatal error message is written to the RDBMS synchronization audit log, synchronization stops.

Although the expected behavior for ACS is to send the error code 2 to the database, ACS RDBMS synchronization does not send the error code 2, nor does it delete the database records if a failure occurs.

You can add new devices and NDGs when performing RDBMS synchronization from the database to ACS. The new devices are appended to the end.

If the device already exists in ACS, ACS reports an error in the log `Failed to create new NAS/AAA record- Host database failure, Host already exists`. Although the expected behavior for ACS is to delete the database records if a failure occurs, ACS remove the entries from the database and does not send an error code to the database.

Table 8-5 lists RDBMS Synchronization fatal errors:

Table 8-5 **List of Fatal Errors**

Error Code
Attempt to create account with user name that already exists
Password supplied for user was not valid
An internal error in packet format has occurred
The file or directory could not be opened - no free handles
File write in the user file space failed
File read in the user file space failed
An invalid directory name was supplied
An invalid file name was supplied
Server could not allocate memory
File set pointer in the user file space failed
CSAuth client tried to send a message greater than 31K
Attempt to create account with user name that already exists
A value in the registry was not found
Database file cannot be made bigger
Proxy database failure
UDB_PROXY_DB_FAILURE
Invalid counter type
UDB_USER_REMOVED
UDB_UDV_CONFIG_ERROR
Failed to parse DACL. User level DACL is not enabled.

Table 8-5 *List of Fatal Errors*

Error Code
Failed to process DACL. DACL not defined.
Failed to parse DACL. User/Group Level DACL is not enabled.
Failed to process DACL. Failed to get UserID.
Invalid NDG name.
Specified file does not exist or error in accessing file from FTP.

IP Pools Server

This section provides information about the IP Pools feature, including procedures for creating and maintaining IP pools.

This section contains:

- [About IP Pools Server, page 8-39](#)
- [Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges, page 8-40](#)
- [Refreshing the AAA Server IP Pools Table, page 8-41](#)
- [Adding a New IP Pool, page 8-41](#)
- [Editing an IP Pool Definition, page 8-42](#)
- [Resetting an IP Pool, page 8-42](#)
- [Deleting an IP Pool, page 8-43](#)

About IP Pools Server

If you are using VPNs you may have to overlap IP address assignments; that is, it may be advantageous for a PPTP tunnel client within a given tunnel to use the same IP address that another PPTP tunnel client in a different tunnel is using. You can use the IP Pools Server feature to assign the same IP address to multiple users, provided that the users are being tunnelled to different home gateways for routing beyond the boundaries of your own network. You can, therefore, conserve your IP address space without having to resort to using illegal addresses. When you enable this feature, ACS dynamically issues IP addresses from the IP pools that you have defined by number or name. You can configure up to 999 IP pools, for approximately 255,000 users.

If you are using IP pooling and proxy, all accounting packets are proxied so that the ACS that is assigning the IP addresses can confirm whether an IP address is already in use.

**Note**

The ACS Database Replication feature does not replicate IP pool definitions; however, user and group assignments to IP pools are replicated. By not replicating IP pool definitions, ACS avoids inadvertently assigning an IP address that a replication partner has already assigned to a different workstation. To support IP pools in a AAA environment that uses replication, you must manually configure each secondary ACS to have IP pools with names that are identical to the IP pools that are defined on the primary ACS.

To use IP pools, the AAA client must have network authorization (in IOS, **aaa authorization network**) and accounting (in IOS, **aaa accounting**) enabled.

**Note**

To use the IP Pools feature, you must set up your AAA client to perform authentication and accounting by using the same protocol; TACACS+ or RADIUS.

For information on assigning a group or user to an IP pool, see [Setting IP Address Assignment Method for a User Group, page 5-21](#) or [Assigning a User to a Client IP Address, page 6-7](#).

Allowing Overlapping IP Pools or Forcing Unique Pool Address Ranges

ACS provides automated detection of overlapping pools.

**Note**

To use overlapping pools, you must be using RADIUS with VPN, and you cannot be using the Dynamic Host Configuration Protocol (DHCP).

You can determine whether overlapping IP pools are allowed by checking which button appears below the AAA Server IP Pools table:

- **Allow Overlapping Pool Address Ranges**—Overlapping IP pool address ranges are *not allowed*. Clicking this button allows IP address ranges to overlap between pools.
- **Force Unique Pool Address Range**—Overlapping IP pool address ranges are *allowed*. Clicking this button prevents IP address ranges from overlapping between pools.

To allow overlapping IP pools or to force unique pool address ranges:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

**Note**

If this feature does not appear, click **Interface Configuration > Advanced Options**, then click **IP Pools**.

The AAA Server IP Pools table lists any IP pools you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 To allow overlapping IP pool address ranges:

- a. If the **Allow Overlapping Pool Address Ranges** button appears, click it.
ACS allows overlapping IP pool address ranges.
- b. If the **Force Unique Pool Address Range** button appears, do nothing.
ACS already allows overlapping IP pool address ranges.

Step 4 To deny overlapping IP pool address ranges:

- a. If the **Allow Overlapping Pool Address Ranges** button appears, do nothing.
ACS already does not permit overlapping IP pool address ranges.
- b. If the **Force Unique Pool Address Range** button appears, click it.

ACS does not permit overlapping IP pool address ranges.

Refreshing the AAA Server IP Pools Table

You can refresh the AAA Server IP Pools table to get the latest usage statistics for your IP pools.

To refresh the AAA Server IP Pools table:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **IP Pools Server**.
- The AAA Server IP Pools table lists any IP pools that you have configured, their address ranges, and the percentage of pooled addresses in use.
- Step 3** Click **Refresh**.
- ACS updates the percentages of pooled addresses in use.
-

Adding a New IP Pool

You can define up to 999 IP address pools.

To add an IP pool:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **IP Pools Server**.
- The AAA Server IP Pools table lists any IP pools that you have already configured, their address ranges, and the percentage of pooled addresses in use.
- Step 3** Click **Add Entry**.
- The New Pool table appears.
- Step 4** In the **Name** box, enter the name (up to 31 characters) to assign to the new IP pool.
- Step 5** In the **Start Address** box, enter the lowest IP address (up to 15 characters) of the range of addresses for the new pool.




Note All addresses in an IP pool must be on the same Class C network; so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.

- Step 6** In the **End Address** box, enter the highest IP address (up to 15 characters) of the range of addresses for the new pool.
- Step 7** Click **Submit**.
- The new IP pool appears in the AAA Server IP Pools table.
-

Editing an IP Pool Definition

To edit an IP pool definition:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **IP Pools Server**.
- The AAA Server IP Pools table lists any IP pools that you have configured, their address ranges, and the percentage of pooled addresses in use.
- Step 3** Click the name of the IP pool to edit.
- The *name* pool table appears, where *name* is the name of the IP pool that you selected. The In Use field displays how many IP addresses in this pool are allocated to a user. The Available field displays how many IP addresses are unallocated to users.
- Step 4** To change the name of the pool, in the **Name** box, enter the name (up to 31 characters) to which to change the IP pool.
- Step 5** To change the starting address of the pool range of IP addresses, in the **Start Address** box, enter the lowest IP address (up to 15 characters) of the new range of addresses for the pool.
-  **Note** All addresses in an IP pool must be on the same Class C network, so the first three octets of the start and end addresses must be the same. For example, if the start address is 192.168.1.1, the end address must be between 192.168.1.2 and 192.168.1.254.
-
- Step 6** To change the ending address of the pool range of IP addresses, in the **End Address** box, enter the highest IP address (up to 15 characters) of the new range of addresses for the pool.
- Step 7** Click **Submit**.
- The edited IP pool appears in the AAA Server IP Pools table.
-

Resetting an IP Pool

The Reset function recovers IP addresses within an IP pool when there are dangling connections. A dangling connection occurs when a user disconnects and ACS does not receive an accounting stop packet from the applicable AAA client. If the Failed Attempts log in Reports and Activity shows a large number of Failed to Allocate IP Address For User messages, consider using the Reset function to reclaim all allocated addresses in this IP pool.



Note Using the Reset function to reclaim all allocated IP addresses in a pool can result in users being assigned addresses that are already in use.

To reset an IP pool and reclaim all its IP addresses:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools that you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click the name of the IP pool to reset.

The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use field displays how many IP addresses in this pool are assigned to a user. The Available field displays how many IP addresses are not assigned to users.

Step 4 Click **Reset**.

ACS displays a dialog box indicating the possibility of assigning user addresses that are already in use.

Step 5 To continue resetting the IP pool, click **OK**.

The IP pool is reset. All its IP addresses are reclaimed. In the In Use column of the AAA Server IP Pools table, zero percent of the IP pool addresses are assigned to users.

Deleting an IP Pool



Note

If you delete an IP pool that has users assigned to it, those users cannot authenticate until you edit the user profile and change their IP assignment settings. Alternatively, if the users receive their IP assignment based on group membership, you can edit the user group profile and change the IP assignment settings for the group.

To delete an IP pool:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **IP Pools Server**.

The AAA Server IP Pools table lists any IP pools that you have configured, their address ranges, and the percentage of pooled addresses in use.

Step 3 Click the name of the IP pool to delete.

The *name* pool table appears, where *name* is the name of the IP pool you selected. The In Use column displays how many IP addresses in this pool are assigned to a user. The Available column displays how many IP addresses are not assigned to users.

Step 4 Click **Delete**.

ACS displays a dialog box to confirm that you want to delete the IP pool.

Step 5 To delete the IP pool, click **OK**.

The IP pool is deleted. The AAA Server IP Pools table does not list the deleted IP pool.

IP Pools Address Recovery

You use the IP Pools Address Recovery feature to recover assigned IP addresses that have not been used for a specified period of time. You must configure an accounting network on the AAA client for ACS to reclaim the IP addresses correctly.

Enabling IP Pool Address Recovery

To enable IP pool address recovery:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **IP Pools Address Recovery**.



Note If this feature does not appear, click **Interface Configuration > Advanced Options**, then click **IP Pools**.

The IP Address Recovery page appears.

- Step 3** Select the **Release address if allocated for longer than X hours** check box and in the **X** box enter the number of hours (up to 4 characters) after which ACS should recover assigned, unused IP addresses.
- Step 4** Click **Submit**.

ACS implements the IP pools address recovery settings that you made.

NAC Attribute Management (ACS SE Only)

You can use the CNAC Attributes Management page to add, delete, or export NAC attributes, which are used with posture validation requests. For more information about posture validation attributes, see [About Posture Credentials and Attributes, page 13-5](#).

This section contains:

- [Posture Validation Attribute Definition File, page 8-44](#)
- [Adding Attributes, page 8-47](#)
- [Deleting Attributes, page 8-48](#)
- [Exporting \(Dumping\) Attributes, page 8-50](#)
- [Default Posture Validation Attribute Definition File, page 8-51](#)

Posture Validation Attribute Definition File

A posture validation attribute definition file is a text file that contains one or more posture validation attribute definitions. Each definition consists of a definition header and several values, as shown in [Example 8-1](#). For an example of the contents of a posture validation attribute definition file, see [Default Posture Validation Attribute Definition File, page 8-51](#).

With the exception of the attribute definition header, each attribute definition value must be formatted as: *name=value*

where *name* is the value name and *value* is a string or integer, as specified in the following list.



Tip

You can use a semicolon (;) to identify lines that are comments.

[Example 8-1](#) shows an example of a posture validation attribute definition, including a comment after the attribute definition:

Example 8-1 Example Attribute Definition

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

; attribute 1 is reserved for the APT
```

A posture validation attribute is uniquely defined by the combination of its *vendor-id*, *application-id*, and *attribute-id*. The following list provides details of these values and of each line required in an attribute definition:

- **[attr#*n*]**—Attribute definition header, where *n* is a unique, sequential integer, beginning with zero (0). ACS uses the definition header to distinguish the beginning of a new attribute definition. Each attribute definition *must* begin with a line containing the definition header. The first attribute definition in the file *must* have the header `[attr#0]`, the second attribute definition in a file must have the header `[attr#1]`, and so on. A break in the numbering causes ACS to ignore attribute definitions at the break and beyond. For example, if in a file with 10 attribute definitions the fifth attribute is defined as `[attr#5]` instead of `[attr#4]`, ACS ignores the attribute defined as `[attr#5]` and the remaining five the attributes following it.



Tip

The value of *n* is irrelevant to any of the *-id* values in the attribute definition file. For example, the 28th definition in a file must have the header `[attr#27]`, but this definition does not limit or otherwise define valid values for *vendor-id*, *application-id*, and *attribute-id*. In addition, it does not limit or define the number of posture validation attributes supported by ACS.

- **vendor-id**—An unsigned integer that specifies the vendor number that belongs to the vendor associated with the posture validation attribute. The vendor number should be the number assigned to the vendor in the [IANA Assigned Numbers RFC](#). For example, *vendor-id* 9 corresponds to Cisco Systems, Inc.

Each *vendor-id* has one or more associated applications, identified by the *application-id* value.

- **vendor-name**—A string that specifies the vendor name that appears in the ACS web interface and logs for the associated posture validation attribute. For example, any attribute definition with a *vendor-id* of 9 could have the vendor name `cisco`.



Note The vendor name cannot differ for attributes that share the same `vendor-id`. For example, you cannot add an attribute with a `vendor-id` of 9 if the vendor name is not `cisco`.

- **application-id**—An unsigned integer that specifies the `application-id` that uniquely identifies the vendor application associated with the posture validation attribute. For example, if the `vendor-id` is 9 and the `application-id` is 1, the posture validation attribute is associated with the Cisco application with an ID of 1, which is the Cisco Trust Agent, also known as a posture agent (PA).
- **application-name**—A string that specifies the application name that appears in the ACS web interface and logs for the associated posture validation attribute. For example, if the `vendor-id` is 9 and the `application-id` is 1, the **application-name** would be `PA`, an abbreviation of posture agent, which is another term for the Cisco Trust Agent.



Note The application name cannot differ when attributes share the same `vendor-id` and `application-id` pair. For example, you cannot add an attribute with a `vendor-id` of 9 and `application-id` of 1 if the **application-name** is not `PA`.

- **attribute-id**—An unsigned integer in the range of 1 to 65535. The `attribute-id` uniquely identifies the posture validation attribute for the specified `vendor-id` and `application-id`.



Note Attributes 1 and 2 are reserved for each application. If you add attributes that imply a new application, ACS automatically creates attribute 1 as Application-Posture-Token and attribute 2 as System-Posture-Token.

- **attribute-name**—A string that specifies the attribute name that appears in the ACS web interface and logs for the associated posture validation attribute. For example, if the `vendor-id` is 9, the `application-id` is 1, and the `attribute-id` is 1, the **attribute-name** is Application-Posture-Token.
- **attribute-profile**—A string that specifies whether ACS can send the attribute in a posture validation response, can receive the attribute in a posture validation request, or can both send and receive the attribute during posture validation. Valid values for **attribute-profile** are:
 - **in**—ACS accepts the attribute in posture validation requests and can log the attribute, and you can use it in local policy rule definitions. Attributes with an `in` value for the **attribute-profile** are also known as inbound attributes.
 - **out**—ACS can send the attribute in posture validation responses but you cannot use it in local policy rule definitions. Attributes with an **attribute-profile** value of `out` are also known as outbound attributes. The only outbound attributes that you can configure ACS to log are the attributes for Application-Posture-Tokens and System-Posture-Tokens; however, these are system-defined attributes that you cannot modify.
 - **in out**—ACS accepts the attribute in posture validation requests and can send the attribute in posture validation responses. Attributes with an `in out` value for the **attribute-profile** are also known as inbound and outbound attributes.
- **attribute-type**—A string that specifies the kind of data that is valid in the associated attribute. For attributes whose `attribute-profile` is `in` or `in out`, the **attribute-type** determines the types of operators available for defining local policy rules that use the attribute. An example of an inbound attribute is the ServicePacks attribute that the Cisco Trust Agent sends. An example of an outbound attribute is the System-Posture-Token attribute, which is sent to the Cisco Trust Agent.

Valid data types for `attribute-type` are:

- boolean
- string
- integer
- unsigned integer
- ipaddr
- date
- version
- octet-array

For more information about attribute data types, see [Posture Validation Attribute Data Types, page 13-6](#).

Adding Attributes

You can use the Add Attribute option to add or modify the posture validation attributes that ACS supports. Adding attributes requires that you have prepared an attribute definition file, which is a text file that provides the required information for each attribute to be added. For an explanation of the contents of a posture validation attribute definition file, see [Posture Validation Attribute Definition File, page 8-44](#). For an example of an attribute definition file, see [Default Posture Validation Attribute Definition File, page 8-51](#).

Before You Begin

You can use the steps in [Exporting \(Dumping\) Attributes, page 8-50](#), to create a backup of posture validation attribute definitions. You can also use the exported attribute definition file to check the `vendor-id`, `application-id`, and `attribute-id` of current posture validation attributes.



Note Completion of this procedure requires restart of the **CSAuth** service, which temporarily suspends authentication services. You should consider performing this procedure when demand for ACS services is low.

To add attributes:

-
- | | |
|---------------|---|
| Step 1 | You can use the discussion in Posture Validation Attribute Definition File, page 8-44 to create a properly formatted attribute definition file. |
| Step 2 | Place the attribute definition file in a directory that ACS can access by using FTP. |
| Step 3 | In the navigation bar, click System Configuration . |
| Step 4 | Click CNAC Attribute Management . |
| | The CNAC Attribute Management page appears. Under Add Attributes, the FTP Server, Login, Password, and Remote Directory options contain the values from the most recent session on this page. |
| Step 5 | Select the Add Attributes option. |

Step 6 To add or modify attributes, place the attribute definition file in a directory that can be accessed by using FTP. Enter the following information to access the attribute definition file:

- a. In the **FTP Server** box, enter the IP address or hostname of the FTP server that has the attribute definition file that you want to download.



Tip If you specify the hostname, DNS must be correctly working on your network.

- b. In the **Login** box, enter a valid username that ACS can use to access the FTP server.
- c. In the **Password** box, enter the password for the username that you specified in the Login box.
- d. In the **Remote Directory** box, enter relative path from the FTP server root directory to the directory containing the attribute definition file that you want ACS to download from the FTP server.
- e. In the **Attributes File Name** box, enter the name of the attribute definition file that you want ACS to download from the FTP server.

Step 7 Click **Submit**.

ACS downloads the attribute definition file and updates its attribute definitions according to the information that you provided in the file. The System Configuration page appears.



Tip If ACS has problems transferring the file, the page on the right displays a self-explanatory error message.

Step 8 If you have no more changes to make to the attribute definitions in ACS and you want your changes to take effect, restart the following services:

- **CSAuth and CSLog**—See [Stopping, Starting, or Restarting Services, page 7-2](#).
- **CSAdmin**—You can use the **restart** command at the serial console. For more information about this command, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Deleting Attributes

You can delete one posture validation attribute at a time from ACS. Posture validation attributes are uniquely identified by the combination of the `vendor-id`, `application-id`, and `attribute-id`. You can determine this information for any attribute by reading the attribute definition file created by the **Dump Attributes** option.

Before You Begin

You can use the steps in [Exporting \(Dumping\) Attributes, page 8-50](#) to create a backup of posture validation attribute definitions. You can also use the exported attribute definition file to check the `vendor-id`, `application-id`, and `attribute-id` of the posture validation attribute that you want to delete.



Caution

ACS provides no confirmation step when you delete a posture validation attribute. Be sure that you use the steps in [Exporting \(Dumping\) Attributes, page 8-50](#) to create a backup of your posture validation attribute definitions.

For more information about posture validation attributes and how they are identified, see [About Posture Credentials and Attributes, page 13-5](#). For more information about extended attributes, see [Extended Attributes, page 13-6](#).



Note Completion of this procedure requires restart of the **CSAuth** service, which temporarily suspends authentication services. You should consider performing this procedure when demand for ACS services is low.

To delete posture validation attributes:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **CNAC Attribute Management**.
The CNAC Attribute Management page appears.
- Step 3** Select the **Delete Attribute** option.
- Step 4** Enter the details that identify the attribute:
- In the **Vendor ID** box, enter the number that identifies the vendor.
 - In the **Application ID** box, enter the number that identifies the application.
 - In the **Attribute ID** box, enter the number that identifies the attribute.
- The attribute that you want to delete is uniquely identified.
- Step 5** Click **Submit**.
ACS deletes the definition for the attribute that you specified.
- Step 6** If you have no more changes to make to the attribute definitions in ACS and you want your changes to take effect, restart the following services:
- **CSAuth and CSLog**—See [Stopping, Starting, or Restarting Services, page 7-2](#).
 - **CSAdmin**—You can use the **restart** command at the serial console. For more information about this command, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.
-

To delete an extended posture validation entity attribute in the Cisco:Host application:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **CNAC Attribute Management**.
The CNAC Attribute Management page appears.
- Step 3** Select the **Delete Extended Attribute Entity** option.
- Step 4** Enter the details required to identify the attribute that you want ACS to delete:
- In the **Attribute ID** box, enter the number that identifies the attribute.
 - In the **Entity** box, enter the name of the entity.
- The attribute that you want to delete is uniquely identified.
- Step 5** Click **Submit**.
ACS deletes its definition for the attribute that you specified.

- Step 6** If you have no more changes to make to the attribute definitions in ACS and you want your changes to take effect, restart the following services:
- **CSAuth and CSLog**—See [Stopping, Starting, or Restarting Services, page 7-2](#).
 - **CSAdmin**—You can use the **restart** command at the serial console. For more information about this command, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

To delete a property of an extended posture validation entity attribute in the Cisco:Host application:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **CNAC Attribute Management**.
The CNAC Attribute Management page appears.
- Step 3** Select the **Delete Extended Attribute Property** option.
- Step 4** Enter the details that identify the attribute property:
- In the **Attribute ID** box, enter the number that identifies the attribute.
 - In the **Property ID** box, enter the number that identifies the property.
- The extended attribute property that you want to delete is uniquely identified.
- Step 5** Click **Submit**.
ACS deletes the property definition for the attribute that you specified.
- Step 6** If you have no more changes to make to the attribute definitions in ACS and you want your changes to take effect, restart the following services:
- **CSAuth and CSLog**—See [Stopping, Starting, or Restarting Services, page 7-2](#).
 - **CSAdmin**—You can use the **restart** command at the serial console. For more information about this command, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Exporting (Dumping) Attributes

You can use the **Dump Attributes** option to download an attribute definition file that contains definitions for all the current attribute definitions that ACS has. This file contains attributes, such as their data type, and their vendor, application, and attribute IDs. The file also is useful for creating a backup of attribute definitions before you add, modify, or delete attributes.

To export a file of definitions for all NAC attributes:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **CNAC Attribute Management**.
The CNAC Attribute Management page appears.
- Step 3** Click the **Dump Attributes** option.
- Step 4** Click **Submit**.
A file generation status message appears.
- Step 5** If the status message indicates that the file is not ready, click **Refresh** until the file is ready.

Step 6 Click **Download**.

A dialog box prompts you for a location to save a file named `AvpDump.txt`. AVP is the abbreviation for attribute-value pair.

Step 7 Choose a location for saving the file and, if you prefer, change the name of the file to a more meaningful name.**Tip**

Consider identifying the attribute definition file by the hostname of ACS and the current date. For example, if the hostname is `acs01primary` and the date is June 13, 2004, saving the file as `avp-acs01primary-06132004.txt` readily identifies the origin of the file.

Step 8 Save the file.

ACS continues to display the status message.

**Tip**

To leave this page, you can click **Cancel**, **Refresh**, or any of the buttons on the navigation bar.

Default Posture Validation Attribute Definition File

[Example 8-2](#) provides the default definitions for the posture validation attributes that ACS provides. If you need to reset the default attributes to their original definitions, use [Example 8-2](#) to create a posture validation attribute definition file. For more information about the format of an attribute definition file, see [Posture Validation Attribute Definition File, page 8-44](#).

Example 8-2 Default Posture Validation Attribute Definitions

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#1]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#2]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00003
```

```
attribute-name=PA-Name
attribute-profile=in out
attribute-type=string

[attr#3]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00004
attribute-name=PA-Version
attribute-profile=in out
attribute-type=version

[attr#4]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00005
attribute-name=OS-Type
attribute-profile=in out
attribute-type=string

[attr#5]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00006
attribute-name=OS-Version
attribute-profile=in out
attribute-type=version

[attr#6]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00007
attribute-name=PA-User-Notification
attribute-profile=out
attribute-type=string

[attr#7]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#8]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#9]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00006
attribute-name=ServicePacks
attribute-profile=in
attribute-type=string

[attr#10]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00007
attribute-name=HotFixes
attribute-profile=in
attribute-type=string

[attr#11]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00008
attribute-name=HostFQDN
attribute-profile=in
attribute-type=string

[attr#12]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#13]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#14]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00005
attribute-name=CSAVersion
attribute-profile=in
attribute-type=version

[attr#15]
vendor-id=9
vendor-name=Cisco
application-id=5
```

```

application-name=HIP
attribute-id=00009
attribute-name=CSAOperationalState
attribute-profile=in
attribute-type=unsigned integer

[attr#16]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00011
attribute-name=TimeSinceLastSuccessfulPoll
attribute-profile=in
attribute-type=unsigned integer

[attr#17]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32768
attribute-name=CSAMCName
attribute-profile=in
attribute-type=string

[attr#18]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32769
attribute-name=CSAStates
attribute-profile=in
attribute-type=string

[attr#19]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#20]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#21]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out

```

```
attribute-type=string

[attr#22]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer

[attr#23]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
attribute-type=version

[attr#24]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00006
attribute-name=Scan-Engine-Version
attribute-profile=in out
attribute-type=version

[attr#25]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00007
attribute-name=Dat-Version
attribute-profile=in out
attribute-type=version

[attr#26]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00008
attribute-name=Dat-Date
attribute-profile=in out
attribute-type=date

[attr#27]
vendor-id=393
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00009
attribute-name=Protection-Enabled
attribute-profile=in out
attribute-type=unsigned integer

[attr#28]
vendor-id=393
```

```
vendor-name=Symantec
application-id=3
application-name=AV
attribute-id=00010
attribute-name=Action
attribute-profile=out
attribute-type=string

[attr#29]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#30]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

[attr#31]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out
attribute-type=string

[attr#32]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer

[attr#33]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
attribute-type=version

[attr#34]
vendor-id=3401
vendor-name=NAI
application-id=3
application-name=AV
attribute-id=00006
```



```
attribute-name=Scan-Engine-Version  
attribute-profile=in out  
attribute-type=version
```

```
[attr#35]  
vendor-id=3401  
vendor-name=NAI  
application-id=3  
application-name=AV  
attribute-id=00007  
attribute-name=Dat-Version  
attribute-profile=in out  
attribute-type=version
```

```
[attr#36]  
vendor-id=3401  
vendor-name=NAI  
application-id=3  
application-name=AV  
attribute-id=00008  
attribute-name=Dat-Date  
attribute-profile=in out  
attribute-type=date
```

```
[attr#37]  
vendor-id=3401  
vendor-name=NAI  
application-id=3  
application-name=AV  
attribute-id=00009  
attribute-name=Protection-Enabled  
attribute-profile=in out  
attribute-type=unsigned integer
```

```
[attr#38]  
vendor-id=3401  
vendor-name=NAI  
application-id=3  
application-name=AV  
attribute-id=00010  
attribute-name=Action  
attribute-profile=out  
attribute-type=string
```

```
[attr#39]  
vendor-id=6101  
vendor-name=Trend  
application-id=3  
application-name=AV  
attribute-id=00001  
attribute-name=Application-Posture-Token  
attribute-profile=out  
attribute-type=unsigned integer
```

```
[attr#40]  
vendor-id=6101  
vendor-name=Trend  
application-id=3  
application-name=AV  
attribute-id=00002  
attribute-name=System-Posture-Token  
attribute-profile=out  
attribute-type=unsigned integer
```

```
[attr#41]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00003
attribute-name=Software-Name
attribute-profile=in out
attribute-type=string

[attr#42]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00004
attribute-name=Software-ID
attribute-profile=in out
attribute-type=unsigned integer

[attr#43]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00005
attribute-name=Software-Version
attribute-profile=in out
attribute-type=version

[attr#44]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00006
attribute-name=Scan-Engine-Version
attribute-profile=in out
attribute-type=version

[attr#45]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00007
attribute-name=Dat-Version
attribute-profile=in out
attribute-type=version

[attr#46]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00008
attribute-name=Dat-Date
attribute-profile=in out
attribute-type=date

[attr#47]
vendor-id=6101
vendor-name=Trend
application-id=3
```

```
application-name=AV
attribute-id=00009
attribute-name=Protection-Enabled
attribute-profile=in out
attribute-type=unsigned integer

[attr#48]
vendor-id=6101
vendor-name=Trend
application-id=3
application-name=AV
attribute-id=00010
attribute-name=Action
attribute-profile=out
attribute-type=string

[attr#49]
vendor-id=10000
vendor-name=out
application-id=1
application-name=CNAC
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=string

[attr#50]
vendor-id=10000
vendor-name=out
application-id=1
application-name=CNAC
attribute-id=00002
attribute-name=System-Posture-Token
attribute-profile=out
attribute-type=string

[attr#51]
vendor-id=10000
vendor-name=out
application-id=1
application-name=CNAC
attribute-id=00003
attribute-name=Reason
attribute-profile=out
attribute-type=string
```



CHAPTER 9

System Configuration: Authentication and Certificates

This chapter addresses authentication and certification features in the System Configuration section of the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

This chapter contains:

- [About Certification and EAP Protocols, page 9-1](#)
- [Global Authentication Setup, page 9-21](#)
- [ACS Certificate Setup, page 9-22](#)
- [EAP-FAST PAC Files Generation \(ACS SE\), page 9-37](#)
- [Advanced System Configuration Pages Reference, page 9-40](#)

About Certification and EAP Protocols

ACS uses Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), and Protected Extensible Authentication Protocol (PEAP) authentication protocols in combination with digital certification to ensure the protection and validity of authentication information.

This section contains:

- [Digital Certificates, page 9-1](#)
- [EAP-TLS Authentication, page 9-2](#)
- [PEAP Authentication, page 9-6](#)
- [EAP-FAST Authentication, page 9-9](#)

Digital Certificates

You use the ACS Certificate Setup pages to install digital certificates to support EAP-TLS, EAP-FAST, and PEAP authentication, as well as to support Secure HyperText Transfer Protocol (HTTPS) protocol for secure access to the ACS web interface. ACS uses the X.509 v3 digital certificate standard. Certificate files must be in Base64-encoded X.509 format or Distinguished Encoding Rules (DER)-encoded binary X.509 format. Also, ACS supports manual certificate enrollment and provides the means for managing a certificate trust list (CTL) and certificate revocation lists (CRL).

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 certification authority (CA) or, if you choose, may be a self-signed certificate. For more information, see [Installing an ACS Server Certificate, page 9-22](#), and [Using Self-Signed Certificates, page 9-33](#).

**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.

EAP-TLS Authentication

This section contains:

- [About the EAP-TLS Protocol, page 9-2](#)
- [EAP-TLS and ACS, page 9-3](#)
- [EAP-TLS Limitations, page 9-4](#)
- [Enabling EAP-TLS Authentication, page 9-4](#)
- [EAP-TLS and ACS in a NAC/NAP Environment, page 9-5](#)

About the EAP-TLS Protocol

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. The EAP-TLS authentication protocol uses the certificates of ACS and of the end-user client, enforcing mutual authentication of the client and ACS. For more detailed information on EAP, TLS, and EAP-TLS, refer to the following IETF RFCs: [Extensible Authentication Protocol \(EAP\) RFC 3784](#), [The TLS Protocol RFC 2246](#), and [PPP EAP TLS Authentication Protocol RFC 2716](#).

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 [About Self-Signed Certificates, page 9-33](#).

EAP-TLS requires support from the end client and the Authentication, Authorization, and Accounting (AAA) client. An example of an EAP-TLS client includes the Microsoft Windows XP operating system.

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.

EAP-TLS and ACS

ACS supports EAP-TLS with any end-user client that supports EAP-TLS, such as Windows XP, Funk (Juniper), or Meetinghouse clients. To learn which user databases support EAP-TLS, see [Authentication Protocol-Database Compatibility, page 1-8](#). For more information about deploying EAP-TLS authentication, see *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks* at

http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a008009256b.shtml

ACS can use EAP-TLS to support machine authentication to Microsoft Windows Active Directory. The end-user client may limit the protocol for user authentication to the same protocol that is used for machine authentication; that is, use of EAP-TLS for machine authentication may require the use of EAP-TLS for user authentication. For more information about machine authentication, see [Machine Authentication, page 12-10](#).

To permit user access to the network or computer authenticating with EAP-TLS, ACS must verify that the claimed identity (presented in the EAP Identity response) corresponds to the certificate that the user presents. ACS can accomplish this verification in three ways:

- **Certificate SAN Comparison**—Based on the name in the Subject Alternative Name field in the user certificate.
- **Certificate CN Comparison**—Based on the name in the Subject Common Name field in the user certificate.
- **Certificate Binary Comparison**—Based on a binary comparison between the user certificate in the user object in the LDAP server or Active Directory and the certificate that the user presents during EAP-TLS authentication. This comparison method cannot be used to authenticate users who are in an ODBC external user database (ACS for Windows only).



Note If you use certificate binary comparison, the user certificate must be stored in a binary format. Also, for generic LDAP and Active Directory, the attribute that stores the certificate must be the standard LDAP attribute named **usercertificate**.

When you set up EAP-TLS, you can select the criterion (one, two, or all) that ACS uses. For more information, see [Configuring Authentication Options, page 9-21](#).

ACS supports a session resume feature for EAP-TLS-authenticated user sessions, which is a particularly useful feature for WLANs, wherein a user may move the client computer to set a different wireless access point. When this feature is enabled, ACS caches the TLS session that is created during EAP-TLS authentication, provided that the user successfully authenticates. If a user needs to reconnect and the original EAP-TLS session has not timed out, ACS uses the cached TLS session, resulting in faster EAP-TLS performance and lessened AAA server load. When ACS resumes an EAP-TLS session, the user reauthenticates by a secure sockets layer (SSL) handshake only, without a certificate comparison.

In effect, enabling an EAP-TLS session resume allows ACS to trust a user based on the cached TLS session from the original EAP-TLS authentication. Because ACS only caches a TLS session when a new EAP-TLS authentication succeeds, the existence of a cached TLS session is proof that the user has successfully authenticated in the number of minutes that the EAP-TLS session timeout option specified.

**Note**

Session timeout is based on the time of the initial, full authentication of the session. It does not depend on an accounting start message.

The Session resume feature does not enforce changes to the group assignment in an external user database; because group mapping does not occur when a user session is resumed. Instead, the user is mapped to the same ACS group to which the user was mapped at the beginning of the session. At the start of a new session, group mapping enforces the new group assignment.

To force an EAP-TLS session to end before the session timeout is reached, you can restart the **CSAuth** service or delete the user from the ACS user database. Disabling or deleting the user in an external user database has no effect because the session resume feature does not involve the use of external user databases.

You can enable the EAP-TLS session resume feature and configure the timeout interval on the Global Authentication Setup page. For more information about enabling this feature, see [Global Authentication Setup, page 9-21](#).

EAP-TLS Limitations

The limitations in the ACS implementation of EAP-TLS are:

- **Server and CA certificate file format**—If you install the ACS server and CA certificates from files, rather than from certificate storage, server and CA certificate files must be in Base64-encoded X.509 format or DER-encoded binary X.509 format.
- **LDAP attribute for binary comparison**—If you configure ACS to perform binary comparison of user certificates, the user certificate must be stored in the Active Directory or an LDAP server by using a binary format. Also, the attribute storing the certificate must be named **usercertificate**.
- **Windows server type**—If you want to use Active Directory to authenticate users with EAP-TLS when ACS runs on a member server, additional configuration is required. For more information, including steps for the additional configuration, see the *Installation Guide for Cisco Secure ACS for Windows Release 4.2* or the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

**Note**

ACS supports UTF-8 (the 8-bit Universal Coded Character Set (UCS)/Unicode Transformation Format) for the username and password only when authenticating with Active Directory (AD). The UTF-8 format can preserve the full US-ASCII range, providing compatibility with the existing ASCII handling software.

Enabling EAP-TLS Authentication

This section explains the procedures that are required to configure ACS to support EAP-TLS authentication.

**Note**

You must configure end-user client computers to support EAP-TLS. This procedure is specific to the configuration of ACS only. For more information about deploying EAP-TLS authentication, see *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks* at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.htm.

Before You Begin

For EAP-TLS machine authentication, if you have configured a Microsoft certification authority server on the domain controller, you can configure a policy in Active Directory to produce a client certificate automatically when a computer is added to the domain. For more information, refer to the pertinent Knowledge Base Article on the Microsoft website.

To enable EAP-TLS authentication:

- Step 1** Install a server certificate in ACS. EAP-TLS requires a server certificate. For detailed steps, see [Installing an ACS Server Certificate, page 9-22](#).

**Note**

If you have previously installed a certificate to support EAP-TLS, or PEAP user authentication, or to support HTTPS protection of remote ACS administration, you do not need to perform this step. A single server certificate is sufficient to support all certificate-based ACS services and remote administration; however, EAP-TLS, EAP-FAST and PEAP require that the certificate be suitable for server authentication purposes.

- Step 2** Edit the certification trust list so that the CA issuing end-user client certificates is trusted. If you do not perform this step, ACS only trusts user certificates that were issued by the same CA that issued the certificate that is installed in ACS. For detailed steps, see [Editing the Certificate Trust List, page 9-28](#).
- Step 3** Establish a certificate revocation list (CRL) for each CA and certificate type in the certificate trust list (CTL). As part of EAP-TLS authentication, ACS validates the status of the certificate presented by the user against the cached CRL to ensure that it has not been revoked. For detailed steps, see [Editing the Certificate Trust List, page 9-28](#).
- Step 4** Enable EAP-TLS on the Global Authentication Setup page. In ACS, you complete this step only after you have successfully completed Step 1. For detailed steps, see [Configuring Authentication Options, page 9-21](#).
- Step 5** Configure a user database. To determine which user databases support EAP-TLS authentication, see [Authentication Protocol-Database Compatibility, page 1-8](#).
- ACS is ready to perform EAP-TLS authentication.

EAP-TLS and ACS in a NAC/NAP Environment

You can deploy ACS in a Cisco Network Admission Control and Microsoft Network Access Protection (NAC/NAP) environment. In the NAC/NAP environment, NAP client computers authorize with ACS by using EAP over UDP (EoU) or EAP over 802.1x.

When a NAP client (a computer running Windows Vista or Windows Longhorn Server) connects, it uses a NAP agent to send ACS one of the following. A

- List of Statements of Health (SoHs).
- Certificate that the client has obtained from a Microsoft Health Registration Authority (HRA).

The ACS host validates the client credentials as follows:

- If the NAP agent sends a list of SoHs, the ACS sends the list to a Microsoft Network Policy Server (NPS) by using the Cisco Host Credentials Authorization Protocol (HCAP). The NPS evaluates the SoHs. The ACS then sends an appropriate network access profile to the network access device (switch, router, VPN, and so on) to grant the authorized level of access to the client.
- If the NAP agent sends a health certificate rather than a list of SoHs, then ACS validates the certificate as the EAP-FAST session is established to determine the overall health state of the client. The ACS then sends the appropriate network access profile to the network to grant the authorized level of access to the client.

You can configure ACS to process access requests from NAP clients by setting up one or more network access profiles that customize ACS to operate in the NAC/NAP environment. For details on how to configure ACS to function in a NAC/NAP environment, refer to Chapter 9 of the *Configuration Guide for Cisco Secure ACS 4.2*, “NAC/NAP Configuration Scenario.”

PEAP Authentication

This section contains:

- [About the PEAP Protocol, page 9-6](#)
- [PEAP and ACS, page 9-7](#)
- [PEAP and the Unknown User Policy, page 9-8](#)
- [Enabling PEAP Authentication, page 9-8](#)

About the PEAP Protocol

The PEAP protocol is a client-server security architecture that you use to encrypt EAP transactions; thereby protecting the contents of EAP authentications.

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 authentication type that is negotiated during the second conversation may be any valid EAP type, such as EAP-GTC (for Generic Token Card). Because PEAP can support any EAP authentication protocol, individual combinations of PEAP and EAP protocols are denoted with the EAP protocol in parentheses, such as PEAP (EAP-GTC). In phase two, PEAP supports the following authentication protocols:
 - EAP-MSCHAPv2
 - EAP-GTC

- EAP-TLS
- One improvement in security that PEAP offers is identity protection. This improvement is the potential of 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 Cisco Aironet PEAP client sends user identity through the SSL tunnel only. The initial identity, used in phase one and which is sent in the clear, is the MAC address of the end-user client with **PEAP_** as a prefix. The Microsoft PEAP client does not provide identity protection; the Microsoft PEAP client sends the username in clear text in phase one of PEAP authentication.

PEAP and ACS

ACS supports PEAP authentication by using the Cisco Aironet PEAP client or the Microsoft PEAP client that is included with Microsoft Windows XP Service Pack 1. ACS can support the Cisco Aironet PEAP client with PEAP(EAP-GTC) only. For the Microsoft PEAP client in Windows XP Service Pack 1, ACS supports PEAP(EAP-MS-CHAPv2) or PEAP (EAP-TLS). For information about which user databases support PEAP protocols, see [Authentication Protocol-Database Compatibility, page 1-8](#).

PEAP with the Cisco Aironet PEAP Client

When the end-user client is the Cisco Aironet PEAP client, and PEAP(EAP-GTC) and PEAP(EAP-MS-CHAPv2) are enabled on the Global Authentication Setup page, ACS first attempts PEAP(EAP-GTC) authentication with the end-user client. If the client rejects this protocol (by sending an EAP NAK message), ACS attempts authentication with PEAP(EAP-MS-CHAPv2). For more information about enabling EAP protocols that PEAP supports, see [Global Authentication Setup, page 9-21](#).

PEAP and Microsoft Windows Active Directory

ACS can use PEAP(EAP-MS-CHAPv2) to support machine authentication to Microsoft Windows Active Directory. The end-user client may limit the protocol that is used for user authentication to the same protocol that is used for machine authentication; that is, use of PEAP for machine authentication requires the use of PEAP for user authentication. For more information about machine authentication, see [Machine Authentication, page 12-10](#).

The Session Resume Feature

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 lessened AAA server load.



Note

Session timeout is based on the time that authentication succeeds. It does not depend on accounting.

You can enable the PEAP session resume feature and configure the timeout interval on the Global Authentication Setup page. For more information about enabling this feature, see [Global Authentication Setup, page 9-21](#).

ACS also supports a fast reconnect feature. When the session resume feature is enabled, the fast reconnect feature causes ACS to allow a PEAP session to resume without checking user credentials. In effect, ACS can trust a user based on the cached TLS session from the original PEAP authentication when this feature is enabled. Because ACS only caches a TLS session when phase two of PEAP authentication succeeds, the existence of a cached TLS session is proof that the user has successfully authenticated in the number of minutes that the PEAP session timeout option specifies.

The session resume feature does not enforce changes to group assignment in an external user database; group mapping does not occur when the session resume feature extends a user session. Instead, the user is mapped to the same ACS group that the user was mapped to at the beginning of the session. At the start of a new session, group mapping enforces the new group assignment.

The fast reconnect feature is particularly useful for wireless LANs, wherein a user may move the client computer so that a different wireless access point is in use. When ACS resumes a PEAP session, the user reauthenticates without entering a password, provided that the session has not timed out. If the end-user client is restarted, the user must enter a password; even if the session timeout interval has not ended.

You can enable the PEAP fast reconnect feature on the Global Authentication Setup page. For more information about enabling this feature, see [Global Authentication Setup, page 9-21](#).

**Note**

Re-use of an established session through fast reconnect will only work when ACS' dynamic users are NOT removed. When dynamic users are explicitly removed, re-use of established sessions is not possible, and ACS will try to do full authentication in the usual manner.

PEAP and the Unknown User Policy

During PEAP authentication, ACS might not know the real username to be authenticated until phase two of authentication. While the Microsoft PEAP client does reveal the actual username during phase one, the Cisco PEAP client does not; therefore, ACS does not attempt to look up the username that is presented during phase one and the use of the Unknown User Policy is irrelevant during phase one, regardless of the PEAP client used.

When phase two of PEAP authentication occurs and the username that the PEAP client presents is unknown to ACS, ACS processes the username in the same way that it processes usernames that are presented in other authentication protocols. If the username is unknown and the Unknown User Policy is disabled, authentication fails. If the username is unknown and the Unknown User Policy is enabled, ACS attempts to authenticate the PEAP user with unknown user processing.

For more information about unknown user processing, see [About Unknown User Authentication, page 15-3](#).

Enabling PEAP Authentication

This procedure provides an overview of the detailed procedures that are required to configure ACS to support PEAP authentication.

**Note**

You must configure end-user client computers to support PEAP. This procedure is specific to configuration of ACS only.

To enable PEAP authentication:

- Step 1** Install a server certificate in ACS. PEAP requires a server certificate. For detailed steps, see [Installing an ACS Server Certificate, page 9-22](#).

**Note**

If you have previously installed a certificate to support EAP-TLS or PEAP user authentication, or to support HTTPS protection of remote ACS administration, you do not need to perform this step. A single server certificate is sufficient to support all certificate-based ACS services and remote administration; however, EAP-TLS and PEAP require that the certificate be suitable for server authentication purposes.

- Step 2** Enable PEAP on the Global Authentication Setup page. You use ACS to complete this step only after you have successfully completed Step 1. For detailed steps, see [Configuring Authentication Options, page 9-21](#).
- Step 3** Configure a user database. To determine which user databases support PEAP authentication, see [Authentication Protocol-Database Compatibility, page 1-8](#).
- ACS is ready to perform PEAP authentication for most users. For more information, see [PEAP and the Unknown User Policy, page 9-8](#).
- Step 4** Consider enabling the Unknown User Policy to simplify PEAP authentication. For more information, see [PEAP and the Unknown User Policy, page 9-8](#). For detailed steps, see [Configuring the Unknown User Policy, page 15-8](#).

EAP-FAST Authentication

This section contains:

- [About EAP-FAST, page 9-9](#)
- [About Master Keys, page 9-11](#)
- [About PACs, page 9-12](#)
- [Provisioning Modes, page 9-13](#)
- [Types of PACs, page 9-13](#)
- [EAP-FAST for Anonymous TLS Renegotiation, page 9-16](#)
- [PAC Free EAP-FAST, page 9-16](#)
- [EAP-FAST PKI Authorization Bypass, page 9-16](#)
- [Master Key and PAC TTLs, page 9-17](#)
- [Replication and EAP-FAST, page 9-17](#)
- [Enabling EAP-FAST, page 9-19](#)

About 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:

www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

The EAP-FAST protocol 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 the significantly faster of the two solutions that provide encrypted EAP transactions. 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 PAC Provisioning, page 9-14](#).) 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. If EAP-MS-CHAPv2 authentication succeeds, ACS provides the user with a PAC. To determine which databases support EAP-FAST phase zero, see [Authentication Protocol-Database Compatibility, page 1-8](#).



Note Phase zero is optional and PACs can be manually provided to end-user clients. (See [Manual PAC Provisioning, page 9-15](#).) You control whether ACS supports phase zero by checking the Allow automatic PAC provisioning check box in the Global Authentication Configuration page.

The Allow anonymous in-band PAC provisioning option provisions 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-MS-CHAP will be used as inner method only.)

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 and a trusted root CA on ACS.

By default, ACS supports TLS server-side authentication; however, if the client sends the user certificate to ACS, mutual TLS authentication is performed and inner methods are bypassed.

Phase zero of EAP-FAST does not enable a network service; therefore, even a successful EAP-FAST phase zero transaction is recorded in the ACS Failed Attempts log.

If the Accept client on authenticated provisioning option is selected, ACS always sends an Access-Reject at the end of the provisioning phase (phase zero), forcing the client to reauthenticate by using the tunnel PAC. This option sends an Access-Accept to the client and can be enabled only when you check the Allow authenticated in-band PAC provisioning check box.

- **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 based on a master key that has not expired. The means by which PAC provisioning has occurred is irrelevant; you can use automatic or manual provisioning.

No network service is enabled by phase one of EAP-FAST.

- **Phase two**—In phase two, ACS authenticates the user credentials with EAP-GTC, which is protected by the TLS tunnel that was created in phase one. EAP-GTC, TLS and MS-CHAP are supported as inner methods. No other EAP types are supported for EAP-FAST. To determine which databases support EAP-FAST phase two, see [Authentication Protocol-Database Compatibility, page 1-8](#).

ACS authorizes network service with a successful user authentication in phase two of EAP-FAST and logs the authentication in the Passed Authentications log, if it is enabled. Also, if necessary, ACS may refresh the end-user client PAC, which creates a second entry in the Passed Authentication log for the same phase two transaction.

**Note**

This version of ACS supports EAP-FAST phase two for NAC phase two and is for wired clients only.

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. The Cisco Aironet EAP-FAST client protects the username in phase one by sending `FAST_MAC address` in place of the username. 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. For more information about password aging for Windows user databases, see [Enabling Password Aging for the ACS Internal Database, page 5-15](#).

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 9-12](#).
- **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: the active master key or a retired master key.

To increase the security of EAP-FAST, ACS changes the master key that it uses to generate PACs. ACS uses time-to-live (TTL) values that you define to determine when it generates a new master key and the age of all master keys. Based on TTL values, ACS assigns master keys one of the these states:

- **Active**—An active master key is the master key used by ACS to generate PACs. The master key TTL setting determines the duration that a master key remains active. At any time, only one master key is active. When you define TTLs for master keys and PACs, ACS permits only a PAC TTL that is shorter than the active master key TTL. This limitation ensures that a PAC is refreshed at least once before the expiration of the master key used to generate the PAC, provided that EAP-FAST users log in to the network at least once before the master key expires. For more information about how TTL values determine whether PAC refreshing or provisioning is required, see [Master Key and PAC TTLs, page 9-17](#).

When you configure ACS to receive replicated EAP-FAST policies and master keys, a backup master key is among the master keys received. The backup master key is used only if the active master key retires before the next successful master key replication. If the backup master key also retires before the next successful master key replication, EAP-FAST authentication fails for all users requesting network access with EAP-FAST.

**Tip**

If EAP-FAST authentication fails because the active and backup master keys have retired and ACS has not received new master keys in replication, you can force ACS to generate its own master keys by checking the **EAP-FAST Master Server** check box and clicking **Submit**.

ACS records the generation of master keys in the logs for the **CSAuth** service.

- **Retired**—When a master key becomes older than the master key TTL settings, it is considered retired for the duration that the Retired master key TTL settings specify. ACS can store up to 255 retired master keys. While a retired master key is not used to generate new PACs, ACS needs it to authenticate PACs that were generated by using it. When you define TTLs for master keys and retired master keys, ACS permits only TTL settings that require storing 255 or fewer retired master keys. For example, if the master key TTL is one hour and the retired master key TTL is four weeks, this would require storing up to 671 retired master keys; therefore, an error message appears and ACS does not allow these settings.

When a user gains network access by using a PAC that is generated with a retired master key, ACS provides the end-user client with a new PAC that the active master key generated. For more information about ACS master keys and PACs, see [Master Key and PAC TTLs, page 9-17](#).

- **Expired**—When a master key becomes older than the sum of the master key TTL and retired master TTL settings, it is considered expired and ACS deletes it from its records of master keys. For example, if the master key TTL is one hour and the retired master key TTL is one week, a master key expires when it becomes greater than one week and one hour old.

PACs that an expired master key cannot be used to access your network. An end-user client presenting a PAC that generated an expired master key requires a new PAC by using automatic or manual provisioning before phase one of EAP-FAST can succeed.

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 server's identify 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. ACS determines whether the PAC was generated using one of the master keys it is aware of: active or retired. (A PAC that is generated by using a master key that has since expired can never be used to gain network access.) When an end-user client has a PAC that is generated with an expired master key, the end-user client must receive a new PAC before EAP-FAST phase one can succeed. The means of providing PACs to end-user clients, known as PAC provisioning, are discussed in [Automatic PAC Provisioning, page 9-14](#) and [Manual PAC Provisioning, page 9-15](#).

After end-user clients are provided PACs, ACS refreshes them as that master key and PAC TTL values specify. ACS generates and sends a new PAC as needed at the end of phase two of EAP-FAST; however, if you shorten the master key TTL, you might require that PAC provisioning occur. For more information about how master key and PAC states determine whether ACS sends a new PAC to the end-user client at the end of phase two, see [Master Key and PAC TTLs, page 9-17](#).

Regardless of the master key TTL values that you define, a user will require PAC provisioning when the user does not use EAP-FAST to access the network before the master key that generated the user's PAC has expired. For example, if the master key TTL is one week old and the retired master key TTL is one week old, each EAP-FAST end-user client used by someone who goes on vacation for two weeks will require PAC provisioning.

Provisioning Modes

ACS supports out-of-band and in-band provisioning modes. The in-band provisioning mode operates inside an Authenticated Diffie-Hellman Key Agreement Protocol (ADHP) tunnel before the peer authenticates the ACS server.

Since an unauthenticated server is provisioned, it is not possible to use a plain text password; so only MS-CHAP credentials can be used inside the tunnel. MS-CHAPv2 is used to prove the peer's identity and receives a PAC for further authentication sessions. This method minimizes the risk of exposing the user's credentials.

EAP-FAST has been enhanced to support an authenticated tunnel (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.

Since the server is authenticated as part of setting up the tunnel, weaker EAP methods, such as EAP-GTC can be used inside the tunnel to provide supplicant authentication.

At the end of a provisioning session that uses an authenticated tunnel, network access can be granted; since the server and user have authenticated each other.

ACS supports the following EAP types inside the tunnel for provisioning:

- EAP-GTC
- EAP-MS-CHAPv2
- EAP-TLS



Note By default, when using the EAP-GTC and EAP-MSCHAP inner methods, ACS allows up to three additional authentication attempts inside the SSL tunnel if the initial authentication attempt fails. After the fourth failed authentication attempt inside the SSL tunnel, ACS will terminate the EAP conversation, resulting in a RADIUS Access-Reject.

Types of PACs

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 PAC that have a wider contextual use.

The following types of PACs are provisioned to ACS, as per server policies:

- **Tunnel (Shared Secret) PAC, user or machine**—Distributed shared secret between the peer and ACS that is used to establish a secure tunnel and convey the policy of what must and can occur in the tunnel. The policy can include EAP methods, TLV exchanges, and identities that are allowed in the tunnel. It is up to the server policy to include what's necessary in PAC to enforce the policy in subsequent authentications that use the PAC. For example, in EAP-FAST Protocol Version 1, user identity I-ID is included as the part of the server policy. It limits the inner EAP methods to be carried only on the user identity that is provisioned. Other types of information can also be included, such as which EAP method and which cipher suite is allowed, for example. If the server policy is not

included in the PAC, then no validation or limitation on the inner EAP methods or user identities inside the tunnel established by use of this PAC. The PAC user of machine contains a type field. The format for the machine will be **host/name of machine**.

- **User Authorization PAC**—Distributed user authentication and authorization result based on a previous authentication. You can use it a with combination of the Tunnel PAC to bypass subsequent user authentication. This result is intended to be short-lived and also controlled by the peer. If any state of the user has changed that will affect the user authentication result (for example, user has logged on or off), the peer should discard it and not use it again. You can use the User Authorization PACs in combination of Tunnel PAC to allow a stateless server session resume as described in [Stateless Session Server Resume, page 9-20](#).
- **Posture PAC**—Distributed posture checking and authorization result based on a previous posture validation. You can use a posture PAC to optimize posture validation in the case of frequent revalidations. This result is specific to the posture validation application and may be used outside the contents of EAP-FAST.

The various means by which an end-user client can receive PACs are:

- **PAC provisioning**—Required when an end-user client has no PAC or has a PAC that is based on an expired master key. For more information about how master key and PAC states determine whether PAC provisioning is required, see [Master Key and PAC TTLs, page 9-17](#).

The two supported means of PAC provisioning are:

- **Automatic provision**—Sends a PAC by using a secure network connection. For more information, see [Automatic PAC Provisioning, page 9-14](#).
- **Manual provision**—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 9-15](#).
- **PAC refresh**—Occurs automatically when EAP-FAST phase two authentication has succeeded, and master key and PAC TTLs dictate that the PAC must be refreshed. For more information about how master key and PAC states determine whether a PAC is refreshed, see [Master Key and PAC TTLs, page 9-17](#).

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, provided that the master key that was used to generate it has not expired. Regardless of whether a PAC is active, if it is based on an expired master key, PAC provisioning must occur before EAP-FAST phase one can succeed.
- **Expired**—A PAC that is older than the PAC TTL is considered expired. Provided that the master key used to generate the PAC has not expired, an expired PAC can be used to complete EAP-FAST phase one and, at the end of EAP-FAST phase two, ACS will generate a new PAC for the user and provide it to the end-user client.

Automatic PAC Provisioning

Automatic PAC provisioning sends a new PAC to an end-user client over a secured network connection. Automatic PAC provisioning requires no intervention of the network user or a ACS administrator, provided that you configure ACS and the end-user client to support automatic provisioning.

EAP-FAST phase zero requires EAP-MS-CHAPv2 authentication of the user. At successful user authentication, ACS establishes a Diffie-Hellman tunnel with the end-user client. ACS generates a PAC for the user and sends it to the end-user client in this tunnel, along with the Authority ID and Authority ID information about this ACS.

**Note**

Because EAP-FAST phase zero and phase two use different authentication methods (EAP-MS-CHAPv2 in phase zero versus EAP-GTC in phase two), some databases that support phase two cannot support phase zero. Given that ACS associates each user with a single user database, the use of automatic PAC provisioning requires that EAP-FAST users are authenticated with a database 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-Database Compatibility, page 1-8](#).

No network service is enabled by phase zero of EAP-FAST; therefore, ACS logs a EAP-FAST phase zero transaction in the Failed Attempts log, including an entry that PAC provisioning occurred. After the end-user client has received a PAC through a successful phase zero, it sends a new EAP-FAST request to begin phase one.

**Note**

Because transmission of PACs in phase zero is secured by MS-CHAPv2 authentication and MS-CHAPv2 is vulnerable to dictionary attacks, we recommend that you limit use of automatic provisioning to initial deployment of EAP-FAST. After a large EAP-FAST deployment, PAC provisioning should be performed manually to ensure the highest security for PACs. For more information about manual PAC provisioning, see [Manual PAC Provisioning, page 9-15](#).

To control whether ACS performs automatic PAC provisioning, you use the options on the Global Authentication Setup page in the System Configuration section. For more information, see [EAP-FAST Configuration Page, page 9-44](#).

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. For example, if your EAP-FAST end-user client is the Cisco Aironet Client Utility (ACU), configuring the ACU to support EAP-FAST requires that you import a PAC file. For more information about configuring a Cisco ACU, see the applicable configuration guide for your ACU.

You can use manual PAC provisioning to control who can use EAP-FAST to access your network. If you disable automatic PAC provisioning, any EAP-FAST user denied a PAC cannot access the network. If your ACS deployment includes network segmentation, wherein access to each network segment is controlled by a separate ACS, 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.

**Note**

Replicating EAP-FAST master keys and policies affects the ability to require different PACs per ACS. For more information, see [Table 9-2](#).

While the administrative overhead of manual PAC provisioning is much greater than automatic PAC provisioning, it does not include the risk of sending the PAC over the network. When you first deploy EAP-FAST, using manual PAC provisioning would require a lot of manual configuration of end-user clients; however, this type of provisioning is the most secure means for distributing PACs. We recommend that, after a large EAP-FAST deployment, you should manually perform PAC provisioning to ensure the highest security for PACs.

You can generate PAC files for specific usernames, groups of users, lists of usernames, or all users. When you generate PAC files for groups of users or all users, the users must be known or discovered users and cannot be unknown users.

**Note**

ACS for Windows only: ACS for Windows supports the generation of PAC files with **CSUtil.exe**. For more information about generating PACs with **CSUtil.exe**, see [PAC File Generation, page C-26](#).

EAP-FAST for Anonymous TLS Renegotiation

You may be prompted to enter a password twice when you use an anonymous PAC provisioning schema. When you enter the password the first time, ACS provisions the PAC and sends an access-reject to the client. The client is then prompted to re-enter the password so that they will be able to authenticate and be granted access to the network.

ACS checks for a TLS client handshake record. If it finds the TLS client handshake record, ACS will initiate a TLS renegotiation at the end of EAP-Fast phase zero, instead of rejecting the user's request for access.

**Note**

You should use this option with a Vista client when the host is using anonymous PAC provisioning. When this option is enabled, ACS initiates the TLS renegotiation request to the client at the end of EAP-FAST phase zero, instead of rejecting the access attempt after PAC provisioning.

PAC Free EAP-FAST

With PAC Free EAP-FAST Authentication, you can run EAP-FAST on ACS without issuing or accepting any tunnel or machine generated PAC. Some PACs may be long-lived and not updated, which may cause authentication and security problems. When PAC Free 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 access-reject Reject is sent. The host/supplicant can reattempt to connect.

Anonymous phase zero, also known as ADHP is not supported for PAC Free since the protocol does not support rolling over to phase two. PAC Free EAP-Fast supports configuration and does not require a client certificate. For more information on how to configure PAC Free EAP-FAST see [Protocols Settings for profile_name Page, page 14-43](#), for more information.

EAP-FAST PKI Authorization Bypass

EAP-FAST PKI Authorization Bypass allows ACS to perform EAP-FAST tunnel establishment without authorizing the user against any database. Authorization is performed by retrieving the user's group data and certificate from an external database. ACS then compares at least one of the certificates, CN, or SAN to the values received from the client supplied certificate. If the comparison succeeds the group is mapped to an ACS user-group, otherwise authentication fails. When PKI Authorization Bypass is enabled this stage is passed over and the session is mapped to a pre-configured user-group. This feature allows a configuration that does not rely on external databases and increases reliability.

Although the EAP-FAST PKI Authorization Bypass feature is distinct from the PAC Free EAP-FAST feature, ACS does not allow you to enable PKI Authorization Bypass if PAC Free is not enabled. This dependency provides a way of revoking a user or machine's access, by forcing a mutually authenticated

handshake with a CRL or an external database lookup. If PKI Authorization Bypass would be able to implemented without PAC Free EAP-FAST, the user would be issued a PAC and access to the network would not be revoked until the PAC expired.

Master Key and PAC TTLs

The TTL values for master keys and PACs determine their states, as described in [About Master Keys, page 9-11](#) and [About PACs, page 9-12](#). Master key and PAC states determine whether someone requesting network access with EAP-FAST requires PAC provisioning or PAC refreshing.

[Table 9-1](#) summarizes ACS behavior with respect to PAC and master key states.

Table 9-1 Master Key versus PAC States

Master key state	PAC active	PAC expired
Master key active	Phase one succeeds. PAC is <i>not</i> refreshed at end of phase two.	Phase one succeeds. PAC is refreshed at end of phase two.
Master key retired	Phase one succeeds. PAC is refreshed at end of phase two.	Phase one succeeds. PAC is refreshed at end of phase two.
Master key expired	PAC provisioning is required. If automatic provisioning is <i>enabled</i> , phase zero occurs and a new PAC is sent. The end-user client initiates a new EAP-FAST authentication request using the new PAC. If automatic provisioning is <i>disabled</i> , phase zero does not occur and phase one fails. You must use manual provisioning to give the user a new PAC.	PAC provisioning is required. If automatic provisioning is <i>enabled</i> , phase zero occurs and a new PAC is sent. The end-user client initiates a new EAP-FAST authentication request using the new PAC. If automatic provisioning is <i>disabled</i> , phase zero does not occur and phase one fails. You must use manual provisioning to give the user a new PAC.

Replication and EAP-FAST

The Database Replication feature supports the replication of EAP-FAST settings, Authority ID, and master keys. Replication of EAP-FAST data occurs only if on the:

- Database Replication Setup page of the primary ACS, under Send, you have checked the EAP-FAST master keys and policies check box.
- Global Authentication Setup page of the primary ACS, you have enabled EAP-FAST and checked the EAP-FAST master server check box.
- Database Replication Setup page of the secondary ACS, under Receive, you have checked the EAP-FAST master keys and policies check box.
- Global Authentication Setup page of the secondary ACS, you have enabled EAP-FAST and unchecked the EAP-FAST master server check box.

EAP-FAST-related replication occurs for three events:

- **Generation of master keys**—A primary ACS sends newly generated active and backup master keys to secondary ACSs. This event occurs immediately after master key generation, provided that you configure the replication properly and it is not affected by replication scheduling on the Database Replication Setup page.

- **Manual replication**—All EAP-FAST components that can be replicated are replicated if you click **Replicate Now** on the Database Replication Setup page of the primary ACS. Some of the replicated components are configurable in the web interface. [Table 9-2](#) shows whether an EAP-FAST component is replicated or configurable.



Note EAP-FAST replication is not included in scheduled replication events.

- **Changes to EAP-FAST settings**—If, on a primary ACS, you change any EAP-FAST configurable components that are replicated, ACS begins EAP-FAST replication. Whether an EAP-FAST component is replicated or configurable is detailed in [Table 9-2](#).

The Database Replication log on the primary ACS records replication of master keys. Entries related to master key replication contain the text `MKEYReplicate`.

Table 9-2 *EAP-FAST Components and Replication*

EAP-FAST Component	Replicated?	Configurable?
EAP-FAST Enable	No	Yes, on the Global Authentication Setup page.
Master key TTL	Yes	Yes, on the Global Authentication Setup page.
Retired master key TTL	Yes	Yes, on the Global Authentication Setup page.
PAC TTL	Yes	Yes, on the Global Authentication Setup page.
Authority ID	Yes	No, generated by ACS.
Authority ID info	Yes	Yes, on the Global Authentication Setup page.
Client initial message	Yes	Yes, on the Global Authentication Setup page.
Master keys	Yes	No, generated by ACS when TTL settings dictate.
EAP-FAST master server	No	Yes, on the Global Authentication Setup page.
Actual EAP-FAST server status	No	No, determined by ACS.

The EAP-FAST master server setting has a significant effect on EAP-FAST authentication and replication:

- **Enabled**—When you check the EAP-FAST master server check box, the `Actual EAP-FAST server status` is `Master` and ACS ignores the EAP-FAST settings, Authority ID, and master keys it receives from a primary ACS during replication, preferring instead to use master keys that it generates, its unique Authority ID, and the EAP-FAST settings that are configured in its web interface.

Enabling the EAP-FAST master server setting requires providing a PAC from the primary ACS that is different than the PAC from the secondary ACS for the end-user client. Because the primary and secondary ACSs send different Authority IDs at the beginning of the EAP-FAST transaction, the end-user client must have a PAC for each Authority ID. A PAC that the primary ACS generates is not accepted by the secondary ACS in a replication scheme where the EAP-FAST master server setting is enabled on the secondary ACS.



Tip

In a replicated ACS environment, use the EAP-FAST master server feature in conjunction with disallowing automatic PAC provisioning to control EAP-FAST access to different segments of your network. Without automatic PAC provisioning, users must request PACs for each network segment.

- **Disabled**—When you do not check the EAP-FAST master server check box, ACS continues to operate as an EAP-FAST master server until the first time it receives replicated EAP-FAST components from the primary ACS. When *Actual EAP-FAST server status* displays the text *Slave*, ACS uses the EAP-FAST settings, Authority ID, and master keys that it receives from a primary ACS during replication; rather than using the master keys that it generates and its unique Authority ID.

**Note**

When you uncheck the EAP-FAST master server check box, the *Actual EAP-FAST server status* remains *Master* until ACS receives replicated EAP-FAST components and then the *Actual EAP-FAST server status* changes to *Slave*. Until *Actual EAP-FAST server status* changes to *Slave*, ACS acts as a master EAP-FAST server by using master keys that it generates, its unique Authority ID, and the EAP-FAST settings that are configured in its web interface.

Disabling the EAP-FAST master server setting eliminates the need for providing a different PAC from the primary and secondary ACSs. This elimination occurs because the primary and secondary ACSs send the end-user client the same Authority ID at the beginning of the EAP-FAST transaction; therefore, the end-user client uses the same PAC in its response to either ACS. Also, a PAC that one ACS generated for a user in a replication scheme where the EAP-FAST master server setting is disabled is accepted by all other ACSs in the same replication scheme.

For more information about replication, see [ACS Internal Database Replication, page 8-1](#).

Enabling EAP-FAST

This section explains the procedures to configure ACS to support EAP-FAST authentication.

**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 PAC provisioning places different limits on user database support.

To enable ACS to perform EAP-FAST authentication:

Step 1

Configure a user database that supports EAP-FAST authentication. To determine which user databases support EAP-FAST authentication, see [Authentication Protocol-Database Compatibility, page 1-8](#). For user database configuration, see [Chapter 12, “User Databases.”](#)

**Note**

User database support differs for EAP-FAST phase zero and phase two.

ACS supports use of the Unknown User Policy and group mapping with EAP-FAST, as well as password aging with Windows external user databases.

- Step 2** Determine master key and PAC TTL values. While changing keys and PACs more frequently could be considered more secure, it also increases the likelihood that PAC provisioning will be needed for machines left offline so long that the PACs on them are based on expired master keys.
- Also, if you reduce the TTL values with which you initially deploy EAP-FAST, you may force PAC provisioning to occur because users would be more likely to have PACs based on expired master keys.
- For information about how master key and PAC TTL values determine whether PAC provisioning or PAC refreshing is required, see [Master Key and PAC TTLs, page 9-17](#).
- 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 PAC Provisioning, page 9-14](#), and [Manual PAC Provisioning, page 9-15](#).



Note We recommend that you limit the use of automatic PAC provisioning to initial deployments of EAP-FAST, followed by using 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 on the Global Authentication Setup page. For detailed steps, see [Configuring Authentication Options, page 9-21](#).
- 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.

Stateless Session Server Resume

To provide better support for server performance, load balancing and peer roaming to different servers, EAP-FAST supports the stateless-server session resume by using the short-lived Authorization PACs. Once a peer establishes a TLS session and is authenticated, the EAP server can provision it with a Tunnel PAC. The tunnel PAC can be used to establish a TLS session much more quickly than a normal TLS handshake. With the normal TLS session resume, the EAP server must maintain the TLS session cache, as well as the peer's authentication and authorization result. This storage requirement often hinders the server's performance, as well as introduces difficulties with server load balancing and peer roaming to different servers. The use of Tunnel PAC eliminates the server's need to maintain a TLS session cache. The TLS session can be quickly established in a fast and secure way; however, the server still has to cache the peer's previous authentication and authorization state for a quick session resume.

You can further optimize by using the User Authorization PAC in combination with the Tunnel PAC. The server generated key protects User Authorization PACs which store previous authentication and authorization states on the peer. If the peer has the authorization PACs corresponding to the EAP server connected (by matching A-ID), and detects no state change affecting the peer, the peer can piggyback the opaque part of these PACs in the PAC-TLV with Client TLS Finished as TLS application data, which the TLS cipher suite that is negotiated protects. This method prevents attackers from snooping the authorization PACs without introducing an extra round trip. Once the EAP server receives and decrypts the authorization PAC, the EAP server can recreate its previous state information based on the peer's authentication and authorization result. If the state information in these PACs is still valid, based on a server side policy, it might bypass one or all of the inner EAP method authentications. In case inner methods are bypassed, the EAP Server sends the Result TLV only without the Crypto-binding TLV, and the peer responds with Result TLV with Success. The EAP-Server may start a full sequence of EAP authentication or a partial sequence if one or all of the PACs are not present or accepted.

ACS supports the following inner methods and TLV exchange support combinations:

- EAP-MS-CHAP Authentication + Posture Validation TLV exchange
- EAP-GTC Authentication + Posture Validation TLV exchange
- EAP-TLS Authentication + Posture Validation TLV exchange
- Posture Validation TLV exchange without authentication

**Note**

Re-use of an established session using an Authorization PAC will only work when ACS' dynamic users are NOT removed. When dynamic users are explicitly removed, re-use of established sessions is not possible, and ACS will try to perform full authentication in the usual manner.

Global Authentication Setup

You use the Global Authentication Setup page to enable or disable some of the authentication protocols that ACS supports. You can also configure other options for some of the protocols on the Global Authentication Setup page.

This section contains:

- [Configuring Authentication Options, page 9-21](#)
- [EAP-FAST Configuration Page, page 9-44](#)

**Caution**

Network Access Profile settings override the global authentication settings.

Configuring Authentication Options

Use this procedure to select and configure how ACS handles options for authentication. In particular, use this procedure to specify and configure the varieties of EAP that you allow, and to specify whether you allow MS-CHAP Version 1, MS-CHAP Version 2, or both.

For more information on the EAP-TLS Protocol, see [EAP-TLS Authentication, page 9-2](#). For more information on the PEAP protocol, see [PEAP Authentication, page 9-6](#). For more information on the PEAP protocol, see [EAP-FAST Authentication, page 9-9](#). For details about how various databases support various password protocols, see [Authentication Protocol-Database Compatibility, page 1-8](#).

You use the [EAP-FAST Configuration Page, page 9-44](#) to set up authentication configuration options.

**Note**

If users access your network by using a AAA client that is defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, you must enable one or more of the LEAP, EAP-TLS, or EAP-FAST protocols on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.

Before You Begin

For information about the options see the [EAP-FAST Configuration Page, page 9-44](#).

To configure authentication options:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Global Authentication Setup**.
The Global Authentications page appears.
- Step 3** Configure options, as applicable. For more information about the significance of the options, see [EAP-FAST Configuration Page, page 9-44](#).
- Step 4** If you want to immediately implement the settings that you have made, click **Submit + Apply**.
ACS restarts its services and implements the authentication configuration options that you selected.
- Step 5** If you want to save the settings that you have made but implement them later, click **Submit**.



Tip You can restart ACS services at any time by using the Service Control page in the System Configuration section.

ACS saves the authentication configuration options that you selected.

ACS Certificate Setup

This section contains:

- [Installing an ACS Server Certificate, page 9-22](#)
- [Adding a Certificate Authority Certificate, page 9-26](#)
- [Editing the Certificate Trust List, page 9-28](#)
- [Deleting a Certificate from the Certificate Trust List, page 9-29](#)
- [Managing Certificate Revocation Lists, page 9-29](#)
- [Generating a Certificate Signing Request, page 9-32](#)
- [Using Self-Signed Certificates, page 9-33](#)
- [Updating or Replacing an ACS Certificate, page 9-36](#)

Installing an ACS Server Certificate

Perform this procedure to install (that is, enroll) a server certificate for your ACS. You can perform certificate enrollment to support EAP-TLS and PEAP authentication, as well as to support HTTPS protocol for GUI access to ACS.

The three options for obtaining your server certificate are:

- Obtain a certificate from a CA.
- Use an existing certificate from local machine storage.
- Generate a self-signed certificate.

Before You Begin

You must have a server certificate for your ACS before you can install it. With ACS, certificate files must be in Base64-encoded X.509. If you do not already have a server certificate in storage, you can use the procedure in [Generating a Certificate Signing Request, page 9-32](#), or any other means, to obtain a certificate for installation.

If you are installing a server certificate that replaces an existing server certificate, the installation could affect the configuration of the CTL and CRL settings on your ACS. After you have installed a replacement certificate, you should determine whether you need to reconfigure any CTL or CRL settings.

If you want to use a server certificate from local machine storage, we recommend that you read *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks*, available on the ACS CD and at <http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml>. This white paper provides information about how to add a certificate to machine storage and how to configure a Microsoft certification authority server for use with ACS.

To install an existing certificate for use on ACS:

ACS for Windows

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

ACS displays the Install ACS Certificate page.



Note

The ACS certificate should be installed on the local server where the ACS is installed.

Step 4 You must specify whether ACS reads the certificate from a specified file or uses a certificate already on the local machine. To specify that ACS:

- Reads the certificate from a specified file, chose the **Read certificate from file** option, and then type the full directory path and filename of the certificate file in the Certificate file box.
- Uses a particular existing certificate from local machine certificate storage, chose the **Use certificate from storage** option, and then type the certificate CN (common name or subject name) in the Certificate CN box.



Tip

Type the certificate CN only; omit the **cn=** prefix.

- Uses a particular existing certificate from local machine certificate storage, chose the **Select Certificate from Storage** option, and then select a certificate from the drop down list.

Step 5 If you generated the request by using ACS, in the Private key file box, type the full directory path and name of the file that contains the private key.



Note

If the certificate was installed in storage with the private key, you do not have the private key file and do not need to type it.



Tip This is the private key that is associated with the server certificate.

Step 6 In the Private key password box, type the private key password.



Tip If you used ACS to generate the certificate signing request, this is the same value that you entered as the *Private key password* on the Generate Certificate Signing Request page. If the private key file is unencrypted, leave this box empty.

Step 7 Click **Submit**.

To show that the certificate setup is complete, ACS displays the Installed Certificate Information table, which contains:

- Issued to: *certificate subject*
- Issued by: *CA common name*
- Valid from:
- Valid to:
- Validity:

ACS SE

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

ACS displays the Install ACS Certificate page.

Step 4 To install a new certificate, click the **Read certificate from file** option and then click the **Download certificate file** link.

The Download Certificate File page appears.

Step 5 To download the certificate file to ACS, enter the following information into the Download File table:

- a. In the **FTP Server** box, type the IP address or hostname of the FTP server that contains the certificate file that you want to download.



Tip If you specify the hostname, DNS must be correctly working on your network.

- b. In the **Login** box, type a valid username that ACS can use to access the FTP server.
- c. In the **Password** box, type the password for the username that you specified in the Login box.
- d. In the **Remote FTP Directory** box, type the relative path from the FTP server root directory to the directory containing the certificate file that you want ACS to download from the FTP server.
- e. In the **Remote FTP File Name** box, type the name of the certificate file that you want ACS to download from the FTP server.
- f. Click **Submit**.

The system downloads the certificate file and displays the filename in the Certificate file box on the Install ACS Certificate page.



Tip If the file transfer encounters errors, the pane on the right displays the errors.

Step 6 If you generated the request by using ACS, click the **Download private key file** link.

The Download Private Key File page appears.

Step 7 To download the private key file to ACS, enter the following information into the Download File table:

- a. In the **FTP Server** box, type the IP address or hostname of the FTP server that contains the private key file that you want to download.



Tip If you specify the hostname, DNS must be correctly working on your network.

- b. In the **Login** box, type a valid username that ACS can use to access the FTP server.
- c. In the **Password** box, type the password for the username that you specified in the Login box.
- d. In the **Remote FTP Directory** box, type the relative path from the FTP server root directory to the directory containing the private key file that you want ACS to download from the FTP server.

Step 8 You must specify whether ACS reads the certificate from a specified file or uses a certificate already on the local machine. To specify that ACS:

- Reads the certificate from a specified file, select the **Read certificate from file** option, and then type the full directory path and filename of the certificate file in the Certificate file box.
- Uses a particular existing certificate from local machine certificate storage, select the **Use certificate from storage** option, and then type the certificate CN (common name or subject name) in the Certificate CN box.



Tip Type the certificate CN only; omit the **cn=** prefix.

Step 9 If you generated the request by using ACS, in the Private key file box, type the full directory path and name of the file that contains the private key.



Note If the certificate was installed in storage with the private key, you do not have the private key file and do not need to type it.



Tip This is the private key that is associated with the server certificate.

Step 10 In the Private key password box, type the private key password.

Step 11 Click **Submit**.

The system downloads the private key file and displays the filename in Private key file box on the Install ACS Certificate page.



Tip If the file transfer encounters errors, the pane on the right displays the errors.

Step 12 In the **Private key password** box, type the private key password.



Tip

If you used ACS to generate the certificate signing request, this is the same value that you entered as the *Private key password* on the Generate Certificate Signing Request page. If the private key file is unencrypted, leave this box empty.

Step 13 Click **Submit**.

To show that the certificate setup is complete, ACS displays the Installed Certificate Information table, which contains:

- Issued to: *certificate subject*
- Issued by: *CA common name*
- Valid from:
- Valid to:
- Validity:

Adding a Certificate Authority Certificate

Use this procedure to add new CA certificates to ACS local certificate storage.



Note

If the clients and ACS are getting their certificates from the same CA, you do not need to perform this procedure because ACS automatically trusts the CA that issued its certificate.

When a user certificate is from an unknown CA (that is, one that is different from the CA that certifies the ACS), you must specifically configure ACS to trust that CA or authentication fails. Until you perform this procedure to explicitly extend trust by adding another CA, ACS only recognizes certificates from the CA that issued its own certificate.

Configuring ACS to trust a specific CA is a two-step process that comprises this procedure of adding a CA's certificate and the procedure in [Editing the Certificate Trust List, page 9-28](#), in which you specify that the particular CA is to be trusted. (ACS comes configured with a list of popular CAs, none of which is enabled until you explicitly specify trustworthiness.)

To add a certificate authority certificate to your local storage:

ACS for Windows

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **ACS Certification Authority Setup**.

ACS displays the CA Operations table on the Certification Authorities Setup page.

Step 4 In the **CA certificate file** box, type the full path and filename for the certificate to use.

Step 5 Click **Submit**.

The new CA certificate is added to local certificate storage. And, if it is not already there, the name of the CA that issued the certificate is placed on the CTL.

**Tip**

To use this new CA certificate to authenticate users, you must edit the certificate trust list to specify that this CA is trusted. For more information, see [Editing the Certificate Trust List, page 9-28](#).

ACS SE

**Note**

You need to download the CA certificate from an FTP server.

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **ACS Certification Authority Setup**.

ACS displays the CA Operations table on the Certification Authorities Setup page.

Step 4 Download the certificate from an FTP server:

- a. Enter the FTP IP address.
- b. Enter the Path where the certificate is located.
- c. Log in to the server and enter the Password.
- d. Download the certificate file from the location in your directory.

Step 5 In the **CA certificate file** box, type the full path and filename for the certificate to use.

Step 6 Click **Submit**.

The system downloads the private key file and displays the filename in the Private key file box on the Install ACS Certificate page.

**Tip**

If the file transfer encounters errors, the errors appear in the pane on the right.

Step 7 In the **Private key password** box, type the private key password.

Step 8 Click **Submit**.

The new CA certificate is added to local certificate storage. And, if it is not already there, the name of the CA that issued the certificate is placed on the CTL.

**Tip**

To use this new CA certificate to authenticate users, you must edit the certificate trust list to specify that this CA is trusted. For more information, see [Editing the Certificate Trust List, page 9-28](#).

Editing the Certificate Trust List

ACS uses the CTL to verify the client certificates. For ACS to trust a CA, its certificate must be installed and the ACS administrator must explicitly configure the CA as trusted by editing the CTL. If the ACS server certificate is replaced, the CTL is erased; you must then configure the CTL explicitly each time you install or replace a ACS server certificate.



Note

The single exception to the requirement that you must explicitly specify a CA as trustworthy occurs when the clients and ACS are getting their certificates from the same CA. You do not need to add this CA to the CTL because ACS automatically trusts the CA that issued its certificate.

How you edit your CTL determines the type of trust model that you have. Many use a restricted trust model wherein very few privately controlled CAs are trusted. This model provides the highest level of security; but restricts adaptability and scalability. The alternative, an open trust model, allows for more CAs or public CAs. This open trust model trades increased security for greater adaptability and scalability.

We recommend that you fully understand the implications of your trust model before editing the CTL in ACS.

Use this procedure to configure CAs on your CTL as trusted or not trusted. Before you can configure a CA as trusted on the CTL, you must have added the CA to the local certificate storage; for more information, see [Adding a Certificate Authority Certificate, page 9-26](#). If a user's certificate is from a CA that you have not specifically configured ACS to trust, authentication fails.

To edit the CTL:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Edit Certificate Trust List**.

The Edit the Certificate Trust List (CTL) table appears.



Warning

Adding a public CA, which you do not control, to your CTL may reduce your system security.

Step 4 To configure a CA on your CTL as trusted, check the corresponding check box.



Tip

You can check, or uncheck, as many CAs as you want. Unchecking a CA check box configures the CA as not trusted.

Step 5 Click **Submit**.

ACS configures the specified CA (or CAs) as trusted or not trusted in accordance with checking or unchecking check boxes. The selected Certificate Trust Lists automatically appear on the CRL Issuers page.

Deleting a Certificate from the Certificate Trust List

To delete a certificate from the Certificate Trust List:

-
- | | |
|--------|--|
| Step 1 | In the navigation bar, click System Configuration . |
| Step 2 | Click ACS Certificate Setup . |
| Step 3 | Click Delete Certificate from Certificate Trust List .
ACS displays the list of Certificate Trust lists that can be deleted. |
| Step 4 | Click Submit .
The selected CA certificate is deleted from the local certificate storage. |
-

Managing Certificate Revocation Lists

Certificate revocation lists (CRLs) are the means by which ACS determines that the certificates employed by users who seek authentication are still valid, according to the CA that issued them.

This section contains:

- [About Certificate Revocation Lists, page 9-29](#)
- [Certificate Revocation List Configuration Options, page 9-30](#)
- [Editing a Certificate Revocation List Issuer, page 9-31](#)

About Certificate Revocation Lists

When a digital certificate is issued, you generally expect it to remain valid throughout its predetermined period of validity. However, various circumstances may call for invalidating the certificate earlier than expected. Such circumstances might include compromise or suspected compromise of the corresponding private key, or a change in the CAs issuance program. Under such circumstances, a CRL provides the mechanism by which the CA revokes the legitimacy of a certificate and calls for its managed replacement.

ACS performs certificate revocation by using the X.509 CRL profile. A CRL is a signed and time-stamped with a data structure that a CA (or CRL issuer) issues and which is freely available in a public repository (for example, in an LDAP server). Details on the operation of the X.509 CRL profile are contained in RFC3280.

CRL functionality in ACS includes:

- **Trusted publishers and repositories configuration**—In the ACS web interface, you can view and configure CRL issuers, and their CRL Distribution Points (CDPs) and periods.
- **Retrieval of CRLs from a CDP**—Using a transport protocol (LDAP or HTTP), ACS is configured to periodically retrieve CRLs for each CA that you configure. These CRLs are stored for use during EAP-TLS authentication. Note that there is no timestamp mechanism; instead ACS waits for a specified period of time and then automatically downloads the CRL. If the new CRL differs from the existing CRL, the new version is saved and added to the local cache. CRL retrievals appear in the log for the **CSAuth** service only when you have configured the level of detail in service logs to **full**. The status, date, and time of the last retrieval appears on the Certificate Revocation List Issuer edit page of the ACS web interface.



Note Automatic CRL retrieval scheduling only functions if EAP-TLS is enabled.

- **Verification of certificate status**—During EAP-TLS authentication, ACS checks the certificate that the user against the corresponding CRL that the CA of the user's certificate issues. If, according to the CRL that ACS currently stores, the certificate has been revoked and authentication fails.

CRL issuers can only be added in association with trusted CAs (that is, CAs on the CTL). If you install a new server certificate for ACS, your CTL is cleared of all trust relationships. While you must reestablish CAs on the CTL, the associated CRLs that you previously configured remain in place and do not have to be reconfigured.

Certificate Revocation List Configuration Options

The Certificate Revocation List Issuers edit page contains the following configuration options:

- **Name**—The name given by the CA Issuer.
- **Description**—A description that you give this CRL issuer.
- **CRL Distribution URL**—The URL that ACS should use to retrieve the CRL. If a CA certificate contains a `CRL distribution points` parameter, this field will be populated automatically. Otherwise, ensure that you specify a URL for the CRL corresponding to the CA that you selected from the Issuer's Certificate list. You can specify a URL that uses HTTP, LDAP, or FTP. Alternatively, you can specify the URL for the file itself; however, this is only necessary when the repository URL lists multiple files.

An example of an HTTP URL is:

http://crl.verisign.com/pca1.1.1.crl.

An example of an LDAP URL is:

ldap://10.36.193.5:388/CN=development-CA,CN=acs-westcoast2,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cisco,DC=com



Note

In LDAP, the default placement for the CRL is under `objectclass=crlDistributionPoint`. ACS adds the object class information to the URL. If the CRL is located elsewhere, you must add the object class to the URL. For example, if the CRL is situated under `objectclass=CertificateRevocationList` the URL should be: *ldap://10.36.193.5:388/CN=development-CA,CN=acs-westcoast2,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=cisco,DC=com?(objectclass=CertificateRevocationList)*.



Tip

The URL must specify the CRL itself when the repository contains multiple files.

- **Retrieve CRL**—Initially ACS attempts to download a CRL from the CA. The CRL folder and file are created in the installation directory after a CRL is successfully downloaded. The CRL issuer is not modifiable. The Next Update field in the CRL file contains a value for the Next Update. Select the method that ACS should use for retrieving a CRL:
 - **Automatically**—Uses the value in the Next Update field in the CRL file to retrieve a new CRL from the CA. If unsuccessful, ACS tried to retrieve the CRL every 10 minutes after the first failure until it succeeds.

- **Every**—Determines the frequency between retrieval attempts. Enter the amount in units of time.

**Note**

For the automatic CRL retrieval function to operate, ensure that you have enabled EAP-TLS.

**Note**

In both modes, if retrieval fails, a reattempt occurs every 10 minutes.

- **Last Retrieve Date**—This entry lists the status, and the date and time of the last CRL retrieval or retrieval attempt.
- **Options**—You check the **Ignore Expiration Date** check box to check a certificate against an outdated CRL.

When the **Ignore Expiration Date** is unchecked, ACS examines the expiration date of the CRL in the Next Update field in the CRL file and continues to use this CRL; even though it has expired. If the expiry date passed, the CRL is not valid and all EAP-TLS authentications will be rejected.

When the **Ignore Expiration Date** is checked, ACS continues to use the expired CRL and permits or rejects EAP-TLS authentications according to the contents of the CRL.

- **CRL is in Use**—When checked, the CRL is active and is used in the EAP-TLS authentication process.
- **Submit**—Click **Submit** to download and verify the CRL with the public key of the issuer. Inconsistencies generate CRL Issuer Configuration errors.

When submission succeeds, you must restart ACS to apply the new configuration.

Editing a Certificate Revocation List Issuer

To edit a certificate revocation list issuer:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Certificate Revocation Lists**.

The CRL Issuers page appears.

Step 4 Click the name of the CRL issuer that you want to edit.

The system displays the CRL Issuer Edit page for the CRL that you chose.

Step 5 Edit the information and settings that you want to change.

Step 6 Click **Submit**.

The corresponding CRL is changed in ACS to that of the edited issuer (or is scheduled to be changed at the time that you specify in the Retrieve CRL field).

**Tip**

You can refer to the **Last Retrieve date** box to see the status, date, and time of the last CRL retrieval attempt.

Generating a Certificate Signing Request

You can use ACS to generate a certificate signing request (CSR). After you generate a CSR, you can submit it to a CA to obtain your certificate. You perform this procedure to generate the CSR for future use with a certificate enrollment tool.



Note

If you already have a server certificate, you do not need to use this portion of the ACS Certificate Setup page.

To generate a certificate signing request:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Select **ACS Certificate Setup**, then **Generate Certificate Signing Request**.
ACS displays the Generate Certificate Signing Request page.
- Step 3** In the Certificate subject box, type values for the certificate fields that the CA to which to submit the CSR. Filling in the CN field is mandatory. The format is:
field=value, field=value, . . .

where *field* is the field name, such as *CN*, and *value* is the applicable value for the field, such as *acs01primary*. You can type a maximum of 256 characters in the Certificate subject box. Separate multiple values with commas (,); for example:

CN=acs01primary, O=WestCoast, C=US, S=California

Table 9-3 defines the valid fields that you can include in the Certificate subject box.

Table 9-3 Certificate Subject Fields

Field	Field Name	Min. Length	Max. Length	Required?
CN	commonName	1	64	Yes
OU	organizationalUnitName	—	—	No
O	organizationName	—	—	No
S	stateOrProvinceName	—	—	No
C	countryName	2	2	No
E	emailAddress	0	40	No
L	localityName	—	—	No

- Step 4** In the **Private key file** box:
 - ACS for Windows—Type the full directory path and name of the file in which the private key is saved; for example, *c:\privateKeyFile.pem*.
 - ACS SE—Type only the name of the file in which the private key is saved; for example, *privateKeyFile.pem*.
- Step 5** In the **Private key password** box, type the private key password (that you have invented).
- Step 6** In the **Retype private key password** box, retype the private key password.
- Step 7** From the **Key length** list, select the length of the key to use.

**Tip**

The choices for Key length are 512 or 1024 bits. The default and more secure choice is 1024 bits.

- Step 8** From the **Digest to sign with** list, select the digest (or hashing algorithm). The choices are MD2, MD5, SHA, and SHA1. The default is SHA1.
- Step 9** Click **Submit**.
- ACS displays a CSR on the right side of the browser.
- Step 10** Submit the CSR to the CA of your choice.
- After you receive the certificate from the CA, you can perform the steps in [Installing an ACS Server Certificate, page 9-22](#).

Using Self-Signed Certificates

You can use ACS to generate a self-signed digital certificate to use for the PEAP authentication protocol or HTTPS support of ACS administration. This capability supports TLS/SSL protocols and technologies without the requirement of interacting with a CA.

This section contains:

- [About Self-Signed Certificates, page 9-33](#)
- [Self-Signed Certificate Configuration Options, page 9-34](#)
- [Generating a Self-Signed Certificate, page 9-35](#)

About Self-Signed Certificates

ACS supports TLS/SSL-related protocols, including PEAP, EAP-FAST, and HTTPS, that require the use of digital certificates. Employing self-signed certificates is a way for administrators to meet this requirement without having to interact with a CA to obtain and install the certificate for the ACS. The administrator uses the self-signed certificate feature in ACS to generate the self-signed digital certificate, and use it for the PEAP and EAP-FAST authentication protocols or for HTTPS support in web administration service.

Other than the lack of interaction with a CA to obtain the certificate, installing a self-signed certificate requires exactly the same user actions as any other digital certificate. Although ACS does not support the replication of self-signed certificates, you can export a certificate for use on more than one ACS.

ACS for Windows

To enable self-signed certificate generation, you copy the certificate file (.cer format) and the corresponding private key file (.pvk format) to another ACS where you can then install the certificate in the standard manner. For information on installing certificates, see [Installing an ACS Server Certificate, page 9-22](#).

ACS SE

To enable self-signed certificate generation, you must specify the FTP server to which the certificate file (.cer format) and the corresponding private key file (.pvk format) are transferred. Another ACS can then obtain the certificate from the FTP server and install it in the standard manner. For information on installing certificates, see [Installing an ACS Server Certificate, page 9-22](#).

Both Platforms

To ensure that a self-signed certificate works with the client, refer to your client documentation. You may find that you must import the self-signed server certificate as a CA certificate on your particular client.

Self-Signed Certificate Configuration Options

The Generate Self-Signed Certificate edit page contains the following mandatory configuration fields:

- **Certificate subject**—The subject for the certificate, prefixed with **cn=**. We recommend using the ACS name. For example, **cn=ACS11**. The Certificate subject field here can contain a number of content entries as comma-separated items; these include:
 - **CN**—common name (the mandatory entry)
 - **OU**—organizational unit name
 - **O**—organization name
 - **S**—state or province
 - **E**—email address
 - **L**—locality name

For example, the Certificate subject field might appear as:

`cn=ACS 11, O=Acme Enterprises, E=admin@acme.com`

- **Certificate file**—The certificate file that you want to generate. When you submit this page, ACS creates the certificate file by using the location and filename that you specify.
 - ACS for Windows—Type the full directory path and name of the file; for example, `c:\acs_server_cert\acs_server_cert.cer`.
 - ACS SE—Type only the name of the file; for example, `acs_server_cert.cer`.
- **Private key file**—The private key file you want to generate. When you submit this page, ACS creates the private key file by using the location and filename that you specify.
 - ACS for Windows—Type the full directory path and name of the file; for example, `c:\acs_server_cert\acs_server_cert.pvk`.
 - ACS SE—Type only the name of the file; for example, `acs_server_cert.pvk`.
- **Private key password**—A private key password for the certificate. Minimum length for the private key password is 4 characters, and the maximum length is 64 characters.
- **Retype private key password**—The private key password typed again, to ensure accuracy.
- **Key length**—Select the key length from the list. The choices include 512 bits, 1024 bits, and 2048 bits.
- **Digest to sign with**—Select the hash digest to use to encrypt the key from the list. The choices include SHA1, SHA, MD2, and MD5.
- **Install generated certificate**—Select this check box if you want ACS to install the self-signed certificate that it generates when you click **Submit**. If you employ this option, you must restart ACS services after you submit the page for the new settings to take effect. If you do not select this option, the certificate file and private key file are generated and saved; but are not installed into local machine storage.

The following options apply only to the ACS SE:

The Generate Self-Signed Certificate edit page also contains mandatory configuration fields that you use to specify the FTP server to which the certificate file and the corresponding private key file are transferred:

- **FTP Server**—The IP address or hostname of the FTP server where the certificate file and the corresponding private key file are to be transferred. If you specify a hostname, DNS must be enabled on your network and must be correctly configured on the serial console.
- **Login**—A valid username that enables ACS to access the FTP server.



Tip

The Login box accepts domain-qualified usernames in the format *DOMAIN\username*, which may be required if you are using a Microsoft FTP server.

- **Password**—The password for the username provided in the Login box.
- **Remote Directory**—The directory to which you want to transfer the files. The directory must be specified relative to the FTP root directory.

Generating a Self-Signed Certificate

All fields on the Generate Self-Signed Certificate page are mandatory. For information on the fields' contents, see [Self-Signed Certificate Configuration Options, page 9-34](#).

To generate a self-signed certificate:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Certificate Setup**.
- Step 3** Click **Generate Self-Signed Certificate**.
The Generate Self-Signed Certificate edit page appears.
- Step 4** In the **Certificate subject** box, type the certificate subject in the form **cn=XXXX**. You can enter additional information here, for more information see [Self-Signed Certificate Configuration Options, page 9-34](#).
- Step 5** In the **Certificate file** box, type the full path and file name for the certificate file.
- Step 6** In the **Private key file** box, type the full path and file name for the private key file.
- Step 7** In the **Private key password** box, type the private key password.
- Step 8** In the **Retype private key password** box, retype the private key password.
- Step 9** In the **Key length** box, select the key length.
- Step 10** In the **Digest to sign with** box, select the hash digest to be used to encrypt the key.
- Step 11** To install the self-signed certificate when you submit the page, select the **Install generated certificate** option.



Note

If you select the Install generated certificate option, you must restart ACS services after submitting this form for the new settings to take effect.

**Tip**

If you do not select the Install generated certificate option, the certificate file and private key file are generated and saved when you click Submit in the next step; but are not installed in local machine storage.

- Step 12** ACS SE: In the **FTP Server** box, type the IP address or hostname of the FTP server where the certificate file and the corresponding private key file are to be transferred.

**Tip**

If you specify the hostname, DNS must be correctly working on your network.

- Step 13** ACS SE: In the **Login** box, type a valid username that ACS can use to access the FTP server.
- Step 14** ACS SE: In the **Password** box, type the password for the username that you specified in the Login box.
- Step 15** ACS SE: In the **Remote FTP Directory** box, type the relative path from the FTP server root directory to the directory to which you want ACS to transfer the certificate file and the corresponding private key file.
- Step 16** Click **Submit**.

The specified certificate and private key files are generated and stored. If you selected the **Install generated certificate** option, the certificate becomes operational, only after you restart ACS services.

Updating or Replacing an ACS Certificate

Use this procedure to update or replace an existing ACS certificate that is out of date or out of order.

**Caution**

This procedure eliminates your existing ACS certificate and erases your CTL configuration.

To install a new ACS certificate:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Certificate Setup**.
- ACS displays the Installed Certificate Information table on the ACS Certificate Setup page.

**Note**

If your ACS has not already been enrolled with a certificate, you do not see the Installed Certificate Information table. Rather, you see the Install new certificate table. If this is the case, proceed to Step 5.

- Step 3** Click **Install New Certificate**.
- A confirmation dialog box appears.
- Step 4** To confirm that you intend to enroll a new certificate, click **OK**.
- The existing ACS certificate is removed and your CTL configuration is erased.

- Step 5** You can now install the replacement certificate in the same manner as an original certificate. For detailed steps, see [Installing an ACS Server Certificate, page 9-22](#).

EAP-FAST PAC Files Generation (ACS SE)

You can use the EAP-FAST PAC Files Generation page to create PAC files for manual PAC provisioning. For more information about PACs, see [EAP-FAST Authentication, page 9-9](#).

This section contains:

- [PAC File Generation Options, page 9-37](#)
- [Generating PAC Files, page 9-39](#)

PAC File Generation Options

When generating PAC files, you can use:

- **Specific user**—ACS generates a PAC file for the username typed in the User Name box. For example, if you checked this option and typed **seaniemop** in the User Name box, ACS generates a single PAC file, named *seaniemop.pac*.



Tip

You can also specify a domain-qualified username, using the format *DOMAIN\username*. For example, if you specify *ENGINEERING\augustin*, ACS generates a PAC filename *ENGINEERING_augustin.pac*.

- **Users from specific ACS group**—ACS generates a PAC file for each user in the user group specified by the ACS Group list. ACS has 500 groups, numbered from 0 (zero) to 499. For example, assume that Group 7 has 43 users. If you selected this option and chose **Group 7** from the ACS Group list, ACS would generate 43 PAC files, one for each user who is a member of Group 7. Each PAC file is named in the following format:

where *username.pac* is the name of the particular user.



Note

Generating PAC files for users in a specific group restarts the **CSAuth** service. No users are authenticated while **CSAuth** is unavailable.



Tip

To generate PAC files for more than one group of users, generate PAC files for each group separately. For example, to generate PAC files for users in Groups 7 through 10, generate PAC files four times, once each for Groups 7, 8, 9, and 10.

- **All users in ACS internal DB**—ACS generates a PAC file for each user in the ACS internal database. For example, if you have 3278 users in the ACS internal database and check this option, ACS would generate 3278 PAC files, one for each user. Each PAC file is named in the following format:

username.pac

**Note**

Generating PAC files for all users in the ACS internal database restarts the **CSAuth** service. No users are authenticated while **CSAuth** is unavailable.

- **Users from list**—ACS generates a PAC file for each username in the file that is retrieved from the FTP server that you specify.

Lists of usernames should contain one username per line with no additional spaces or other characters.

For example, if a list retrieved from an FTP server contains the following usernames:

```
seaniemop
jwiedman
echamberlain
```

ACS generates three PAC files: *seaniemop.pac*, *jwiedman.pac*, and *echamberlain.pac*.

**Tip**

You can also specify domain-qualified usernames, using the format *DOMAIN\username*. For example, if you specify **ENIGINEERING\augustin**, ACS generates a PAC file name *ENGINEERING_augustin.pac*.

The options for retrieving a username list are:

- **FTP Server**—The IP address or hostname of the FTP server where the file specified in the User list file box is located. If you specify a hostname, DNS must be enabled on your network and must be configured correctly on the ACS SE console. For more information about IP configuration of ACS, see *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.
- **Login**—A valid username to enable ACS to access the FTP server.

**Tip**

The Login box accepts domain-qualified usernames in the format *DOMAIN\username*, which may be required if you are using a Microsoft FTP server.

- **Password**—The password for the username in the Login box.
- **Remote Directory**—The directory containing the file of usernames in the Users list file box. The directory must be specified relative to the FTP root directory. For example, if the username file is in a directory named *paclist*, which is a subdirectory of the FTP root directory, you should type **paclist** in the Remote Directory box.

**Tip**

To specify the FTP root directory, enter a single period or “dot”(.).

- **Users list file**—The filename of the username list. For example, if the name of the username file is *eapfastusers.txt*, type **eapfastusers.txt** in the User list file box.
- **Encrypt PAC file(s) with**—Each PAC file is always encrypted using a password: the default password known to ACS and the end-user clients or a password that you specify. Encrypting PAC files helps prevent use of stolen PAC files for access to your network by unauthorized persons. Although the default password is a strong password, all ACSs and EAP-FAST end-user clients use it.
- ACSs and all EAP-FAST end-user clients:



Note We recommend that you use a password that you devise rather than the default password.

- **Default password**—ACS uses the default password to protect the PAC files that it generates.



Note We recommend that you use a password you devise rather than the default password.

- **This password**—ACS uses the password specified, rather than the default password, to protect the PAC files it generates. The password that you specify is required when the PACs that ACS protects are loaded into an EAP-FAST end-user client.

PAC passwords are alphanumeric, between 4 and 128 characters long, and case sensitive. While ACS does not enforce strong password rules, we recommend that you use a strong password, that is, your PAC password should:

- Be very long.
- Contain uppercase and lowercase letters.
- Contain numbers in addition to letters.
- Contain no common words or names.

Generating PAC Files

Each time you instruct ACS to generate PAC files, ACS produces a single cabinet file named *PACFiles.cab* that you download to a location available to the browser that you use to access the HTML interface. Use the file compression utility of your choice to extract the *.pac* files from the *PACFiles.cab* file. For example, [WinZip](#) can extract files from cabinet files.

Before You Begin

With ACS you can generate PAC files only if EAP-FAST is enabled. For information about enabling EAP-FAST, see [Enabling EAP-FAST, page 9-19](#).

Determine which users for which you want to generate PAC files. If you want to specify the users in a text file, create the text file and place it in a directory under the FTP root directory on an FTP server that is accessible from the ACS SE. For information about using a username list, see [PAC File Generation Options, page 9-37](#).

For information about the options on the EAP-FAST PAC Generation page, see [PAC File Generation Options, page 9-37](#).

To generate PAC files:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **EAP-FAST PAC Files Generation**.
ACS displays the EAP-FAST PAC Files Generation page.
 - Step 3** Use one of the four options to specify for which users ACS should generate PAC files. For more information about the significance of the options, see [PAC File Generation Options, page 9-37](#).



Note If you choose to generate PAC files for all users in the ACS internal database in a specific group, the **CSAuth** service restarts. No user authentication occurs while **CSAuth** is unavailable.

Step 4 Click **Submit**.

ACS begins generating PAC files for the user or users specified. If you use the Users from list option, ACS first retrieves the list from the FTP server specified.

On the EAP-FAST PAC Files Generation page, ACS displays a current PAC CAB file generation status message.

Step 5 If the Current PAC CAB file generation status display is: CAB file generation is in progress

click Refresh occasionally until the Current PAC CAB file generation status display is: CAB file is ready. Press Download to retrieve the file.

Depending on how many users you specified, ACS requires anywhere from a few seconds to a few minutes to generate PAC files.

Step 6 When the Current PAC CAB file generation status display is: CAB file is ready, Click Download to retrieve the file click download.**Note**

The file download options that your web browser provides may differ; however, the fundamental process should be similar to these steps.

The File Download dialog box appears.

Step 7 On the File Download dialog box, click **Save**.

The Save As dialog box appears.

Step 8 Use the Save As dialog box to specify where and with what filename you want to save the *PACFiles.cab* file. Then click **Save**.

ACS sends the *PACFiles.cab* file to your web browser, which saves the file where you specified. When the download is complete, a Download Complete dialog box appears.

Step 9 Note the location of the *PACFiles.cab* file, and then click **Close**.**Step 10** You can use the file compression utility of your choice to extract the PAC files from the *PACFiles.cab* file.

Advanced System Configuration Pages Reference

This section describes the following topics:

- [Global Authentication Setup Page, page 9-41](#)
- [EAP-FAST Configuration Page, page 9-44](#)

Global Authentication Setup Page

Use this page to specify settings for various authentication protocols.

To open this page choose **System configuration > Global Authentication Setup**.

Field	Description
EAP Configuration	PEAP is a certificate-based authentication protocol. Authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.
PEAP	Select the PEAP types. In most cases, all three boxes that specify EAP options should be checked. When none are selected, PEAP will not be allowed for authentication.
Allow EAP-MSCHAPv2	Check this to specify that ACS attempts EAP-MS-CHAPv2 authentication with PEAP clients. Note If you check this box, ACS negotiates the EAP type with the end-user PEAP client.
Allow EAP-GTC	Check this to specify that ACS attempts EAP-GTC authentication with PEAP clients.
Allow Posture Validation	Check this to enable use of PEAP for posture validation of Network Admission Control (NAC) clients.

Field	Description
Allow EAP-TLS	<p>Check this to specify that ACS attempts EAP-TLS authentication with PEAP clients. If you check this check box, select one or more EAP-TLS comparison methods.</p> <ul style="list-style-type: none"> • Certificate SAN comparison—If you want ACS to verify user identity by comparing the name in the Subject Alternative Name field of the end-user certificate to the username in the applicable user database, check this check box. • Certificate CN comparison—If you want ACS to verify user identity by comparing the name in the Common Name field of the end-user certificate to the username in the applicable user database, check this check box. • Certificate Binary comparison—If you want ACS to verify user identity by doing a binary comparison of the end-user certificate to the user certificate stored in Active Directory, check this check box. <p>If you choose more than one comparison type, ACS performs the comparisons in the order listed. If one comparison type fails, ACS attempts the next enabled comparison type. Comparison stops after the first successful comparison.</p> <p>Specify an EAP_TLS Session Timeout value, a Cisco client initial message, a PEAP session timeout, and indicate whether to enable Fast Reconnect.</p> <ul style="list-style-type: none"> • EAP-TLS session timeout (minutes)—Enter a value in minutes for that defines the maximum time for the EAP-TLS session. <p>ACS supports an EAP-TLS session resume feature that caches the TLS session that was created during a new EAP-TLS authentication. When an EAP-TLS client reconnects, the cached TLS session is used to restore the session without performing a certificate comparison, which improves EAP-TLS performance. ACS deletes cached TLS sessions when they time out. If ACS or the end-user client is restarted, certificate comparison is required; even if the session timeout interval has not ended. To disable the session resume feature, set the timeout value to zero (0).</p> <ul style="list-style-type: none"> • Cisco client initial message—The message that you want to appear during PEAP authentication. The message that the PEAP client initially displays is the first challenge that a user of a Cisco Aeronaut PEAP client sees when attempting authentication. It should direct the user what to do next; for example, <i>Enter your message</i>. The message is limited to 40 characters. • PEAP session timeout (minutes)—The maximum PEAP session length to allow users, in minutes. A session timeout value that is greater than zero (0) enables the PEAP session resume feature, which caches the TLS session that was created in phase one of PEAP authentication. When a PEAP client reconnects, ACS uses the cached TLS session to restore the session, which improves PEAP performance. ACS deletes cached TLS sessions when they time out. The default timeout value is 120 minutes. To disable the session resume feature, set the timeout value to zero (0). • Enable Fast Reconnect—This option is related to MS CHAP only, and does not apply to EAP-GTC. If you want ACS to resume sessions for MS PEAP clients without performing phase two of MS PEAP authentication, select this check box. Clearing this check box causes ACS to perform phase two of MS PEAP authentication, even when the PEAP session has not timed out. <p>Fast reconnect can occur only when ACS allows the session to resume because the session has not timed out. If you disable the PEAP session resume feature by entering zero (0) in the PEAP session timeout (minutes) box, checking the Enable Fast Reconnect check box has no effect on PEAP authentication.</p>

Field	Description
EAP-FAST	<p>EAP-FAST Configuration—Select to open the EAP-FAST Configuration Page, page 9-44.</p> <p>Note If you are using ACS to implement NAC, enable each option and then click Submit. When the page reappears, select EAP-FAST Configuration to open the EAP-FAST Settings page.</p>
EAP-TLS Configuration	<p>Check this box to use the EAP-TLS Authentication protocol and configure 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.</p> <p>Note EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps on the ACS Certificate Setup page. See Installing an ACS Server Certificate, page 9-22 for more information.</p> <p>If you check the check box to enable EAP-TLS, select one or more EAP-TLS comparison methods. These methods include:</p> <ul style="list-style-type: none"> – Certificate SAN comparison—If you want ACS to verify user identity by comparing the name in the Subject Alternative Name field of the end-user certificate to the username in the applicable user database, check this check box. – Certificate CN comparison—If you want ACS to verify user identity by comparing the name in the Common Name field of the end-user certificate to the username in the applicable user database, check this check box. – Certificate Binary comparison—If you want ACS to verify user identity by doing a binary comparison of the end-user certificate to the user certificate stored in Active Directory, check this check box. <p>If you choose more than one comparison type, ACS performs the comparisons in the order listed. If one comparison type fails, ACS attempts the next enabled comparison type. Comparison stops after the first successful comparison.</p> <p>Specify an EAP_TLS Session Timeout value, a Cisco client initial message, a PEAP session timeout, and indicate whether to enable Fast Reconnect.</p> <ul style="list-style-type: none"> – EAP-TLS session timeout (minutes)—Enter a value in minutes for that defines the maximum time for the EAP-TLS session. <p>ACS supports an EAP-TLS session resume feature that caches the TLS session created during a new EAP-TLS authentication. When an EAP-TLS client reconnects, the cached TLS session is used to restore the session without performing a certificate comparison, which improves EAP-TLS performance. ACS deletes cached TLS sessions when they time out. If ACS or the end-user client is restarted, certificate comparison is required even if the session timeout interval has not ended. To disable the session resume feature, set the timeout value to zero (0).</p>

Field	Description
Select one of the following options for setting username during authentication.	<p>You can specify which user identity ACS uses when sending an authentication request after the EAP-TLS authentication handshake is completed. use this option to search for a user in the database based on the identity you chose. By default, outer identity is used for EAP-TLS authentication. Select one of the following options:</p> <ul style="list-style-type: none"> • Use Outer Identity—The outer identity is taken as the username to search for in the database. • Use CN as Identity—The Certificate Name is taken as the username to search for in the database. • Use SAN as Identity— The Subject Alternative Name from the user certificate is taken as the username to search for in the database. <p>Note SAN and CN outer identities cannot be used for EAP TLS machine authentication.</p>
LEAP	<p>The Allow LEAP (For Aironet only) check box controls whether ACS performs LEAP authentication. LEAP is currently used only for Cisco Aironet wireless networking. If you disable 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.</p> <p>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 on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.</p>
EAP-MD5	To enable EAP-based Message Digest 5 hashed authentication, check this check box.
Allow EAP request timeout (seconds)	<p>You use this option to instruct Cisco Aironet Access Points (APs) to use the specified timeout value during EAP conversations. The value that is specified must be the number of seconds after which Cisco Aironet APs should assume that an EAP transaction with ACS has been lost and should be restarted. A value of zero (0) disables this feature.</p> <p>During EAP conversations, ACS sends the value that is defined in the AP EAP request timeout box by using the IETF RADIUS Session-Timeout (27) attribute.</p> <p>Note The same settings apply to Cisco Airespace wireless LAN controllers and IOS access points. These devices also have a configuration option to overwrite ACS session timeout settings.</p>
MS-CHAP Configuration	<p>For RADIUS authentication, ACS supports MS-CHAP versions 1 and 2. You can configure whether ACS authenticates users with MS-CHAP when the AAA protocol is RADIUS and, if so, which versions it uses.</p> <p>To enable MS-CHAP in RADIUS-based authentication, check the check box corresponding to the MS-CHAP version that you want to use. To allow MS-CHAP to use either version, check both check boxes.</p> <p>To disable MS-CHAP in RADIUS-based authentication, clear both check boxes.</p> <p>Note For TACACS+, ACS supports only MS-CHAP version 1. TACACS+ support for MS-CHAP version 1 is always enabled and is not configurable.</p>

EAP-FAST Configuration Page

Use this page to configure EAP-FAST authentication settings.

To open this page choose **System Configuration > Global Authentication Setup > EAP-FAST Configuration**.

Field	Description
Allow EAP-FAST	Whether ACS permits EAP-FAST authentication.
Active master key TTL	The duration that a master key is used to generate new PACs. Enter a value for the amount of time that a master key is used to generate new Protected Access Credentials (PACs). When the time to live (TTL) that is defined for the Master Key expires, the master key is considered retired and a new master key is generated. The default master key TTL is one month. Decreasing the master key TTL can cause retired master keys to expire because a master key expires when it is older than the sum of the master key TTL and the retired master key TTL; therefore, decreasing the master key TTL requires PAC provisioning for end-user clients with PACs that are based on the newly expired master keys. For more information about master keys, see About Master Keys, page 9-11 .
Retired master key TTL	Enter a value for the amount of time that PACs that are generated by using a retired master key are acceptable for EAP-FAST authentication. When an end-user client gains network access by using a PAC that is based on a retired master key, ACS sends a new PAC to the end-user client. The default retired master key TTL is three months. Note Decreasing the retired master key TTL can cause retired master keys to expire; therefore, decreasing the retired master key TTL requires PAC provisioning for end-user clients with PACs based on the newly expired master keys.
Tunnel PAC TTL	The duration that a PAC is used before it expires and must be replaced. Enter a value for the amount of time that a PAC is used before it expires and must be replaced. If the master key that is used to generate the Tunnel PAC has not expired, new PAC creation and assignment is automatic. If the master key used to generate the Tunnel PAC that expired, you must use automatic or manual provisioning to provide the end-user client with a new PAC. For more information about PACs, see About PACs, page 9-12 .
Client initial display message	Specify a message to be sent to users who authenticate with an EAP-FAST client. Maximum length is 40 characters. A user will see the initial message only if the end-user client supports its display.
Authority ID Info	The textual identity of this ACS server, which an end user can use to determine which ACS server to be authenticated against. Filling in this field is mandatory.
Allow full TLS renegotiation in case of Invalid PAC	If this check box is checked, when ACS detects a failure to establish the SSL tunnel due to an invalid PAC, it will fallback to full TLS renegotiation.
Allow anonymous in-band PAC provisioning	ACS provisions an end-user client with a PAC by using EAP-FAST phase zero. If you check this check box, ACS establishes a secured connection with the end-user client for the purpose of providing the client with a new PAC.
Enable anonymous TLS renegotiation	This option allows an anonymous TLS handshake between the end-user client and ACS. EAP-MS-CHAP will be used as the only inner method in phase zero.
Allow authenticated in-band PAC provisioning	ACS provisions an end-user client with a PAC by using EAP-FAST phase zero with SSL server-side authentication. This option requires that a server certificate and a trusted root CA are installed on ACS. One of the allowed inner methods will then be used to authenticate the user. In addition, the client may send its certificate to the server, causing the mutual TLS authentication. In this case, ACS skips the inner methods and provisions the PAC.

Field	Description
Accept client on authenticated provisioning	This option is only available when the allow authenticated in-band PAC provisioning option is selected. The server always sends an Access-Reject at the end of the provisioning phase, forcing the client to reauthenticate using the tunnel PAC. This option enables ACS to send an Access-Accept to the client at the end of the provisioning phase.
Require client certificate for provisioning	Allows provisioning PACs based on certificates only. Other inner EAP methods for PAC provisioning are not allowed. If the client does not present its certificate during the first TLS handshake, the server initiates a TLS renegotiation. The renegotiation requests the client to start a new TLS handshake; the cipher that was negotiated in the first handshake protects it. During the second TLS handshake, the server requests the client's certificate. If the certificate is not sent, the handshake fails and the user is denied access.
When receiving client certificate, select one of the following lookup methods:	<p>If you choose more than one comparison type, ACS performs the comparisons in the order listed. If the one comparison type fails, ACS attempts the next enabled comparison type. Comparison stops after the first successful comparison. The two types of comparison are:</p> <ul style="list-style-type: none"> • Certificate SAN comparison—Verifies user identity by comparing the name in the Subject Alternative Name field of the end-user certificate to the username in the applicable user database, check this check box. • Certificate CN comparison—Verifies user identity by comparing the name in the Common Name field of the end-user certificate to the username in the applicable user database, check this check box.
Allow Machine Authentication	<p>ACS provisions an end-user client with a machine PAC and performs 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 database or external databases. After these details are correctly verified, no further authentication is performed.</p> <p>Note After performing machine authentication and when the Required or Posture Only check boxes are checked, ACS also requests the posture credentials.</p>
Machine PAC TTL	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).
Allow Stateless session resume	<p>Uncheck this option:</p> <ul style="list-style-type: none"> • If you do not want ACS to provision authorization PACs for EAP-FAST clients. • To always perform phase two of EAP-FAST.
Authorization PAC TTL	This option determines the expiration time of the user authorization PAC. When ACS receives an expired authorization PAC, Allow Stateless session resume fails and, therefore, phase two EAP-FAST authentication is performed.

Field	Description
Allowed inner methods	<p>This option determines which inner EAP methods can run inside the EAP-FAST TLS tunnel. For anonymous in-band provisioning, you must enable EAP-GTC and EAP-MS-CHAP for backward compatibility. If you selected Allow anonymous in-band PAC provisioning, you must select EAP-MS-CHAP (phase zero) and EAP-GTC (phase two). If you selected Allow authenticated in-band PAC provisioning, the inner method in the authentication phase is negotiable. (EAP-GTC is used by default in phase zero.) Select one or more of the following inner methods:</p> <ul style="list-style-type: none"> • EAP-GTC—To enable EAP-GTC in EAP FAST authentication, check this box. • EAP-MS-CHAPv2—To enable EAP-MS-CHAPv2 in EAP FAST authentication, check this box. • EAP-TLS—To enable EAP-TLS in EAP FAST authentication, check this box. <p>Note ACS always runs the first enabled EAP method. For example, if you select EAP-GTC and EAP-MS-CHAPv2, then the first enabled EAP method is EAP-GTC.</p>
Choose one or more of the following EAP-TLS comparison methods:	<p>If you choose more than one comparison type, ACS performs the comparisons in the order listed. If the one comparison type fails, ACS attempts the next enabled comparison type. Comparison stops after the first successful comparison. The two types of comparison are:</p> <ul style="list-style-type: none"> • Certificate SAN comparison—Verifies user identity by comparing the name in the Subject Alternative Name field of the end-user certificate to the username in the applicable user database, check this check box. • Certificate CN comparison—Verifies user identity by comparing the name in the Common Name field of the end-user certificate to the username in the applicable user database, check this check box. • Certificate Binary comparison—Verifies user identity by doing a binary comparison of the end-user certificate to the user certificate stored in Active Directory, check this check box.
EAP-TLS session timeout (minutes)	<p>EAP-TLS session timeout (minutes)—Enter a value in minutes that defines the maximum time for the EAP-TLS session.</p> <p>ACS supports an EAP-TLS session resume feature that caches the TLS session created during a new EAP-TLS authentication. When an EAP-TLS client reconnects, the cached TLS session is used to restore the session without performing a certificate comparison, which improves EAP-TLS performance. ACS deletes cached TLS sessions when they time out. If ACS or the end-user client is restarted, certificate comparison is required; even if the session timeout interval has not ended. To disable the session resume feature, set the timeout value to zero (0).</p>
EAP-FAST Master Server	<p>Select this check box to determine whether ACS creates its own master keys, and uses its own EAP-FAST settings and Authority ID; or, if it uses the EAP-FAST settings, master keys, and Authority ID received from another (slave or replicated) ACS that has been replicated. If you change this setting, click Submit + Apply.</p>
Actual EAP-FAST server status	<p>This option displays the status of the ACS. If you uncheck the EAP-FAST master server check box, the server status does not change to <code>slave</code> until after ACS receives replicated EAP-FAST settings.</p> <p>Note If you uncheck the EAP-FAST Master Server check box, EAP-FAST server status remains <code>Master</code> until ACS receives replicated EAP-FAST components.</p>



CHAPTER 10

Logs and Reports

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, produces a variety of logs. You can download many of these logs, or view them in the ACS web interface as HTML reports.

These topics describe how to configure and view ACS logs and reports:

- [About ACS Logs and Reports, page 10-1](#)
- [Configuring ACS Logs, page 10-22](#)
- [Viewing and Downloading Reports, page 10-30](#)
- [Update Packets in Accounting Logs, page 10-37](#)
- [Logging Configuration Pages Reference, page 10-37](#)
- [Service Control Page Reference, page 10-43](#)
- [Reports Page Reference, page 10-44](#)

About ACS Logs and Reports

ACS logs a variety of user and system activities to different formats and targets. These topics describe the information that you can log:

- [AAA-Related Logs, page 10-1](#)
- [ACS Audit Logs, page 10-5](#)
- [ACS Logging Formats and Targets, page 10-5](#)
- [Dynamic Administration Reports, page 10-11](#)
- [Entitlement Reports, page 10-11](#)
- [Service Logs, page 10-12](#)

AAA-Related Logs

AAA-related logs contain information about the use of remote access services by users. [Table 10-1](#) describes all AAA-related logs.

In the web interface, you can enable, configure, and view AAA-related logs, if you have the appropriate permissions.

Table 10-1 AAA-Related Log Descriptions

Log	Description
TACACS+ Accounting	<p>Contains:</p> <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification (CLID) • Session duration
TACACS+ Administration	<p>Lists configuration commands entered on a AAA client by using TACACS+ (Cisco IOS). Particularly if you use ACS to perform command authorization, we recommend that you use this log.</p> <p>Note To use the TACACS+ Administration log, you must configure TACACS+ AAA clients to perform command accounting with ACS. The following line must appear in the access server or router configuration file:</p> <pre>aaa accounting commands start-stop tacacs+</pre>
RADIUS Accounting	<p>Contains:</p> <ul style="list-style-type: none"> • User sessions stop and start times • AAA client messages with username • Caller line identification information • Session duration <p>You can configure ACS to include accounting for Voice-over-IP (VoIP) in the RADIUS Accounting log, in a separate VoIP accounting log, or in both places.</p>
VoIP Accounting	<p>Contains:</p> <ul style="list-style-type: none"> • VoIP session stop and start times • AAA client messages with username • CLID information • VoIP session duration • cisco-av-pair attribute information <p>You can configure ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS Accounting log, or in both places.</p>
Failed Attempts	<p>Lists authentication and authorization failures with an indication of the cause. For posture-validation requests, this log records the results of any posture validation that returns a posture token other than <code>Healthy</code>.</p> <p>You can use these reports to find out who disabled the account if a given number of failed attempts has been enabled under the expiration information. This can also provide some insight into intrusion attempts and is a valuable tool for troubleshooting.</p>
Passed Authentications	<p>Lists successful authentication requests. This log does not depend on accounting packets from your AAA clients, so it is available; even if your AAA clients do not support RADIUS accounting or if you have disabled accounting on your AAA clients. For posture-validation requests, this log records the results of all posture-validation requests resulting in an SPT.</p>

Logging Attributes

Information is logged as a set of logging attributes. These attributes can be:

- Cisco generic.
- RADIUS generic—See [Appendix B, “RADIUS Attributes”](#) for information about these attributes.
- TACACS generic—See [Appendix A, “TACACS+ Attribute-Value Pairs”](#) for information about these attributes.
- ACS specific.— See [Table 10-17](#) for additional Audit Log Attributes specific to ACS.

Among the many attributes that ACS can record in its logs, a few are of special importance. The following list explains the special logging attributes that ACS provides.

- **User Attributes**—These logging attributes appear in the Attributes list for any log configuration page. ACS lists them by using their default names: Real Name, Description, User Field 3, User Field 4, and User Field 5. If you change the name of a user-defined attribute, the default name, rather than the new name, still appears in the Attributes list.

The values that you enter in the corresponding fields in the user account determine the content of these attributes. For more information about user attributes, see [Customizing User Data, page 2-5](#).

- **ExtDB Info**—If the user is authenticated with an external user database, this attribute contains a value that the database returns. In the case of a Windows user database, this attribute contains the name of the domain that authenticated the user.

In entries in the Failed Attempts log, this attribute contains the database that last successfully authenticated the user. It does not list the database that failed the user-authentication attempt.

- **Access Device**—The name of the AAA client that is sending the logging data to ACS.
- **Network Device Group**—The network device group to which the access device (AAA client) belongs.
- **Filter Information**—The result of network access restrictions (NARs) applied to the user, if any. The message in this field indicates whether all applicable NARs permitted the user access, all applicable NARs denied the user access, or more specific information about which NAR denied the user access. If no NARs apply to the user, this logging attribute notes that no NARs were applied.

The Filter Information attribute is available for Passed Authentication and Failed Attempts logs.

- **Device Command Set**—The name of the device command set, if any, that was used to satisfy a command authorization request.

The Device Command Set attribute is available for Failed Attempts logs.

- **Bypass info**—Information about the MAC authentication bypass feature. The message in this field indicates whether the MAC address was found or not found.

The Bypass info attribute is available for Failed Attempts and Passed Authentications logs.

- **Remote Logging Result**—Whether a remote logging service successfully processes a forwarded accounting packet. This attribute is useful for determining which accounting packets, if any, a central logging service did not log. It depends on the receipt of an acknowledgment message from the remote logging service. The acknowledgment message indicates that the remote logging service properly processed the accounting packet according to its configuration. A value of `Remote-logging-successful` indicates that the remote logging service successfully processed the accounting packet. A value of `Remote-logging-failed` indicates that the remote logging service did not process the accounting packet successfully.

**Note**

ACS cannot determine how a remote logging service is configured to process accounting packets that it forwarded. For example, if a remote logging service is configured to discard accounting packets, it discards a forwarded accounting packet and responds to ACS with an acknowledgment message. This message causes ACS to write a value of `Remote-logging-successful` in the Remote Logging Result attribute in the local log that records the account packet.

- **Posture-Validation Logging Attributes:**

- **Application-Posture-Token**—The application posture token (APT) that a particular policy returns during a posture-validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs.
- **System-Posture-Token**—The system posture token (SPT) that a particular policy returns during a posture-validation request. This attribute is available only in the Passed Authentications and Failed Attempts logs.
- **Other Posture-Validation Attributes**—Attributes that a NAC client sends to ACS during a posture-validation request. The attributes are uniquely identified by the vendor name, application name, and attribute name. For example, the NAI:AV:DAT-Date attribute is an attribute containing information about the date of the DAT file on the NAC client for the antivirus application by Network Associates, Inc. These attributes are available only in the Passed Authentications and Failed Attempts logs.

You can choose to log posture-validation attributes in the Passed Authentications and Failed Attempts logs. All inbound attributes are available for logging. The only two outbound attributes that you can record in logs are `Application-Posture-Assessment` and `System-Posture-Assessment`.

All posture-validation requests resulting in a system posture token (SPT), also known as a system posture assessment, are logged in the Passed Authentications log. Posture-validation requests resulting in an SPT of anything other than `Healthy` are logged in the Failed Attempts log. For more information about posture tokens, see [Posture Tokens, page 13-3](#).

- **Authen-Failure-Code attribute for HCAP errors:**

When Host Credentials Authentication Protocol (HCAP) fails, the `Authen-Failure-Code` attribute entry in the Failed Attempts report may display one of the following errors:

- Version failure - Could not communicate with external policy server - wrong HCAP version
- Connection failure - Could not open a connection to external policy server
- Authentication failure - Could not communicate with external policy server - authentication failure
- Timeout error - Could not connect to external policy server - timeout error
- Other - Posture Validation Failure on External Policy

Related Topics

- [Configuring ACS Logs, page 10-22](#)
- [Viewing and Downloading CSV Reports, page 10-31](#)

ACS Audit Logs

Audit logs contain information about the ACS system and activities and, therefore, record system-related events. These logs are useful for troubleshooting or audits. Comma-separated value (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 made for each user. ACS audit logs list all the attributes that were changed for a given user. For the list of the 95 attributes audit log attributes, see [Audit Log Attributes, page 10-46](#).

[Table 10-2](#) provides information about each audit log.

Table 10-2 **Audit Log Descriptions**

Log	Description and Related Topics
ACS Backup and Restore	Lists dates and times that the ACS system information was backed up and restored, and whether the action was successful. For information about changing the schedule or the location of the backup and restore files, see ACS Backup, page 7-8 and ACS System Restore, page 7-14 .
RDBMS Synchronization	Lists the times the RDBMS database was synchronized and whether the synchronization was manual or scheduled. For information about changing the RDBMS synchronization schedule, see RDBMS Synchronization, page 8-17 .
Database Replication	Lists the times the ACS Internal Database was replicated to the backup server and whether the replication was manual or scheduled. For information about changing the database replication schedule, see ACS Internal Database Replication, page 8-1 .
Administration Audit	Lists actions taken by each system administrator, such as adding users, editing groups, configuring a AAA client, or viewing reports.
User Password Changes	Lists user password changes that users initiate, regardless of which password-change mechanism was used to change the password. Thus, this log contains records of password changes that the ACS Authentication Agent, the User Changeable Password web interface, or the Telnet session made on a network device that is using TACACS+. This log does not list password changes that an administrator makes in the ACS web interface.
ACS Service Monitoring	Lists when ACS services start and stop.
Appliance Administration Audit	Lists administrator activity on the serial console, including logins, logouts, and commands executed.

Related Topics

- [Configuring ACS Logs, page 10-22](#)
- [Viewing and Downloading CSV Reports, page 10-31](#)

ACS Logging Formats and Targets

ACS *loggers* provide logging interfaces to record AAA-related logs and audit logs in different formats, and to different targets. You can use:

- [CSV Logger, page 10-6](#)
- [Syslog Logger, page 10-7](#)
- [ODBC Logger \(ACS for Windows only\), page 10-9](#)
- [Remote Logging for ACS for Windows, page 10-10](#)
- [Remote Logging for ACS SE with ACS Remote Agents, page 10-10](#)

You can configure ACS to log information to more than one logger. For information about configuring logs, see [Configuring ACS Logs, page 10-22](#).

You can configure a *critical logger* for accounting logs to guarantee delivery of these logs to at least one logger. For more information, see [Configuring Critical Loggers, page 10-23](#).

CSV Logger

The CSV logger records data for logging attributes in columns separated by commas (.). You can import this format into a variety of third-party applications, such as Microsoft Excel or Microsoft Access. After you import data from a CSV file into such applications, you can prepare charts or perform queries, such as determining how many hours a user was logged in to the network during a given period. For information about how to use a CSV file in a third-party application such as Microsoft Excel, see the documentation from the third-party vendor.



Tip

Using a CSV file may not work well for every language or locale; for example, when imported into programs such as Word or Excel. You may need to replace the commas (,) with semicolons (;), if necessary.

You can access the CSV files on the ACS server hard drive or you can download the CSV file from the web interface.

CSV Log File Locations

By default, ACS keeps log files in directories that are unique to the log. You can configure the log file location of CSV logs. The default directories for all logs reside in `sysdrive:\Program Files\CiscoSecure ACS vx.x`. For the subdirectory of this location for a specific log, see [Table 10-3](#).

Table 10-3 *Default CSV Log File Locations*

Log	Default Location
TACACS+ Accounting	<i>Logs\TACACS+Accounting</i>
CSV TACACS+ Administration	<i>Logs\TACACS+Administration</i>
CSV RADIUS Accounting	<i>Logs\RADIUS Accounting</i>
CSV VoIP Accounting	<i>Logs\VoIP Accounting</i>
CSV Failed Attempts	<i>Logs\Failed Attempts</i>
Passed Authentications	<i>Logs\Passed Authentications</i>
ACS Backup and Restore	<i>Logs\Backup and Restore</i>
RDBMS Synchronization	<i>Logs\DbSync</i>
RDBMS Synchronization	<i>Logs\DBReplicate</i>
Administration Audit	<i>Logs\AdminAudit</i>

Table 10-3 **Default CSV Log File Locations (continued)**

Log	Default Location
User Password Changes	<i>CSAuth\PasswordLogs</i>
ACS Active Service Monitoring	<i>Logs\ServiceMonitoring</i>

CSV Log Size and Retention

For each CSV log, ACS writes a separate log file. When a log file size reaches 10 MB, ACS starts a new log file. ACS retains the seven most recent log files for each CSV log.

Related Topics

- [Configuring a CSV Log, page 10-24](#)
- [Viewing and Downloading CSV Reports, page 10-31](#)

Syslog Logger

The ACS syslog logger supports the standard syslog format. You can send log data for any report to up to two syslog servers. You configure the syslog servers for each report individually. You can use syslog to centralize the data from multiple ACSs.

ACS syslog logging follows the standard syslog protocol (RFC 3164). Messages are sent connectionless to syslog servers by using an unsecured UDP port without data encryption.

**Note**

The syslog protocol contains no mechanism to ensure delivery, and since the underlying transport is UDP, message delivery is not guaranteed.

Syslog Message Format

The format of the ACS syslog message content is:

```
<n> mmm dd hh:mm:ss XX:XX:XX:XX TAG msg_id total_seg seg# A1=V1
```

where:

- **<n>**—The Priority value of the message; it is a combination of the facility and severity of the syslog message. The Priority value is calculated according to RFC 3164, by first multiplying the *facility* value by 8 and then adding the *severity* value.

ACS syslog messages use the following facility values:

- 4 (Auth)—Security and authorization messages. This value is used for all AAA-related messages (failed attempts, passed attempts, accounting, and so on).
- 13 (System3)—Log audit. This value is used for all other ACS report messages.

All ACS syslog messages use a severity value of 6 (Info).

For example, if the facility value is 13 and the severity value is 6, the Priority value is 110 ((8 x 13) + 6). The Priority value appears according to the syslog server setup, and might appear as one of:

- `System3.Info`
- `<110>`



Note You cannot configure the format of the syslog facility and severity on ACS.

- **mmm dd hh:mm:ss**—Date and time of the message.
- **XX:XX:XX:XX**—IP Address of the machine generating this syslog message.
- **TAG**—A value representing the ACS report name:
 - CisACS_01_PassedAuth—Cisco ACS Passed Authentications
 - CisACS_02_FailedAuth—Cisco ACS Failed Attempts
 - CisACS_03_RADIUSAcc—Cisco ACS RADIUS Accounting
 - CisACS_04_TACACSAcc—Cisco ACS TACACS+ Accounting
 - CisACS_05_TACACSAdmin—Cisco ACS TACACS+ Administration
 - CisACS_06_VoIPAcc—Cisco ACS VoIP Accounting
 - CisACS_11_BackRestore—Cisco ACS Backup and Restore log messages
 - CisACS_12_Replication—Cisco ACS Database Replication log messages
 - CisACS_13_AdminAudit —Cisco ACS Administration Audit log messages
 - CisACS_14_PassChanges—Cisco ACS User Password Changes log messages
 - CisACS_15_ServiceMon—Cisco ACS Service Monitoring log messages
 - CisACS_16_RDBMSSync—Cisco ACS RDBMS Synchronization Audit log messages
 - CisACS_17_ApplAdmin—Cisco ACS Appliance Administration Audit log messages
- **msg_id**—Unique message ID. All segments of one message share the same message ID.
- **total_seg**—Total number of segments in this message. For more details, see [Syslog Message Length Limitations, page 10-8](#).
- **seg#**—Segment sequence number within this message segmentation. For more details, see [Syslog Message Length Limitations, page 10-8](#).
- **A1=V1**—Attribute value pairs delimited by a comma (,) for Cisco ACS log messages and the message itself.

Syslog Message Length Limitations

You can configure the maximum length for ACS syslog messages. We recommend a maximum message length of 1,024 bytes for messages to a standard syslog server; however, the configuration should correspond to the target server specifications.

When an ACS message, including header and data, exceeds the syslog standard length limitation or target length limitation, the message content is split into several segments:

- The message is split between attribute value pairs keeping an attribute value pair complete within the segment, if possible. Each segment ends with the comma (,) delimiter; the next segment starts with the header and then the next attribute value pair.
- All segments of the same message have the same header. The **<msg_id>** and **<total_seg>** values are shared between all segments. The **<seg#>** is set according to the sequence of the segments.

For information about enabling and configuring syslog logs, see [Configuring Syslog Logging, page 10-24](#).

Related Topics

[Configuring Syslog Logging, page 10-24](#)

ODBC Logger (ACS for Windows only)

These topics describe ODBC logging and what to do before you configure ODBC logs in ACS:

- [About ODBC Logging, page 10-9](#)
- [Preparing for ODBC Logging, page 10-9](#)

About ODBC Logging

You can use Open DataBase Connectivity (ODBC) loggers to log directly in an ODBC-compliant relational database, where the logs are stored in tables, one table per log. After the data is exported to the relational database, you can use the data however you need. For more information about querying the data in your relational database, refer to the documentation from the relational database vendor.

Preparing for ODBC Logging

Before you can configure ODBC logs in ACS, you must:

1. Set up the relational database to which you want to export logging data. For more information, refer to your relational database documentation.
2. On the computer that is running ACS, set up a system data source name (DSN) for ACS to communicate with the relational database that will store your logging data.

To set up a system DSN for use with ODBC logging:

-
- | | |
|---------------|--|
| Step 1 | In the Windows Control Panel, double-click ODBC Data Sources . |
| Step 2 | In the ODBC Data Source Administrator page, click the System DSN tab. |
| Step 3 | Click Add . |
| Step 4 | Select the driver to use with your new DSN, and then click Finish . |
| | A dialog box displays fields requiring information that is specific to the selected ODBC driver. |
| Step 5 | Type a descriptive name for the DSN in the Data Source Name box. |
| Step 6 | Complete the other fields that are required by the selected ODBC driver. These fields may include information such as the IP address of the server on which the ODBC-compliant relational database runs. |
| Step 7 | Click OK . |
| Step 8 | Close the ODBC window and Windows Control Panel. |

The System DSN that ACS uses for communicating with the relational database is created on the computer running ACS. The name you assigned to the DSN appears in the Data Source list on each ODBC log configuration page.

Related Topics

[Configuring an ODBC Log \(ACS for Windows only\), page 10-25](#)

Remote Logging for ACS for Windows

You can use Remote Loggers to centralize AAA-related and audit logs that multiple ACSs generate. You can configure each ACS to point to one or more ACSs to use as a remote logging server. The remote logging ACS still performs AAA functions, but it also is the repository for the logs that it receives.

The Remote Logging feature enables ACS to send data directly to the CSLog service on the remote logging server, where the data is written to the logs. The remote logging server generates the logs in the formats that it is configured to use regardless of the local logging configuration on the ACSs that are sending the data.

ACS listens on TCP port 2001 for remote logging communication. A 128-bit proprietary algorithm encrypts remote logging data.

**Note**

The Remote Logging feature does not affect the forwarding of data for proxied authentication requests. ACS only applies Remote Logging settings to data for sessions that the proxy authenticates when data for sessions that the proxy authenticates is logged locally. For more information about proxied authentication requests and data for sessions that the proxy authenticates, see [Configuring Proxy Distribution Tables, page 3-28](#).

**Note**

Do not configure bidirectional remote logging for ACS. For example, you should not have ACS_SERVER_1 refer to ACS_SERVER_2 as a remote logger, and then have ACS_SERVER_2 refer to ACS_SERVER_1 as a remote logger.

Related Topics

[Configuring and Enabling Remote Logging \(ACS for Windows only\), page 10-26](#)

Remote Logging for ACS SE with ACS Remote Agents

The Remote Logging feature enables ACS to send data to one or more ACS Remote Agents. The remote agent runs on a computer on your network. It writes the data that ACS sends to it into CSV files. You can configure many ACS SEs to point to a single remote agent, thus making the computer that runs the remote agent a central logging server.

For more information about installing and configuring an ACS Remote Agent, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

**Note**

The Remote Logging feature does not affect the forwarding of data for proxied authentication requests. ACS only applies Remote Logging settings to data for sessions authenticated by proxy when accounting data for sessions authenticated by proxy is logged locally. For more information about proxied authentication requests and data for sessions authenticated by proxy, see [Configuring Proxy Distribution Tables, page 3-28](#).

Regardless of how many ACS SEs send their accounting data to the remote agent server, the remote agent receives its configuration from a single ACS SE. That ACS is the configuration provider for the remote agent. You determine:

- What logs the remote agent keeps.
- What data is recorded for each log kept.
- How the remote agent manages the log files.

Related Topics

[Configuring Logging to Remote Agents \(ACS SE only\), page 10-27](#)

Dynamic Administration Reports

These reports show the status of user accounts when you access them in the ACS web interface. They are available only in the web interface, are always enabled, and require no configuration.

[Table 10-4](#) contains descriptions of ACS administration reports.

Table 10-4 *Dynamic Administration Report Descriptions*

Report	Description and Related Topics
Logged-In Users	<p>Lists all users receiving services for a single AAA client or all AAA clients. You can delete logged-in users from specific AAA clients or from all AAA clients.</p> <p>Users accessing the network with Cisco Aironet equipment appear on the list for the access point that they are currently associated with, provided that the firmware image on the Cisco Aironet Access Point supports sending the RADIUS Service-Type attribute for rekey authentications.</p> <p>On a computer configured to perform machine authentication, machine authentication occurs when the computer starts. When a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section of the ACS web interface. Once user authentication begins, the computer no longer appears on the Logged-In Users List. For more information about machine authentication, see EAP and Windows Authentication, page 12-10.</p> <p>Note To use the logged-in user list feature, you must configure AAA clients to perform authentication and accounting by using the same protocol—TACACS+ or RADIUS.</p> <p>For information about viewing the Logged-in User report in the web interface and deleting logged-in users, see Viewing the Logged-in Users Report, page 10-34.</p>
Disabled Accounts	<p>Lists all user accounts that are disabled and the reason they were disabled. They might have been manually disabled or disabled automatically based on the aging information defined under User Setup.</p> <p>For information about viewing the Disabled Accounts report in the web interface, see Viewing the Disabled Accounts Report, page 10-35.</p>
Appliance Status	<p>Lists information about resource utilization on the ACS SE. Also displays information about the IP configuration for the ACS SE and the MAC address of its network interface card.</p> <p>For information about viewing the Appliance Status report in the web interface, see Viewing the Appliance Status Report, page 10-35.</p>

Related Topics

- [Viewing Dynamic Administration Reports, page 10-34](#)

Entitlement Reports

These reports provide information about administrator privileges and user mappings to groups. All these reports can be downloaded as text files in CSV format. You can display the reports for individual administrators in the ACS web interface. Entitlement reports are always enabled and require no configuration.

[Table 10-5](#) contains descriptions of ACS entitlement reports.

Table 10-5 **Entitlement Report Descriptions**

Report	Description and Related Topics
User Entitlements	The user entitlement report provides mappings of users to group. This report lists all users with their group, Network Access Profile (NAP) if relevant, and the mapping type (static or dynamic). You can download this report in CSV format; however, you cannot display it in the ACS web interface because of its potential size.
Administrator Entitlements	<p>The two types of Administrator Entitlement Reports are:</p> <ul style="list-style-type: none"> • Privilege report for all administrators—Lists the privileges of each administrator. You can download this report in CSV format; however, you cannot display it in the ACS web interface because of its potential size. • Privilege reports for individual administrators—Lists privileges for the selected administrator. You can display reports for individual administrators in the ACS web interface, and you can download them as text files in CSV format.

Related Topics

- [Viewing and Downloading Entitlement Reports, page 10-36](#)

Service Logs

Service logs are considered diagnostic logs, which you use for troubleshooting or debugging purposes only. These logs are not intended for general use by ACS administrators; instead, they are mainly sources of information for Cisco support personnel. Service logs contain a record of all ACS service actions and activities. When service logging is enabled, each service generates a log whenever the service is running, regardless of whether you are using the service. For example, RADIUS service logs are created even if you are not using the RADIUS protocol in your network. For more information about ACS services, see [Chapter 1, “Overview.”](#)

Service log files reside in the `\Logs` subdirectory of the applicable service directory. For example, the following is the default directory for the ACS authentication service:

```
c:\Program Files\CiscoSecure ACS vx.x\CSAuth\Logs
```

Services Logged

ACS generates logs for the following services:

- CSAdmin
- CSAuth
- CSDBSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

The most recent debug log is named:

```
SERVICE.log
```


where *SERVICE* is the name that represents the applicable service, for example *auth* represents the **CSAuth** service.

Older debug logs are named with the year, month, and date on which they were created. For example, a file that was created on July 13, 1999, would be named:

SERVICE 1999-07-13.log

where *SERVICE* is the name that represents the applicable service.

If you selected the Day/Month/Year format, the file would be named:

SERVICE 13-07-1999.log

For information about changing the date format, see [Date and Time Format Control](#), page 7-3.

Related Topics

[Configuring Service Logs](#), page 10-29

Adding Session IDs to the CSAuth Diagnostic Log

ACS supports a session ID parameter for the **CSAuth** diagnostic log. The **CSAuth** diagnostic log tracks each active authentication session by using a session data structure. The ACS services refer to these structures by session ID. You can use a unique session ID to differentiate log threads in the **CSAuth** diagnostic logs.

[Example 10-1](#) shows the session ID **1000** is processed by two different threads (2560, 2548) in the network model thread. You can filter the logs by session ID to restrict the output for each session.

Example 10-1 CSAuth Diagnostic Log with session ID

```
AUTH 09/08/2006 18:29:57 I 5081 2560 1000 Start RQ1040, client 1 (127.0.0.1)
AUTH 09/08/2006 18:30:13 I 5094 2548 Worker 1 processing message 17.
AUTH 09/08/2006 18:30:14 I 0991 2368 0000 pvNASMonitorThreadMain: start NM
update ...
AUTH 09/08/2006 18:30:14 I 1006 2368 0000 pvNASMonitorThreadMain: commit NM
update ...
AUTH 09/08/2006 18:30:14 I 5081 2560 1000 Done RQ1040, client 1, status 0
AUTH 09/08/2006 18:30:14 I 1011 2368 0000 pvNASMonitorThreadMain: succeeded
to commit NM update
AUTH 09/08/2006 18:30:28 I 5081 2548 1000 Start RQ1012, client 2 (127.0.0.1)
AUTH 09/08/2006 18:30:28 I 5081 2548 1000 Done RQ1012, client 2, status 0
```



Note

The additional session ID field in the ACS diagnostic log involves minimal overhead: eight bytes per line for each authentication session.

You use the same session ID for different authentication sessions. This means that the same session ID can appear in the diagnostic logs for more than one session. Cisco recommends that you use unique session IDs for each authentication session. Session IDs are maintained up to a limit of 120 seconds.

Description of Error Codes in the CSAuth Diagnostic Log

CSAuth diagnostic logs display a description of client requests and responses. Previous versions of ACS used a numeric code for client requests and responses. The description is useful for locating client requests and responses in the **CSAuth** diagnostic logs.

Two examples of **CSAuth** diagnostic log entries follow. [Example 10-2](#) represents an entry from previous versions of the **CSAuth** diagnostic log. [Example 10-3](#) represents how this entry for the **CSAuth** diagnostic log appears in this release.

[Example 10-3](#) shows that in the **CSAuth** diagnostic log:

- UDB_AUTHENTICATE_USER replaces the RQ1026 request code in the first example.
- UDB_CHALLENGE_REQUIRED replaces the 2046 status code in the first example.

Example 10-2 CSAuth Diagnostic Log Entry

```
AUTH 09/11/2006 09:55:27 I 5081 2512 Done RQ1026, client 50, status -2046
```

Example 10-3 CSAuth Diagnostic Log Entry (with Descriptive text)

```
AUTH 09/11/2006 09:55:27 I 5081 2512 Done UDB_AUTHENTICATE_USER, client 50, status
UDB_CHALLENGE_REQUIRED
```

Descriptive Request Text in the CSAuth Diagnostic Logs

[Table 10-6](#) and [Table 10-7](#) list the descriptive text for requests and status that appear in the **CSAuth** diagnostic logs.

[Table 10-6](#) lists the descriptive text in the **CSAuth** diagnostic logs and the corresponding request code.

Table 10-6 Descriptive Request Text and Request Code

Request Text	Request Code
UDB_BASE_CMD	1000
UDB_HAIL	1001
UDB_OPEN	1002
UDB_CLOSE	1003
UDB_GOODBYE	1004
UDB_PING	1005
UDB_REFRESH	1006
UDB_REFRESH_EX	1007
UDB_RESET_HOST_CACHE	1008
UDB_USER_ADD	1010
UDB_USER_REMOVE	1011
UDB_VALID_USER	1012
UDB_USER_ENUM_BY_GROUP	1013
UDB_CHANGE_PASSWORD	1014
UDB_SET_PASS_STATUS	1015
UDB_GET_PASS_STATUS	1016
UDB_USER_ENUM	1017
UDB_USER_GET_INFO	1018
UDB_USER_PAP_CHECK	1019

Table 10-6 *Descriptive Request Text and Request Code (continued)*

Request Text	Request Code
UDB_USER_PROF_ASSIGN	1020
UDB_USER_PROF_COUNT	1021
UDB_USER_PROF_GET	1022
UDB_USER_CHAP_CHECK	1023
UDB_USER_CHECK_EXPIRY	1024
UDB_USER_SET_INFO	1025
UDB_AUTHENTICATE_USER	1026
UDB_SEND_RESPONSE	1027
UDB_SET_PASSWORD	1028
UDB_USER_LOCN_CHECK	1029
UDB_SET_VALUE	1030
UDB_GET_VALUE	1031
UDB_GET_NEXT_VALUE	1032
UDB_DEL_VALUE	1033
UDB_FIND_VALUE	1034
UDB_GET_VALUE_BY_NAME	1035
UDB_LOG	1040
UDB_SET_APPDATA	1041
UDB_GET_APPDATA	1042
UDB_DEL_DB	1043
UDB_AVERT_LOG	1044
UDB_DIR_CREATE	1050
UDB_FILE_CREATE	1051
UDB_FILE_WRITE	1052
UDB_FILE_READ	1053
UDB_FILE_CLOSE	1054
UDB_FILE_EXISTS	1055
UDB_FILE_APPEND	1056
UDB_FILE_SET_PTR	1057
UDB_USER_LIST_ADD	1070
UDB_USER_LIST_DEL	1071
UDB_USER_LIST_GET	1072
UDB_USER_LIST_COUNT	1073
UDB_USER_LIST_UPDATE	1074
UDB_USER_ALIAS_SET	1080
UDB_USER_ALIAS_DEL	1081

Table 10-6 *Descriptive Request Text and Request Code (continued)*

Request Text	Request Code
UDB_USER_ALIAS_VALID	1082
UDB_START_TRANSACTION	1090
UDB_END_TRANSACTION	1091
UDB_KICK_SYNC_TX	1092
UDB_KICK_SYNC_RX	1093
UDB_EXCHANGE_SYNC_INFO	1094
UDB_AQUIRE_IP_ADDRESS	1095
UDB_VALIDATE_PASSWORD	1096
UDB_EXTRACT_AGING_DATA	1097
UDB_AUTH_FAILED	1098
UDB_RESET_USER_PASSWORD_AGING_DATA	1099
UDB_GET_AGING_INFO	1100
UDB_DO_BACKUP_NOW	1101
UDB_AQUIRE_CALLBACK	1102
UDB_GET_AGING_LIMIT	1103
UDB_PURGE_NAS	1104
UDB_SEND_FAKE_STOPS	1105
UDB_SERVICE_CONTROL	1106
UDB_RESET_GROUP	1107
UDB_SET_ENABLE_PASS_STATUS	1108
UDB_UPDATE_AGING_POLICY	1109
UDB_ADD_HOST	1110
UDB_DEL_HOST	1111
UDB_GET_HOST	1112
UDB_UPDATE_HOST	1113
UDB_ADD_PROXY	1114
UDB_DEL_PROXY	1115
UDB_ADD_PROXY_TARGET	1116
UDB_ADD_NDG	1117
UDB_DEL_NDG	1118
UDB_GET_NDG_ID	1119
UDB_SET_USER_FEATURE_FLAG	1120
UDB_GET_USER_COUNTER	1121
UDB_RESET_USER_COUNTER	1122
UDB_RESET_GROUP_USERS_COUNTER	1123
UDB_GET_FIRST_QUOTA_TYPE	1124

Table 10-6 Descriptive Request Text and Request Code (continued)

Request Text	Request Code
UDB_GET_NEXT_QUOTA_TYPE	1125
UDB_SET_QUOTA	1126
UDB_HAS_USER_QUOTA_EXHAUSTED	1127
UDB_SHARED_PROFILE	1128
UDB_ADD_UDV	1140
UDB_DEL_UDV	1141
UDB_GET_VID_FROM_IETF	1142
UDB_ADD_UDV_VSA	1143
UDB_ADD_UDV_VSA_ENUM	1144
UDB_ADD_UDV_VSA_PROFILE	1145
UDB_SET_REP_DIRTY_FLAG	1150
UDB_USER_COMMIT_NOW	1151
UDB_POLICY_CREATE_CONTEXT	1152
UDB_USER_REMOVE_DYNAMIC	1153

Table 10-7 lists the descriptive text in the **CSAuth** diagnostic logs and the corresponding status code.

Table 10-7 Descriptive Status Text and Request Code

Status Description	Status Code
UDB_BASE_ERR	1000
UDB_DB_NOT_OPEN	1001
UDB_INVALID_ENTRY	1002
UDB_CANT_CREATE_MAP	1003
UDB_CANT_CREATE_VIEW	1004
UDB_CANT_OPEN_INDEX	1005
UDB_DB_IS_OPEN	1006
UDB_SIZE_MISMATCH	1007
UDB_CANT_OPEN_FILE	1008
UDB_CRC_FAILED	1009
UDB_CANT_INIT_INDEX	1010
UDB_INVALID_DATA	2011
UDB_CANT_GROW_FILE	1012
UDB_USER_INVALID	2013
UDB_DUPLICATE_NAME	1014
UDB_INVALID_PASSWORD	2015
UDB_IPC_DATA_INVALID	1016
UDB_FEATURE_NOT_READY	1017

Table 10-7 *Descriptive Status Text and Request Code (continued)*

Status Description	Status Code
UDB_SERVER_BUSY	1018
UDB_REGISTRY_READ_FAIL	1019
UDB_UNKNOWN_VARIABLE	2020
UDB_NO_FILE_HANDLES	1021
UDB_DIR_CREATE_FAILED	1022
UDB_FILE_WRITE_FAILED	1023
UDB_FILE_READ_FAILED	1024
UDB_INVALID_DIR_NAME	1025
UDB_INVALID_FILE_NAME	1026
UDB_MALLOC_FAIL	1027
UDB_INVALID_HANDLE	1028
UDB_USER_NOT_OWNER	1029
UDB_CANT_REBUILD_INDEX	1030
UDB_CANT_REMOVE_OLD_DB	1031
UDB_USER_REMOVED	2032
UDB_NO_VARIABLE	1033
UDB_PASSWORD_DISABLED	2034
UDB_FILE_SET_PTR_FAILED	1035
UDB_USER_LICENCE_LIMIT	1036
UDB_APP_NOT_LICENSED	1037
UDB_BAD_SECRET	1038
UDB_DB_VERSION_MISMATCH	1039
UDB_DIR_REMOVE_FAILED	1040
UDB_CANT_ASSIGN_PROFILE	1041
UDB_LOGGER_OFFLINE	1042
UDB_CANT_ACCESS_USERLIST	1043
UDB_SESSION_COUNT_EXCEEDED	2044
UDB_PASSWORD_REQUIRED	2045
UDB_CHALLENGE_REQUIRED	2046
UDB_NO_SESSION	1047
UDB_INTERNAL_ERROR	1048
UDB_BAD_TODDOW	2049
UDB_CANT_LOCK_RECORD	1050
UDB_NT_DIALIN_REQUIRED	2051
UDB_NT_PW_WRONG	2052
UDB_NT_AC_RESTRICTED	2053

Table 10-7 *Descriptive Status Text and Request Code (continued)*

Status Description	Status Code
UDB_NT_TOD_DOW	2054
UDB_NT_PW_EXPIRED	2055
UDB_NT_AC_DISABLED	2056
UDB_NT_BAD_WORKSTATION	2057
UDB_NT_UNKNOWN_ERR	1058
UDB_NT_PASS_CHANGE	2059
UDB_NT_NO_DOMAIN	2060
UDB_NT_AC_LOCKED	2061
UDB_NT_NO_BROWSER	2062
UDB_INVALID_CHAP_PW	2063
UDB_INVALID_ARAP_PW	2064
UDB_INVALID_TOKEN_PW	2065
UDB_INVALID_UNIX_PW	2066
UDB_TOKEN_SERVER_DOWN	1067
UDB_USER_CLI_FILTERED	2068
UDB_NO_SENDAUTH_PW	1069
UDB_NO_TOKENSRV	1070
UDB_NT_NO_LOGON_NOT_GRANTED	2071
UDB_CANT_START_TRANSACTION	1072
UDB_VARDDB_NOT_OPEN	1073
UDB_NOT_IN_CACHE	1074
UDB_CANT_OPEN_ODBC_DB	1075
UDB_DLL_MISMATCH	1076
UDB_NOT_INSTALLED	1077
UDB_CHAP_ENFORCED	2078
UDB_ACCESS_DENIED	2079
UDB_REPLICATION_DENIED	1080
UDB_FAILED_TO_AQUIRE_IP_ADDR	1081
UDB_PASSWORD_DEAD	2082
UDB_PASSWORD_STATE_NOT_ACCESSIBLE	1083
UDB_PASSWORD_AGE_CHECK_FAILED	1084
UDB_NEW_PASSWORD_NOT_GOOD	2085
UDB_FAILED_TO_EXTRACT_DATA	1086
UDB_EXTERN_DB_ERROR	2087
UDB_BACKUP_FAILED_TO_START	1088
UDB_FAILED_TO_AQUIRE_CALLBACK	1089

Table 10-7 *Descriptive Status Text and Request Code (continued)*

Status Description	Status Code
UDB_FAILED_TO_PERFORM_SERVICE_OP	1090
UDB_TIME_OUT_WAITING_TO_START_AUTH	1091
UDB_AUTH_NOT_SUPPORTED_BY_EXT_DB	2092
UDB_CACHED_TOKEN_REJECTED	2093
UDB_TOKEN_PIN_CHANGED	2094
UDB_INVALID_MSCHAP_PW	2095
UDB_INVALID_EXT_CHAP_PW	2096
UDB_INVALID_EXT_ARAP_PW	2097
UDB_INVALID_EXT_MSCHAP_PW	2098
UDB_INVALID_EXT_USER	2099
UDB_NT_AC_EXPIRED	2100
UDB_AUTH_DENIED_DUE_TO_VOIP	2101
UDB_MALFORMED_USERNAME	2102
UDB_CANT_OPEN_HOST_DB	1103
UDB_CANT_OPEN_PROXY_DB	1104
UDB_CANT_OPEN_NDG_DB	1105
UDB_HOST_DB_FAILURE	1106
UDB_PROXY_DB_FAILURE	1107
UDB_NDG_DB_FAILURE	1108
UDB_INVALID_COUNTER_TYPE	1109
UDB_EXTERN_DB_TRANSIENT_ERROR	1110
UDB_INVALID_QUOTA_INDEX	1111
UDB_USAGE_QUOTA_EXCEEDED	2112
UDB_NT_CHANGE_PASS_FAILED	2113
UDB_CANT_LOAD_DLL	1114
UDB_EXTN_DLL_REJECTED	2115
UDB_INVALID_EXT_EAP_PW	2116
UDB_EAP_METHOD_NOT_SUPPORTED	2117
UDB_EAP_TLS_PASS_HS_USER_NOT_FOUND	2118
UDB_EAP_NO_MATCH_NAME_IN_CERT	2119
UDB_EAP_TLS_HANDSHAKE_FAILED	2120
UDB_EAP_IGNORE	2121
UDB_SUPPLIER_NOT_CONFIGURED	2122
UDB_UDV_CONFIG_ERROR	1123
UDB_USER_FOUND	2124
UDB_USER_NOT_FOUND	2125

Table 10-7 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_EAP_FAILED	1126
UDB_MISSING_MPPE_DATA	2127
UDB_EAP_MACHINE_AUTH_DISABLED	2128
UDB_NT_NO_REMOTE_AGENT	2129
UDB_EAP_FAST_PAC_PROVISIONING	2130
UDB_EAP_FAST_USER_AND_IID_NOT_MATCH	2131
UDB_EAP_FAST_PAC_INVALID	2132
UDB_EAP_FAST_INBAND_NOT_ALLOWED	2133
UDB_EAP_FAST_INVALID_MASTER_KEY	2134
UDB_GROUP_DISABLED	2135
UDB_AVERT_NO_MAPPING	2136
UDB_EAP_PASSWORD_CHANGE_DISABLED	2137
UDB_AVERT_PROCEED_TO_UUP	2138
UDB_AVERT_LOCAL_POLICY_FAILED	2139
UDB_AVERT_EX_POLICY_FAILED	2140
UDB_AVERT_GENERAL_FAILURE	2141
UDB_ACCESS_DENIED_FAST_REC_NO_USER	2142
UDB_ACCESS_DENIED_MAR_RESTRICTION	2143
UDB_AVERT_UNKNOWN_ATTRIBUTE	2144
UDB_AUTH_PROTOCOL_NOT_ALLOWED	2145
UDB_EAP_FAST_ANON_INBAND_NOT_ALLOWED	2146
UDB_AUDIT_BAD_RESPONSE	2147
UDB_AUDIT_TOO_MANY_ROUND_TRIPS	2148
UDB_POSTURE_VALIDATION_FAILED	2149
UDB_MAC_AUTH_BYPASS_NOT_ALLOWED	2150
UDB_ACCESS_DENIED_NO_SERVICE	2151
UDB_AUTHORIZATION_REJECT	2152
UDB_PV_FAILED_NO_SERVICE	2153
UDB_LOCAL_USER_HAS_EXT_DB_AUTH	2154
UDB_SERVICE_EXT_DB_NOT_ALLOWED	2155
UDB_NT_LOGON_FAILURE	2156
UDB_MAC_AUTH_BYPASS_GROUP_DISABLE	2157
UDB_BADLY_FORMED_DACL_RQ	2158
UDB_INTERNAL_DACL_ERROR	2159
UDB_DACL_ASSIGN_ERROR	2160
UDB_INTERNAL_RAC_ERROR	2161

Table 10-7 Descriptive Status Text and Request Code (continued)

Status Description	Status Code
UDB_RAC_MISSING_ERROR	2162
UDB_AUDIT_RECIEVED_ERROR	2163
UDB_AUDIT_SERVER_UNREACHEABLE	2164
UDB_AUDIT_PARSE_ERROR	2165
UDB_EXT_POLICY_VER_ERROR	2166
UDB_EXT_POLICY_CONN_ERROR	2167
UDB_EXT_POLICY_AUTH_ERROR	2168
UDB_EXT_POLICY_TIMEOUT_ERROR	2169
UDB_ERR_PROFILE_TOO_BIG	1170
UDB_EXT_POLICY_CONN_ERROR_CA_UNKNOWN	2171
UDB_BASE_WARN	1000
UDB_ALREADY_OPEN	1001
UDB_PASSWORD_EXPIRED	1002
UDB_UNKNOWN_PASS_STATUS	1003
UDB_UDB_VALUE_OVERWRITE	1004
UDB_BUFFER_TOO_SMALL	1005
UDB_SIZE_SMALLER	1006
UDB_USER_NOT_ALIAS	1007
UDB_NO_MORE_QUOTA_TYPES	1008

Line Numbers in Diagnostic Logs

The ACS diagnostic log files contain the correct line number of the source code that generated the error. In previous versions of ACS, the **dzlog** function contained the hard-coded source code line number, which was populated to the ACS diagnostic log.

Generic EAP Code Debug Messages

ACS reports all EAP debug messages to the **CSAuth** diagnostic log.

Configuring ACS Logs

You can enable and configure logging for individual logs. ACS can log information to multiple loggers simultaneously.

The starting point for enabling and configuring service logs is the Service Control page, which you access by choosing **System Configuration > Service Control**. The starting point for enabling and configuring all other logs and loggers is the Logging Configuration page, which you access by choosing **System Configuration > Logging**. The Logging Configuration page also displays which ACS logs are currently enabled.

These topics describe how to configure and enable ACS logs:

- [Configuring Critical Loggers](#), page 10-23
- [Configuring a CSV Log](#), page 10-24
- [Configuring Syslog Logging](#), page 10-24
- [Configuring an ODBC Log \(ACS for Windows only\)](#), page 10-25
- [Configuring and Enabling Remote Logging \(ACS for Windows only\)](#), page 10-26
- [Configuring Logging to Remote Agents \(ACS SE only\)](#), page 10-27
- [Configuring Service Logs](#), page 10-29
- [Providing Service Logs for Customer Support](#), page 10-29

Configuring Critical Loggers

You can configure a critical logger for accounting logs to guarantee delivery of these logs to at least one logger.

When you configure a critical logger, the reply that ACS sends to an authenticating device depends on the success or failure of logging the relevant message to the critical logger only. ACS sends the message to other loggers off-stream, (best effort but not guaranteed), which does not affect the authentication result. (For all other AAA-related reports, such as failed attempts, passed authentications and TACACS+ administration, logging is done off-stream, and does not affect the authentication attempt result.)

You can configure a different critical logger for each accounting report; the default critical logger for each report is the local CSV log. If you do not select a critical logger, delivery of accounting messages is not guaranteed.



Note

We do not recommend that you configure a syslog logger as a critical logger; because, according to syslog standards, syslog message logging is not guaranteed.

To configure a critical logger for accounting reports:

-
- | | |
|---------------|---|
| Step 1 | In the navigation bar, click System Configuration . |
| Step 2 | Click Logging .
The Logging Configuration page appears. |
| Step 3 | Click Critical Loggers Configuration .
The Critical Loggers Configuration page appears. |
| Step 4 | Select a critical logger for each accounting report. For more information about the options for selecting critical loggers, see Critical Loggers Configuration Page , page 10-38. |
| Step 5 | Click Submit .
ACS implements the specified critical loggers configuration. |
-



Note

If a critical logger is chosen but the specified log is disabled, ACS will not implement critical logging for the specific report.

Configuring a CSV Log

You can configure ACS to record AAA-related logs and audit logs to a CSV logger.

To configure a CSV log:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**. The Logging Configuration page appears.
 - Step 3** In the ACS Reports table, click **Configure** for the CSV log that you want to configure.
The CSV *log* File Configuration page appears, where *log* is the name of the CSV log that you selected.
 - Step 4** To enable or disable the log, under Enable Logging, check or uncheck the **Log to *log* report** check box, where *log* is the name of the selected log.
 - Step 5** For AAA-related reports, configure the attributes that you want ACS to log. For more information about the options for configuring attributes, see [CSV log File Configuration Page, page 10-40](#).
 - Step 6** (ACS for Windows only) Specify file management options for the CSV files. For more information about the file management options, see [CSV log File Configuration Page, page 10-40](#).
 - Step 7** Click **Submit**.
ACS implements the specified CSV log configuration.
-

Related Topics

[Viewing and Downloading CSV Reports, page 10-31](#)

Configuring Syslog Logging

You can configure ACS to record AAA-related logs and audit logs to a syslog logger.

To configure a syslog log:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**. The Logging Configuration page appears.
 - Step 3** In the ACS Reports table, click **Configure** for the syslog log that you want to configure.
The *log* Configuration page appears, where *log* is the name of the syslog log that you selected.
 - Step 4** To enable or disable the log, under Enable Logging, check or uncheck the **Log to *log* report** check box, where *log* is the name of the selected log.
 - Step 5** For AAA-related reports, configure the attributes that you want ACS to log. For more information about the options for configuring attributes, see [Syslog log Configuration Page, page 10-41](#).
 - Step 6** Configure the syslog servers to which you want to send the syslog messages. For more information about the options for configuring syslog servers, see [Syslog log Configuration Page, page 10-41](#).
 - Step 7** Click **Submit**.
ACS implements the specified syslog log configuration.
-

Configuring an ODBC Log (ACS for Windows only)

You can configure ACS to record AAA-related logs and audit logs to an ODBC logger. You can configure the SQL create table statement before or after configuring the ODBC log in ACS.



Note

Before you can configure an ODBC log, you must prepare for ODBC logging. For more information, see [Preparing for ODBC Logging, page 10-9](#).

To configure an ODBC log:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Logging**. The Logging Configuration page appears.
- Step 3** In the ACS Reports table, click **Configure** for the ODBC log that you want to configure.
The ODBC *log* Configuration page appears, where *log* is the name of the ODBC log you selected.
- Step 4** To enable or disable the log, under Enable Logging, check or uncheck the **Log to *log* report** check box, where *log* is the name of the selected log.
- Step 5** For AAA-related reports, configure the attributes that you want ACS to send to the relational database. For more information about the options for configuring attributes, see [ODBC log Configuration Page \(ACS for Windows only\), page 10-42](#).
- Step 6** Configure ACS to communicate with the ODBC database. For more information about Connection Settings options, see [ODBC log Configuration Page \(ACS for Windows only\), page 10-42](#).
- Step 7** Click **Submit**.
ACS saves the log configuration. The Logging Configuration page appears.

To configure an SQL create table statement:

- Step 1** In the Logging Configuration page, click **Configure** for the ODBC log that you are configuring.
The ODBC log configuration page appears.
- Step 2** To display a SQL create table statement, click **Show Create Table**.
A SQL create table statement for Microsoft SQL Server appears in the right panel of the ACS window. The table name is the name that is specified in the Table Name field. The column names are the attributes that are specified in the Logged Attributes list.



Note

The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.

- Step 3** Using the information provided in the generated SQL, create a table in your relational database for this ODBC log. For ODBC logging to work, the table name and the column names must exactly match the names in the generated SQL.

When you enable the log, ACS begins sending logging data to the relational database table that you created by using the system DSN that you configured.

Configuring and Enabling Remote Logging (ACS for Windows only)

You can configure remote logging for AAA-related logs and audit logs. You must first configure the remote logging server, and then configure remote logging on each ACS that will send information to the remote logging server.

These topics describe how to set up remote logging:

- [Configuring the Remote Logging Server, page 10-26](#)
- [Configuring ACS to Send Data to a Remote Logger, page 10-27](#)

Configuring the Remote Logging Server

Before You Begin

- On a computer that you want to use as a remote logging server to store all logging data, install ACS. For information about installing ACS, see the *Installation Guide for Cisco Secure ACS for Windows Release 4.2*.
- Ensure that gateway devices between the ACSs that are sending data and the remote logging ACS server permit the remote logging ACS server to receive data on TCP port 2001.

To configure the remote logging server:

- Step 1** Configure and enable the individual logs as needed. All data that is sent to the remote logging server will be recorded in the way that you configure logs on this ACS. For information about:
- Configuring CSV logs, see [Configuring a CSV Log, page 10-24](#).
 - Configuring syslog logs, see [Configuring Syslog Logging, page 10-24](#).
 - Configuring ODBC logs, see [Configuring an ODBC Log \(ACS for Windows only\), page 10-25](#).



Note You can configure Remote Logging on the remote logging server so that it will send all data to another remote logging server. However, you must use this option with caution; otherwise, you might create an endless logging loop.

- Step 2** To the AAA Servers table, add each ACS from which the remote logging server will receive logging data. For more information, see [Configuring AAA Servers, page 3-15](#).



Note If the remote logging server logs watchdog and update packets for an ACS, you must check the Log Update/Watchdog Packets from this remote AAA Server check box for that ACS in the AAA Servers table.

If you want to implement remote logging on other remote logging servers for use as secondary servers or as mirrored logging servers, repeat this procedure for each additional remote logging server.

Related Topics

[Configuring ACS to Send Data to a Remote Logger, page 10-27](#)

Configuring ACS to Send Data to a Remote Logger



Note

Before configuring the Remote Logging feature on each ACS server that will send data to the remote logging server, ensure that you have configured your remote logging ACS server. For more information, see [Configuring the Remote Logging Server, page 10-26](#).

On each ACS that will send data to the remote logging server:

- Step 1** Add the remote logging server to the AAA Servers table. For more information, see [Configuring AAA Servers, page 3-15](#). If you have created multiple remote logging servers, repeat this step for each remote logging server.
- Step 2** In the navigation bar, click **System Configuration**.
- Step 3** Click **Logging**.
The Logging Configuration page appears.
- Step 4** Click **Remote Logging Servers Configuration**.
The Remote Logging Setup page appears.
- Step 5** Set the applicable Remote Logging Services Configuration options. For information about these options, see [Remote Logging Setup Page, page 10-39](#).
- Step 6** Click **Submit**.
ACS saves and implements the remote logging configuration that you specified.

Related Topics

- [Configuring the Remote Logging Server, page 10-26](#)

Configuring Logging to Remote Agents (ACS SE only)

You can configure remote logging of AAA-related logs and audit logs to installed ACS remote agents. For more information about installing and configuring an ACS Remote Agent, see *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

The following steps are required to set up remote logging:

1. On each ACS SE, add the remote agent. For more information, see [Configuring Remote Agents \(ACS SE Only\), page 3-19](#).
2. Configure each ACS SE to send logs to the remote agent. For more information, see [Configuring ACS SE to Send Data to the Remote Agent, page 10-28](#).
3. On the ACS SE that the remote agent is configured to use as its configuration provider, configure log content and log-file management for all logs recorded on the remote agent. For more information, see [Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#).

You can set up remote logging to another remote agent, for use as a secondary server or as a mirror server by repeating these steps.

Configuring ACS SE to Send Data to the Remote Agent

You configure each local ACS SE to send data to the remote agent. Local configuration of remote logging does not affect the types of logs sent to remote agents or the configuration of the data included in logs sent to remote agents. For information about configuring which logs are sent to remote agents and the data the logs contain, see [Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#).

Before You Begin

Install and configure the remote agent before configuring the Remote Logging feature on each ACS SE that will send data to the remote agent.

On each ACS SE that will send data to the remote agent:

-
- Step 1** Add the remote agent on ACS SE. For more information, see [Configuring Remote Agents \(ACS SE Only\), page 3-19](#).
 - Step 2** In the navigation bar, click **System Configuration**.
 - Step 3** Click **Logging**.
The Logging Configuration page appears.
 - Step 4** Click **Remote Logging Servers Configuration**.
The Remote Logging Setup page appears.
 - Step 5** Set the applicable Remote Logging Services Configuration options. For information about these options, see [Remote Logging Setup Page, page 10-39](#).
 - Step 6** Click **Submit**.
ACS saves and implements the remote logging configuration that you specified.
-

Related Topics

[Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#)

Configuring Remote Agent Logs on the Configuration Provider

On the configuration provider, you configure which logs will be stored on the remote agent, the log content, and how the remote agent will manage the log files.

For information about specifying to which remote agents ACS sends log data, see [Configuring ACS SE to Send Data to the Remote Agent, page 10-28](#).

To configure a CSV log for a remote agent:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Logging**.
The Logging Configuration page appears
 - Step 3** Click **Remote Agent Reports Configuration**.

The Remote Agent Reports Configuration page appears.

- Step 4** Click **Configure** for the remote logging report that you want to configure.

The CSV *log* File Configuration page appears, where *log* is the name of the remote agent log that you selected.

- Step 5** To enable or disable the log, check or uncheck the **Log to CSV *log* name report** check box, where *log* is the name of the remote agent log that you selected.

- Step 6** For AAA-related reports, configure the attributes that you want ACS to log. For more information about the options for configuring attributes, see [CSV log File Configuration Page, page 10-40](#).

- Step 7** Specify file management options for the CSV files. For more information about the file management options, see [CSV log File Configuration Page, page 10-40](#).

- Step 8** Click **Submit**.

ACS implements the remote agent log configuration that you specified.

Related Topics

[Configuring ACS SE to Send Data to the Remote Agent, page 10-28](#)

Configuring Service Logs

To configure how ACS generates and manages the service log file:

-
- Step 1** In the navigation bar, click **System Configuration**.

- Step 2** Click **Service Control**.

The status of the services appears in ACS on *hostname* table, where *hostname* is the name of the computer that is running ACS.

- Step 3** Set service log options in the Services Log File Configuration page. For information about the options in this page, see [Service Control Page Reference, page 10-43](#).

To disable the service log file, under Level of Detail, select the **None** option.

- Step 4** Click **Restart**.

ACS restarts its services and implements the service log settings that you specified.

Related Topics

[Providing Service Logs for Customer Support, page 10-29](#)

Providing Service Logs for Customer Support

To provide customer support with enough data to research potential issues, set the Level of Detail to Full in the Services Log File Configuration page. See [Service Control Page Reference, page 10-43](#) for more details. Ensure that you have sufficient disk space to handle your log entries.

If a problem exists on your ACS, customer support will ask you to create a *package.cab* file. The *package.cab* file contains various files including:

- **Certificate files**—The ACS server certificate, as well as the certificate's CA.
- **Admin.txt**—Contains information regarding ACS administrators.
- **Host.txt and HostServices.txt**—Contain information regarding hosts and hosts configuration.
- **NDG.txt**—Contains configured network device groups.
- **DictionaryKey.txt and DictionaryValue.txt**—Contains ACS dictionary files.

To create a *package.cab* file:

-
- Step 1** At the command prompt, type **drwtsn32**.
- Check the Dr. Watson settings to be sure the **Dump Symbol Table** and **Dump All Thread Contents** options are selected in addition to the default options.
- Step 2** Go to the *bin* subdirectory in the directory in which ACS was installed.
- Step 3** Type **CSSupport.exe**.
- Run the executable with all default options. The program will collect all the necessary information including Dr. Watson logs and place them in a file called *package.cab*. The location of the file appears when the executable is finished.
-

The Support feature in the System Configuration section of the ACS web interface includes service logs in the *package.cab* file that it generates if you click Run Support Now. For information about this feature, see [Support Page, page 7-25](#).



Note

When creating a *package.cab* file that is larger than 2GB, additional *.cab* files are created due to the size limit of the packer. The first package name is *package.cab*, the second is *package1.cab*, and so on, until the N package, *packageN.cab*, where N is the number of packages minus one. The files are saved in the same location that is specified before the packing begins. These files are not standalone and all of them must be sent to package. Problems with the packed file (*package.cab*) may arise if there is not enough hard-disk space.

Related Topics

[Configuring Service Logs, page 10-29](#)

Viewing and Downloading Reports

The starting point for viewing and downloading reports is the Reports page, which you access from **Reports and Activity in the navigation bar**. See [Reports Page Reference, page 10-44](#) for a list of all the reports that can be accessed from this page.



Note

The RDBMS Synchronization report and the Database Replication report are available only if those options are enabled in **Interface Configuration > Advanced Options**.

These topics describe how to view reports in the ACS web interface, and how to download reports:

- [Viewing and Downloading CSV Reports, page 10-31](#)
- [Viewing Dynamic Administration Reports, page 10-34](#)

- [Viewing and Downloading Entitlement Reports, page 10-36](#)

Viewing and Downloading CSV Reports

These topics describe how to view and download ACS CSV reports:

- [CSV Log File Names, page 10-31](#)
- [Viewing a CSV Report, page 10-31](#)
- [Downloading a CSV Report, page 10-33](#)

CSV Log File Names

When you access a report in Reports and Activity, ACS lists the CSV files in chronological order, with the current CSV file at the top of the list. The current file is named *log.csv*, where *log* is the name of the log.

Older files are named as:

logyyyy-mm-dd.csv

where:

log is the name of the log.

yyyy is the year that the CSV file was started.

mm is the month that the CSV file was started, in numeric characters.

dd is the date that the CSV file was started.

For example, a Database Replication log file that was generated on October 13, 2002, would be named *Database Replication 2002-10-13.csv*.

Related Topics

- [Viewing a CSV Report, page 10-31](#)
- [Downloading a CSV Report, page 10-33](#)

Viewing a CSV Report

You can view the contents of CSV reports in the ACS web interface. You can sort the table by entries in the column, and you can filter CSV log reports.

Filtering criteria includes a regular expression, a time range, or both:

- Regular expression-based filtering checks that at least one of each column's value, per row, matches the provided regular expression. When you use regular-expression filtering, ACS traverses each column and displays only the rows that match the filtering criteria.
- You can use time-based filtering by specifying values for a Start Date & Time and an End Date & Time. Rows dated within the specified time range appear.

When you enter a regular expression and use time-based filtering as well, the report will include only the rows that match both criteria.

To view a CSV report:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
- Step 2** Click the name of the CSV report that you want to view.
On the right side of the browser, ACS lists the current CSV report filename and the filenames of any old CSV report files.
- Step 3** Click the CSV report filename whose contents you want to view.
If the CSV report file contains information, the information appears in the display area.
- Step 4** To check for newer information in the current CSV report, click **Refresh**.
- Step 5** Use the **Next** and **Previous** buttons to navigate forward and backward through the report pages.
- Step 6** To sort the table by entries in the column, in ascending or descending order. Click a column title once to sort the table by that column's entries in ascending order. Click the column a second time to sort the table by that column's entries in descending order.
- Step 7** To specify filtering criteria and apply the filter to the log file's content:
- In the **Regular Expression** text box enter a string value. The expression can be up to 100 characters long. See [Table 10-8](#) for Regular Expression characters and their syntax definitions.
 - In the **Start Date & Time** and **End Date & Time** text boxes, enter string values. The date and time format is *dd/mm/yyyy, hh:mm:ss* or *mm/dd/yyyy, hh:mm:ss* as defined in the ACS system configuration for the date format.
 - In the **Rows per Page** box choose the number of rows to display per page. (The default is 50.)
 - Click **Apply Filter**. The ACS web server will apply the specified filtering criteria to the report file and display the filtered results in the report's table.
 - Click **Clear Filter** to reset filtering parameters to their default values. Use this option to display the entire report unfiltered.
-

Table 10-8 *Regular Expression Syntax Definitions*

Character	Regular Expression Use
^	A caret (^) matches to the beginning of the string. Referred to as “begins with.” For example, ^A will match ABc , A123 , but not 1A234 . See the last table entry for another caret usage.
\$	The dollar sign (\$) matches the end of the string. Referred to as “ends with.” For example, yz\$ will match strings ending with xyz , 0123yz , but not 12yzA .
\	The backslash (\) matches a given string at any location. Referred to as “contains.” A backslash is also used for expressing 'special characters' in a given regular expression (For example, \+ will match against the plus sign (+), to differentiate from the plus sign (+) usage in regular expressions.
.	The dot (.) matches any character.
*	The asterisk (*) indicates that the character to the left of the asterisk in the expression should match for any number of instances (that is, 0 or more times).
+	The plus sign (+) is similar to the asterisk (*) but at least one match of the character should appear to the left of the plus sign (+) in the expression.

Table 10-8 *Regular Expression Syntax Definitions*

Character	Regular Expression Use
?	The question mark (?) matches the expression or character to its left 0 or 1 times.
	The pipe () allows the expression on either side of it to match the target string. For example, A a matches against A as well as a .
-	The hyphen (-) indicates a range of values. For example, a-z.
()	The parentheses are used for grouping of expressions and affect the order of pattern evaluation.
[]	Brackets ([]) enclosing a set of characters indicate that any of the enclosed characters may match the target character. Values in brackets can be one or more characters, or ranges. For example, [02468], [0-9].
[^	When a caret (^) immediately follows a left bracket ([), it excludes the remaining characters within brackets from matching the target string. For example, [^0-9] indicates that the target character is alpha rather than numeric.

Related Topics

- [CSV Log File Names, page 10-31](#)
- [Downloading a CSV Report, page 10-33](#)

Downloading a CSV Report

You can download the CSV file for any CSV report that you view in ACS.

After downloading a CSV log file, you can import it into spreadsheets by using most popular spreadsheet application software. Refer to your spreadsheet software documentation for instructions. You can also use a third-party reporting tool to manage report data. For example, aaa-reports! by Extraxi supports ACS.

To download a CSV report:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
 - Step 2** Click the name of the required CSV report.
On the right side of the browser, ACS lists the current CSV report filename and the filenames of any old CSV report files.
 - Step 3** Click the CSV report filename that you want to download.
If the CSV report file contains information, the information appears in the display area in the right pane.
 - Step 4** In the right pane of the browser, click **Download**.
The browser displays a dialog box for accepting and saving the CSV file.
 - Step 5** Choose a location where you want to save the CSV file, and click **Save** to save the file.
-

Related Topics

- [CSV Log File Names, page 10-31](#)
- [Viewing a CSV Report, page 10-31](#)

Viewing Dynamic Administration Reports

These topics describe how to view and use dynamic administration reports:

- [Viewing the Logged-in Users Report, page 10-34](#)
- [Viewing the Disabled Accounts Report, page 10-35](#)
- [Viewing the Appliance Status Report, page 10-35](#)

Viewing the Logged-in Users Report



Note

The Logged-In Users report might take up to 20 seconds to open. Specific user information might take up to several minutes to appear.

You can view the Logged-in Users report in the ACS web interface.



Note

This list of users is cleared and restarted anytime ACS services are restarted. This list contains the names of users who logged in since the last time ACS was started; unless the list has been purged manually.

From this report, you can instruct ACS to delete users who are logged in to a specific AAA client. When a user session terminates without a AAA client sending an accounting stop packet to ACS, the Logged-in Users Report continues to show the user. Deleting logged-in users from a AAA client ends the accounting for those user sessions.



Note

Deleting logged-in users terminates only the ACS accounting record of users who are logged in to a particular AAA client. It does not terminate active user sessions, nor does it affect user records.

To view the Logged-in Users report:

Step 1 In the navigation bar, click **Reports and Activity**.

Step 2 Click **Logged-in Users**.

The Select a AAA Client page displays the name of each AAA client, its IP address, and the number of users who are logged in through the AAA client. At the bottom of the table, the **All AAA Clients** entry shows the total number of users who are logged in.

Step 3 To see a list of all users who are logged in, click **All AAA Clients**.

Step 4 To see a list of users who are logged in through a particular AAA client, click the name of the AAA client.

For each list of users, ACS displays tabular information on all users who are logged in, including:

- Date and Time
- User
- Group
- Assigned IP
- Port
- Source AAA Client



Tip To print this list, click anywhere in the right window and print the window from your browser.

- Step 5** To sort the table by any column's entries, in ascending or descending order. Click a column title once to sort the table by the entries in that column in ascending order. Click the column a second time to sort the table by the entries in that column in descending order.
- Step 6** To purge users who are logged in through a particular AAA client:
- a. Click the name of the AAA client.
ACS displays a table of all users who are logged in through the AAA client. The Purge Logged in Users button appears below the table.
 - b. Click **Purge Logged in Users**.
ACS displays a message, which shows the number of users who are purged from the report and the IP address of the AAA client.
-

Viewing the Disabled Accounts Report

To view the Disabled Accounts report:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
- Step 2** Click **Disabled Accounts**.
The Select a user account to edit page displays disabled user accounts, the account status, and the group to which the user account is assigned.



Tip To print this list, click anywhere in the right window and print the window from your browser.

- Step 3** To edit a user account listed, in the User column, click the username.
ACS opens the user account for editing.
For more information about editing a user account, see [Basic User Setup Options, page 6-2](#).
-

Viewing the Appliance Status Report

To view the Appliance Status report:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
- Step 2** Click **Appliance Status Page**.
The Appliance Status report appears in the right pane of the browser.

**Tip**

To print this list, click anywhere in the right window and print the window from your browser.

Viewing and Downloading Entitlement Reports

You can download the CSV User Entitlement report file of mappings of users to groups. You can download a report of all administrators and their privileges as well as reports or privileges for each individual administrator. You can also view the reports for individual administrators in the ACS web interface.

To view and download entitlement reports:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
- Step 2** Click **Entitlement Reports**.
The Entitlement Reports page appears.
- Step 3** To download the User Entitlement report:
- Click **Download report for mappings of users to groups**.
The browser displays a dialog box for accepting and saving the CSV file.
 - Choose a location where you want to save the CSV file, and click **Save**.
- Step 4** To download the privilege report for all administrators:
- Click **Download Privilege Report for All Administrators**.
The browser displays a dialog box for accepting and saving the CSV file.
 - Choose a location where you want to save the CSV file, and click **Save**.
- Step 5** To view and download the privilege report for an individual administrator:
- Click **Privilege Report for *Admin***, where *Admin* is the name of the administrator account.
The report appears in the right pane of the browser.

**Tip**

To print this list, click anywhere in the right pane and print the window from your browser.

- To download the CSV log file, click **Download** in the right pane of the browser.
The browser displays a dialog box for accepting and saving the CSV file.
 - Choose a location where you want to save the CSV file, and click **Save**.
-

Update Packets in Accounting Logs

Whenever you configure ACS to record accounting data for user sessions, ACS records start and stop packets. If you want, you can configure ACS to record update packets, too. In addition to providing interim accounting information during a user session, update packets drive password-expiry messages via the ACS Authentication Agent. In this use, the update packets are called watchdog packets.

**Note**

To record update packets in ACS accounting logs, you must configure your AAA clients to send the update packets. For more information about configuring your AAA client to send update packets, refer to the documentation for your AAA clients.

- **Logging Update Packets Locally**—To log update packets according to the local ACS logging configuration, enable the Log Update/Watchdog Packets from this Access Server option for each AAA client in Network Configuration.

For more information on setting this option for a AAA client, see [Adding AAA Clients, page 3-12](#).

- **Logging Update Packets Remotely**—To log update packets on a remote logging server, enable the Log Update/Watchdog Packets from this remote AAA Server option for the remote server AAA Server table entry on the local ACS.

For more information on setting this option for a AAA server, see [Adding AAA Servers, page 3-17](#).

Logging Configuration Pages Reference

The following topics describe the logging configuration pages.

- [Logging Configuration Page, page 10-37](#)
- [Critical Loggers Configuration Page, page 10-38](#)
- [Remote Logging Setup Page, page 10-39](#)
- [Remote Agents Reports Configuration Page \(ACS SE only\), page 10-39](#)
- [CSV log File Configuration Page, page 10-40](#)
- [Syslog log Configuration Page, page 10-41](#)
- [ODBC log Configuration Page \(ACS for Windows only\), page 10-42](#)

Logging Configuration Page

The Logging Configuration page is the starting point for configuring loggers and individual logs.

To open this page, choose **System Configuration > Logging**.

Table 10-9 *Logging Configuration Page*

Option	Description
Critical Loggers Configuration	Opens the Critical Loggers Configuration Page, page 10-38 , in which you can configure <i>critical loggers</i> when ACS records accounting messages to multiple loggers.
Remote Logging Services Configuration	Opens the Remote Logging Setup Page, page 10-39 , to configure remote loggers.
Remote Agent Reports Configuration (ACS SE only)	Opens the Remote Agents Reports Configuration Page (ACS SE only), page 10-39 , to configure the log content and file management of logs on the remote agent.
ACS Reports table	Displays which logs are enabled. The Configure links open the individual configuration page for each log: <ul style="list-style-type: none"> • CSV log File Configuration Page, page 10-40 • Syslog log Configuration Page, page 10-41 • ODBC log Configuration Page (ACS for Windows only), page 10-42

Related Topics

- [Configuring ACS Logs, page 10-22](#)
- [Remote Logging for ACS for Windows, page 10-10](#)
- [Remote Logging for ACS SE with ACS Remote Agents, page 10-10](#)

Critical Loggers Configuration Page

Use the Critical Loggers Configuration page to configure *critical loggers* for accounting logs to guarantee delivery of these logs to at least one logger.

To open this page, choose **System Configuration > Logging**. In the Logging Configuration Page, click the **Critical Loggers Configuration** link.

Table 10-10 *Critical Loggers Configuration Page*

Option	Description
RADIUS accounting critical logger	Specifies the critical logger for RADIUS accounting logs.
TACACS+ accounting critical logger	Specifies the critical logger for TACACS+ accounting logs.
VoIP accounting critical logger	Specifies the critical logger for VoIP accounting logs.

**Note**

We do not recommend that you configure a syslog logger as a critical logger; because, according to syslog standards, syslog message logging is not guaranteed.

Related Topics

[Configuring Critical Loggers, page 10-23](#)

Remote Logging Setup Page

Use the Remote Logging Setup page to configure to which remote loggers to send logs from the local ACS.

To open this page, choose **System Configuration > Logging**. In the Logging Configuration Page, click the Remote Logging Servers Configuration link.

Table 10-11 Remote Logging Setup Page

Option	Description
Do not log remotely	Disables logging to remote loggers.
Log to all selected remote log services	Sends logging data to all remote loggers in the Selected Log Services list.
Log to subsequent remote log services on failure	Sends logging information for this ACS server to one remote logger. ACS logs to the first accessible remote logger in the Selected Log Services list. Use this option when you want to configure ACS to send logging data to the next remote logger in the Selected Log Services list only if the first remote logger fails.
Log Services lists	These lists contain the ACS servers that are configured in the AAA Services table. The right (->) and left (<-) arrow buttons add and remove logging services to and from the Selected Log Services list. The Up and Down buttons order the logging services in the Selected Log Services list.

Related Topics

- [Remote Logging for ACS for Windows, page 10-10](#)
- [Remote Logging for ACS SE with ACS Remote Agents, page 10-10](#)

Remote Agents Reports Configuration Page (ACS SE only)

Use the Remote Agent Reports Configuration page on the ACS SE that the remote agent is configured to use as its configuration provider, to configure log content and log file management for all logs recorded on the remote agent.

To open this page, choose **System Configuration > Logging**. In the Logging Configuration Page, click the Remote Agent Reports Configuration link.

Table 10-12 Logging Configuration Page

Option	Description
Remote Logging Reports table	Displays which logs are enabled for the remote agent. The Configure links open the individual configuration page for each log.

Related Topics

[Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#)

CSV *log* File Configuration Page

Use the CSV *log* File Configuration page to enable logging to an individual local or remote CSV logger, and configure the content and file management of that log.

To open this page, choose **System Configuration > Logging**. In the Reports Configurations tables, click **Configure** for a log in the CSV column.

For an ACS SE configuration provider, to enable remote logging to a remote agent, click **Remote Agent Reports Configuration**, then click **Configure** for a log.



Note

For ACS SE, there are no configurable options for local CSV Audit logs.

Table 10-13 CSV *log* File Configuration Page

Option	Description
Enable Logging	Contains the option to enable or disable the log.
Log to CSV <i>log</i> report check box	Enables or disables logging to the selected logger. Note This check box is grayed out for CSV Audit logs, which are always enabled.
Configure Log Content (AAA-related reports only)	Contains the options to specify which attributes will be logged.
Select Columns to Log	The Attribute list contain attributes that have not been selected for logging. The Logged Attributes list contains attributes that have been selected for logging. The right (->) and left (<-) arrow buttons add and remove attributes to and from the Logged Attributes list. The Up and down buttons order the attributes in the Logged Attributes list.
Reset Columns button	Sets the attributes in the Logged Attributes list back to the default selections.
Log File Management (ACS for Windows and Remote Agent Reports configuration only)	Contains log file management options.
Generate New File	Specifies when ACS or the remote agent should generate a new CSV file: <ul style="list-style-type: none"> • Every day—At 12:01 A.M. local time every day. • Every week—At 12:01 A.M. local time every Sunday. • Every month—At 12:01 A.M. on the first day of every month. • When size is greater than <i>x</i> KB—When the current file reaches the size, which you enter in kilobytes, in the X box.
Directory	The directory to which ACS or the remote agent writes the CSV log file. We recommend that you specify the full path including drive letter, otherwise the file location will be relative to the installation directory. If the remote agent server uses Sun Solaris, the path must begin at the root directory, such as <i>/usr/data/acs-logs</i> .
Manage Directory	Manages which CSV files are retained.

Table 10-13 CSV log File Configuration Page (continued)

Option	Description
Keep only the last X files	Limits the number of CSV files that are retained. Enter the maximum number of files you want to retain in the X box.
Delete files older than X days	Limits the age of the CSV files that are retained. Enter the number of days to retain a CSV file before deleting it.

Related Topics

- [Configuring a CSV Log, page 10-24](#)
- [Configuring the Remote Logging Server, page 10-26](#)
- [Configuring Remote Agent Logs on the Configuration Provider, page 10-28](#)

Syslog log Configuration Page

Use the Syslog *log* File Configuration page to enable logging to up to two syslog loggers, and configure the content of those logs.

To open this page, choose **System Configuration > Logging**. In the Reports Configurations tables, click **Configure** for a log in the Syslog column.

Table 10-14 Syslog log File Configuration Page

Option	Description
Enable Logging	Contains the option to enable or disable the log.
Log to syslog <i>log</i> report check box	Enables or disables logging to the selected logger. The default is disabled.
Configure Log Content (AAA-related reports only)	Contains the options to specify which attributes will be logged.
Select Columns to Log	<p>The Attribute list contain attributes that have not been selected for logging. The Logged Attributes list contains attributes that have been selected for logging.</p> <p>The right (->) and left (<-) arrow buttons add and remove attributes to and from the Logged Attributes list.</p> <p>The Up and down buttons order the attributes in the Logged Attributes list.</p>
Reset Columns button	Sets the attributes in the Logged Attributes list back to the default selections.
Syslog Servers	Contains options to configure up to two syslog logging servers.
IP	Specifies the IP addresses of the syslog servers.
Port	Specifies the ports of the syslog servers to which log messages will be sent.
Max message length (bytes)	<p>Specifies the maximum message length of syslog messages, in bytes. The default length, which is the recommended length for a standard syslog server, is 1024 bytes. If the syslog is used as a proxy you can reduce the message length to allow some room for the proxy headers.</p> <p>The minimum value allowed is 200 bytes.</p>

Related Topics

- [Configuring Syslog Logging, page 10-24](#)
- [Configuring the Remote Logging Server, page 10-26](#)

ODBC *log* Configuration Page (ACS for Windows only)

Use the ODBC *log* Configuration page to enable logging to an individual ODBC logger, and configure the content and connection settings for ACS to the ODBC database.

To open this page, choose **System Configuration > Logging**. In the Reports Configurations tables, click the icon by the name of a log in the ODBC column.

Table 10-15 ODBC *log* Configuration Page

Option	Description
Enable Logging	Contains the option to enable or disable the log.
Log to ODBC <i>log</i> report check box	Enables or disables logging to the selected logger. The default is disabled.
Configure Log Content (AAA-related reports only)	Contains the options to specify which attributes will be logged.
Select Columns to Log	<p>The Attribute list contain attributes that have not been selected for logging. The Logged Attributes list contains attributes that have been selected for logging.</p> <p>The right (->) and left (<-) arrow buttons add and remove attributes to and from the Logged Attributes list.</p> <p>The Up and down buttons order the attributes in the Logged Attributes list.</p>
Reset Columns button	Sets the attributes in the Logged Attributes list back to the default selections,
ODBC Connection Settings	Contains options for ACS to communicate with the ODBC database.
Data Source list	The system DSN that you created to allow ACS to send ODBC logging data to your relational database.
Username	<p>The username of a user account in your relational database (up to 80 characters).</p> <p>Note The user must have sufficient privileges in the relational database to write the ODBC logging data to the appropriate table.</p>
Password	The password (up to 80 characters) for the specified relational database user account
Table Name	The name (up to 80 characters) of the table to which you want ODBC logging data appended.

Table 10-15 ODBC log Configuration Page (continued)

Option	Description
Create Table Statement	Contains the option to display a SQL create table statement.
Show Create Table button	<p>Displays a SQL create table statement for Microsoft SQL Server. The statement appears in the right panel of the ACS window.</p> <p>The table name is the name that is specified in the Table Name field. The column names are the attributes that are specified in the Logged Attributes list.</p> <p>Note The generated SQL is valid for Microsoft SQL Server only. If you are using another relational database, refer to your relational database documentation for information about writing a command to create a table.</p>

Related Topics

- [Configuring an ODBC Log \(ACS for Windows only\), page 10-25](#)
- [Configuring the Remote Logging Server, page 10-26](#)

Service Control Page Reference

Use the Services Log File Configuration page to enable or disable logging of services logs, and configure the detail and file management of that log.

To open this page, choose **System Configuration > Service Control**.

You must click the Restart button for these options to take effect.

Table 10-16 Services Log File Configuration Page

Option	Description
Cisco Secure ACS on <server>	Displays whether ACS services are running or stopped.
Services Log File Configuration	Contains options to enable, disable, and configure logging of services.
Level of Detail	<p>Disables logging, or sets the level of logging:</p> <ul style="list-style-type: none"> • None—No log file is generated. • Low—Only start and stop actions are logged. This is the default setting. • Full—All services actions are logged. Use this option when collecting data for customer support. This option provides customer support with enough data to research potential issues. Ensure that you have sufficient disk space to handle your log entries.
Log File Management (ACS for Windows only)	Contains log file management options.

Table 10-16 *Services Log File Configuration Page (continued)*

Option	Description
Generate New File	Select when ACS or the remote agent should generate a new CSV file: <ul style="list-style-type: none"> • Every day—At 12:01 A.M. local time every day. • Every week—At 12:01 A.M. local time every Sunday. • Every month—At 12:01 A.M. on the first day of every month. • When size is greater than <i>x</i> KB—When the current file reaches the size, that you enter, in kilobytes, in the <i>X</i> box.
Manage Directory	Check to manage which CSV files are retained.
Keep only the last <i>X</i> files	Select to limit the number of CSV files that are retained. Enter the maximum number of files to retain in the <i>X</i> box.
Delete files older than <i>X</i> days	Select to limit the age of the CSV files that are retained. Enter the number of days to retain a CSV file before deleting it.

Related Topics

[Configuring Service Logs, page 10-29](#)

Reports Page Reference

Use this page to access and download ACS CSV reports.

To open this page, click **Reports and Activity** in the navigation bar.

Table 10-17 *Reports Page*

Option	Description
TACACS+ Accounting Reports	Displays TACACS+ accounting reports, which contain a record of all successful authentications for the applicable item during the period that the report covers.
TACACS+ Administration Reports	Displays TACACS+ Administration reports, which contain all TACACS+ commands requested during the period that the report covers. This information is typically used when you use ACS to manage access to routers.
RADIUS Accounting Report	Displays RADIUS accounting reports, which contain a record of all successful authentications for the applicable item during the period that the report covers.
VoIP Accounting Reports	Displays VoIP accounting reports, which contain a record of all successful authentications for the applicable item during the period that the report covers.
Passed Authentications	Displays Passed Authentications reports, which list successful authentications during the period that the report covers.
Failed Attempts	Displays the Failed Attempts reports, which contain a record of all unsuccessful authentications during the period that the report covers for TACACS+ and RADIUS. The reports capture the username attempted, time and date, and cause of failure.

Table 10-17 *Reports Page (continued)*

Option	Description
Logged-in Users	Displays all users currently logged in, grouped by AAA client. You can delete logged-in users from specific AAA clients or from all AAA clients.
Disabled Accounts	Displays accounts that have been disabled.
ACS Backup and Restore	Displays ACS Backup and Restore reports, which list dates and times that the ACS system information was backed up and restored and whether the action was successful.
RDBMS Synchronization	Displays RDBMS Synchronization reports, which contain the times the RDBMS database was synchronized and whether synchronization was manual or scheduled. This report is available only if you enable this option in the Interface Configuration > Advanced Options page.
Database Replication	Displays Database Replication reports, which contain the times the ACS Internal Database was replicated to the backup server and whether replication was manual or scheduled. This report is available only if you enable this option in the Interface Configuration > Advanced Options page.
Administration Audit	Displays Administration Audit reports, which contain a list of the administrators who accessed ACS on the applicable date, the actions they made or attempted to make, and the time of the action. Examples of actions logged include starting and stopping the administration session, editing user and group data, and changing the network configuration.
User Password Changes	Displays User Password Changes reports, which contain information about user-initiated changes to passwords stored in the ACS internal database.
ACS Service Monitoring	Displays ACS Service Monitoring reports, which contain a log of the events that ACS encounters when it attempts to monitor services, such as CSAdmin. This information includes events for the Active Service Monitor, CSMon, which is a service.
Entitlement Reports	Lists the available user and administrator entitlement reports. The user entitlement report lists all users with their group, Network Access Profile (NAP) if relevant, and the mapping type (static or dynamic). the administrator entitlement reports lists privileges of administrators.
Appliance Status Page (ACS SE only)	Displays current statistics about hardware resource usage with information about the IP network configuration and network interface card of the ACS appliance.
Appliance Administration Audit (ACS SE only)	Displays Appliance Administration Audit reports, which contain a list of activity on the serial console of the ACS appliance. It records when the appliance administrator account is used to log in, the commands issued during the serial console session, and when the administrator logs out, ending the session.

Related Topics

- [About ACS Logs and Reports, page 10-1](#)
- [Viewing and Downloading Reports, page 10-30](#)

Audit Log Attributes

Table 10-18 lists the attributes that are monitored in ACS and specify administrative user actions for editing fields in the user page.

Table 10-18 **Audit Log Attributes**

Code	Editing Field
1	Account_Disabled
2	Real_Name
3	Description
4	Password_Authentication
5	PAP_Passowrd
6	Separate_PWD_For_CHAP
7	CHAP_Password
8	User_Group
9	Callback_setting
10	Client_IP_ADDR_Assignment
11	Selected_Pools
12	Shared_NAR
13	Selected_NARs
14	PerUser_NAR
15	Per_User_Def_Net_Access_Restriction_Table
16	CLI/DNIS-based_Access_Restrictions
17	CLI/DNIS-based_Access_Restrictions_Table
18	MAX_Sessions
19	User_Usage_Quotas
20	reset_Usage_Counters
21	Advanced_Account_Disable_options
22	Time_Bound_Alternate_Group
23	DownloadableACL
24	Tacacs+Enable_Control
25	AssociationTable
26	Tacacs+Enable_Passwd_settings
27	Tacacs+Passwd
28	Tacacs+OutBoundPasswd
29	Tacacs+Settings_PPP_IP
30	Tacacs+Settings_Custom_Attr_PPP_IP
31	Tacacs+Settings_PPP_IPX
32	Tacacs+Settings_Custom_Attr_PPP_IPX

Table 10-18 **Audit Log Attributes**

33	Tacacs+Settings_PPP_Multilink
34	Tacacs+Settings_Custom_Attr_PPP_MultiLink
35	Tacacs+Settings_PPP_Apple_Talk
36	Tacacs+Settings_Custom_Attr_PPP_Apple_Talk
37	Tacacs+Settings_PPP_VPDN
38	Tacacs+Settings_Custom_Attr_PPP_VPDN
39	Tacacs+Settings_PPP_LCP
40	Tacacs+Settings_Custom_Attr_PPP_LCP
41	Tacacs+Settings_ARAP
42	Tacacs+Settings_Custom_Attr_ARAP
43	Tacacs+Settings_Shell_exec
44	Tacacs+Settings_Custom_shell_exec
45	Tacacs+Settings_PIXShell
46	Tacacs+Settings_PIXShell_Custom_Attributes
47	Tacacs+Settings_Slip
48	Tacacs+Settings_Slip_Custom_Attributes
49	Tacacs+Settings_shell_cmd_Auth_Set
50	Shell_Cmd_Auth_Set_Table
51	Per_User_Command_Authorization
52	PIX/ASA_Command_Authorization
53	PIX/ASA_Command_Authorization_Table
54	Tacacs+UnknownServices
55	IETF_RADIUS_Attributes_Service_Type
56	IETF_RADIUS_Attributes_Framed_Protocol
57	IETF_RADIUS_Attributes_Framed-IP-Netmask
58	IETF_RADIUS_Attributes_Framed-Routing
59	IETF_RADIUS_Attributes_Filter-ID
60	IETF_RADIUS_Attributes_Framed-MTU
61	IETF_RADIUS_Attributes_Framed-Compression
62	IETF_RADIUS_Attributes_Login-IP-Host
63	IETF_RADIUS_Attributes_Login-Service
64	IETF_Radius_Attributes_Login-TCP-Port
65	IETF_RADIUS_Attributes_Reply-Message
66	IETF_RADIUS_Attributes_CallBack-ID
67	IETF_RADIUS_Attributes_Framed-Route
68	IETF_RADIUS_Attributes_Framed-IPX-Network
69	IETF_RADIUS_Attributes_State

Table 10-18 *Audit Log Attributes*

70	IETF_RADIUS_Attributes_Class
71	IETF_RADIUS_Attributes_Session-Timeout
72	IETF_RADIUS_Attributes_Termination-Action
73	IETF_RADIUS_Attributes_Proxy-State
74	IETF_RADIUS_Attributes_Login-LAT-Service
75	IETF_RADIUS_Attributes_Login-LAT-Node
76	IETF_RADIUS_Attributes_Login-LAT-Group
77	IETF_RADIUS_Attributes_Framed-AppleTalk-Link
78	IETF_RADIUS_Attributes_Framed-AppleTalk-Network
79	IETF_RADIUS_Attributes_Framed-AppleTalk-Zone
80	IETF_RADIUS_Attributes_Port-Limit
81	IETF_RADIUS_Attributes_Login-LAT-Port
82	IETF_RADIUS_Attributes_Tunnel-Type
83	IETF_RADIUS_Attributes_Tunnel-Medium-Type
84	IETF_RADIUS_Attributes_Tunnel-Client-Endpoint
85	IETF_RADIUS_Attributes_Tunnel-Server-Endpoint
86	IETF_RADIUS_Attributes_Tunnel-Password
87	IETF_RADIUS_Attributes_ARAP-Features
88	IETF_RADIUS_Attributes_ARAP-Zone-Access
89	IETF_RADIUS_Attributes_Configuration-Token
90	IETF_RADIUS_Attributes_Tunnel-Private-Group-ID
91	IETF_RADIUS_Attributes_Tunnel-Assignment-ID
92	IETF_RADIUS_Attributes_Tunnel-Preference
93	IETF_RADIUS_Attributes_Acct-Interim-Interval
94	IETF_RADIUS_Attributes_Tunnel-Client-Auth-ID
95	IETF_RADIUS_Attributes_Tunnel-Server-Auth-ID



CHAPTER 11

Administrators and Administrative Policy

This chapter addresses the features in the Administration Control section of the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

This chapter contains:

- [Administrator Accounts, page 11-1](#)
- [Logging In, page 11-5](#)
- [Adding, Editing, and Deleting Accounts, page 11-6](#)
- [Configuring Policy Options, page 11-8](#)
- [Administration Control Pages Reference, page 11-10](#)

Administrator Accounts

Administrator accounts provide the only access to the ACS web interface.

This section contains:

- [About Administrator Accounts, page 11-1](#)
- [Privileges, page 11-2](#)
- [Group Access Privileges, page 11-3](#)
- [Password Expirations and Account Lockouts, page 11-3](#)
- [Support for Regulatory Compliance, page 11-4](#)

About Administrator Accounts

From the Administration Control page, you can link to pages that establish the names, passwords, and privileges for individual administrators or groups of administrators.

ACS administrator accounts are:

- Unique to ACS and not related to other accounts, such as Windows administrator accounts, ACS TACACS+ accounts, or any other ACS user accounts.
- Unrelated to external ACS users because ACS stores ACS administrator accounts in a separate internal database.

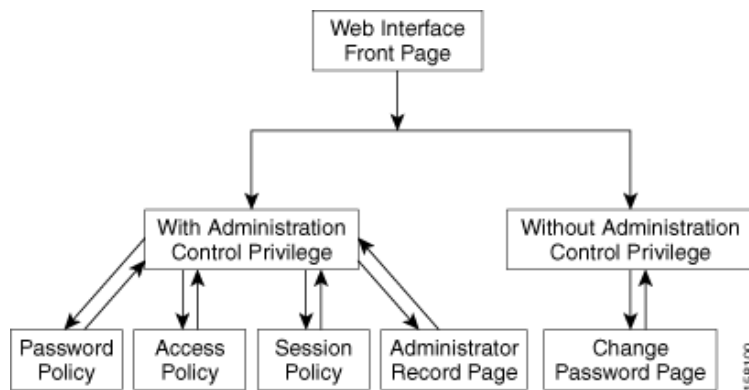
Privileges

The privileges that you grant to each administrator determine access to areas of the web interface. By default, new administrators do not have any privileges.

Administration Control Privilege

Administrators who have the Administration Control privilege can access the complete Administration Control page. For these administrators, this page provides management of administrators and access to pages that control administrative access policy. Restricted administrators can update their passwords. [Figure 11-1 on page 11-2](#) shows the access granted by the administration control privilege.

Figure 11-1 *The Administration Control Privilege*



Examples of privileges that you can grant to administrators or groups of administrators include:

- Shared profile components
- Network, system, and interface configuration
- Administration control
- External user databases, posture validation, and network access profiles (NAPs)
- Reports and activities

For example, you are an administrator with the Administration Control privilege who wants to configure access to the Network Configuration section of the web interface for administrators whose responsibilities include network management. Therefore, you check only the Network Configuration privilege for the applicable administrator accounts.

However, you might want to configure all privileges for an administrator or an administrative group. In this case, you click the Grant All (privileges) option.

The web interface also includes a filter that can control the type of access granted to administrators. For example, you can configure an administrator for read-only access to groups of users, or you can grant them add and edit access to the same groups.



Note

See [Chapter 10, “Logs and Reports,”](#) for information on generating reports of privileges granted to administrators.

The Influence of Policy

The Administration Control page also includes links to access, session, and password policy configuration pages. These policies influence all account logins and include the following configuration options:

- **Access Policy**—IP address limitations, HTTP port restrictions, and secure socket layer (SSL) setup.
- **Session Policy**—Timeouts, automatic local logins, and response to invalid IP address connections.
- **Password Policy**—Password validation, lifetime, inactivity, and incorrect attempts.

Group Access Privileges

ACS includes options that determine the type of administrator access to groups or users in groups. When enabled, these options grant an administrator the following privileges with respect to any available group:

- Add or edit user pages
- Edit group pages
- Read access to user pages
- Read access to the group pages

Table 11-1 describes the interaction of the options:

Table 11-1 *Group Access Options*

Add and Edit Access	Read Access	Result
No	No	Administrators cannot view the users in the Editable groups.
No	Yes	Administrators can view the users in the Editable groups, but Submit is not available.
Yes	No	Full access granted in either case. When enabled, Add/Edit Users in these groups overrides Read Access.
Yes	Yes	

Password Expirations and Account Lockouts

Successful logins take administrators to the main ACS web interface page. However, all logins are subject to the restrictions that have been configured in Administration Control, including expiration, account lockout, and password configuration options.

Limits set for password lifetime and password inactivity can force password change or account lockout. In addition, the limit set for failed attempts can force password change, and privileged administrators can manually lock accounts. In the case of an account lockout, a privileged administrator must unlock the account.

ACS includes the Account Never Expires option that can globally override automatic account lockouts and password configuration options. If the Account Never Expires option is enabled for a specific administrator, all administrator lockout options are ignored.

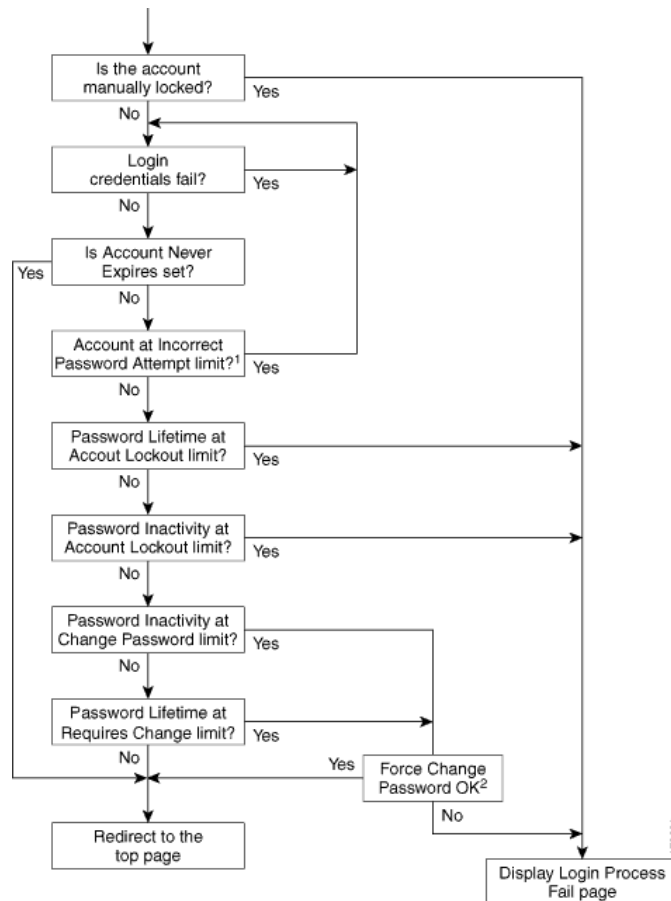
In the case of an account lockout, ACS displays the Login Process Fail page. Depending on the options, ACS displays the following pages for changing passwords:

- A password update page appears when you attempt to log in.

- The Change Password page appears when you click the Administration Control button in the navigation bar, if you do not have the Administration Control privilege. The Change Password page includes a list of the password criteria.

Figure 11-2 on page 11-4 shows the process flow at login time.

Figure 11-2 Login Process Flow



¹ When the administrator reaches the Incorrect Password Attempts limit, ACS locks the account. At this point, successful attempts will fail. However, if Account Never Expires is set, then the account cannot be locked out.

² The administrator has successfully logged in. Therefore, if only the password has been incorrectly used, ACS allows retries even though the administrator has exceeded the Incorrect Password Attempt limit.

Support for Regulatory Compliance

ACS includes options that can support regulatory compliance. For example, an administrator with the Administration Control privilege can decide whether to grant the Administration Control privilege to other administrators. Administrators who do not have this privilege cannot access the administrator configuration details.

All administrator logins are subject to the policy that you configure for passwords and accounts, unless you check the **Account Never Expires** option. For example, ACS provides configurable limits on password lifetime, activity, and incorrect password attempts. These options can force password change and can result in automatic account lockout. Privileged administrators can also lock out an account. In addition, you can monitor the last password change and last account activity for each administrator.

In addition, you can restrict access to reports. For example, you can enable or disable an administrator's ability to change the Administration Audit report configuration.

You can also configure administrator access to user groups. You can selectively choose to allow administrators to setup groups and add or edit users. ACS also provides configuration of administrator read access to users and groups.

Logging In

The ACS login page is the access point for the web interface. If your valid password expires, or if a change in policy affects a password, ACS forces you to change your password when you log in. If you are locked out, contact an administrator who has the Administration Control privilege.



Note

Administrators must have a Windows domain administrator account in order to log in and manage ACS services. However, Windows domain administrators cannot log in to ACS. Only administrators with valid ACS accounts can log in to ACS. For information, see the *Installation Guide for Cisco Secure ACS for Windows Release 4.2* or the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

ACS for Windows

To log in from a client, you must have an administrator account. However, the Session Policy includes an Allow automatic local login option. If this option is enabled, you can bypass the login page on the server that is running ACS. This option is available for unintentional lockouts. For more information about automatic local logins, see [Configuring Session Policy, page 11-8](#).

ACS SE

To access the ACS web interface from a browser, log in to ACS by using an administrator account.

The first administrator to log in must create an administrator name and password by using the **Add ACS Admin** command in the command line interface (CLI) to create the administrator name and password for the first account. For complete information on the CLI, see the “Administering Cisco Secure ACS Solution Engine” chapter of the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

In cases where ACS has locked out all administrators, use the **Unlock** *<administrator name>* command from the CLI. Only an administrator with the Administration Control privilege can use this command. For complete information on the CLI, see the “Administering Cisco Secure ACS Solution Engine” chapter of the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

To log in:

- Step 1** To start ACS, click the **ACS Admin** button in the Cisco Secure ACS program group.
The Cisco Secure ACS login page appears.
- Step 2** Type your Username and Password.
- Step 3** Click the **Login** button.

The Cisco Secure ACS main page appears.

Adding, Editing, and Deleting Accounts

Administrators with the Administration Control privilege can add, edit, and delete administrator accounts.

This section contains:

- [Adding or Editing Accounts](#)
- [Deleting an Account](#)

Adding or Editing Accounts

To add or edit an administrator account:

- Step 1** In the navigation bar, click **Administration Control**.
The [Administration Control Page](#) appears if the current account has the Administration Control privilege. Otherwise, a Change Password page appears.
- Step 2** Click **Add Administrator**, and the Add Administrator page appears; or, click the name of the administrator account that you want to edit and the Edit Administrator *administrator_name* page appears.
- Step 3** Type the Administrator Name, Password, and Password Confirmation for new accounts. If necessary, change the Password and Password Confirmation fields for an existing account. For information about these fields, see [Add Administrator and Edit Administrator Pages, page 11-11](#).
- Step 4** Check **Account Never Expires** to prevent the account for this administrator from expiring. For information, see [Add Administrator and Edit Administrator Pages, page 11-11](#).
- Step 5** Check the **Account Locked** check box to lock this account. If the **Account Locked** check box is checked, uncheck the box to unlock the account.
- Step 6** Click **Grant All** or **Revoke All** to globally add or remove all privileges. For information on these commands, see [Add Administrator and Edit Administrator Pages, page 11-11](#). Removing privileges from an existing account disables the account.
- Step 7** Move the group names between the Available groups and Editable groups list boxes. Groups in the Editable groups list, and associated users, will be available to the current administrator according to the access options that you check.
- Step 8** Check the appropriate options to grant access privileges to the Editable groups and associated users. For information on these options, see [Add Administrator and Edit Administrator Pages, page 11-11](#).
- Step 9** Check the appropriate options in the Shared Profile Components area to grant access to specific areas of the Shared Profile Components section of the web interface. For information on these options, see [Add Administrator and Edit Administrator Pages, page 11-11](#). For information on shared profile components, see [Chapter 4, “Shared Profile Components.”](#)
- Step 10** Check **Network Configuration** to grant access to the Network Configuration section of the web interface. For information on network configuration, see [Chapter 3, “Network Configuration.”](#)

- Step 11** Check options in the System Configuration area to grant access to pages in the System Configuration section of the web interface. For information on these options, see [Add Administrator and Edit Administrator Pages, page 11-11](#). For information on system configuration, see [Chapter 7, “System Configuration: Basic,”](#) [Chapter 8, “System Configuration: Advanced,”](#) and [Chapter 10, “Logs and Reports.”](#)
- Step 12** Check the **Interface Configuration** option to grant access to the Interface Configuration section of the web interface. For information on interface configuration, see [Chapter 2, “Using the Web Interface.”](#)
- Step 13** Check the **Administration Control** option to grant access to the Administration Control section of the web interface.
- Step 14** Check the **External User Databases** option to grant access to the External User Databases section of the web interface. For information on external user databases, see [Chapter 12, “User Databases.”](#)
- Step 15** Check the **Posture Validation** option to grant access to the Posture Validation section of the web interface. For information on posture validation, see [Chapter 13, “Posture Validation.”](#)
- Step 16** Check the **Network Access Profiles** option to grant access to the Network Access Profiles section of the web interface. For information on network access profiles, see [Chapter 14, “Network Access Profiles.”](#)
- Step 17** Check options in the **Reports and Activities** area to grant access to pages in the Reports and Activities section of the web interface. For information on these options, see [Add Administrator and Edit Administrator Pages, page 11-11](#). For information on reports, see [Chapter 10, “Logs and Reports.”](#)
- Step 18** Click **Submit**.
- ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control page.
-

Deleting an Account

You use this feature to delete administrator accounts. You can disable an account by clicking the **Revoke All** button. However, we recommend that you delete any unused administrator accounts.

To delete an account:

-
- Step 1** In the navigation bar, click **Administration Control**.
- ACS displays the Administration Control page.
- Step 2** Click the name of the administrator account that you want to delete.
- The Edit Administrator *administrator_name* page appears, where *administrator_name* is the name of the administrator account that you have selected.
- Step 3** Click the **Delete** button.
- ACS displays a confirmation dialog box.
- Step 4** Click **OK**.
- ACS deletes the administrator account. The Administrators list on the Administration Control page no longer contains the administrator account.
-

Configuring Policy Options

The options on these pages control access, session, and password policies.

This section contains the following options:

- [Configuring Access Policy, page 11-8](#)
- [Configuring Session Policy, page 11-8](#)
- [Configuring Password Policy, page 11-9](#)

Configuring Access Policy

If you have the Administration Control privilege, you can use the Access Policy feature to limit access by IP address and by the TCP port range used for administrative sessions. You can also enable the secure socket layer (SSL) for access to the web interface.

Before You Begin

If you want to enable the SSL for administrator access, you must have completed the steps in [Installing an ACS Server Certificate, page 9-22](#), and [Adding a Certificate Authority Certificate, page 9-26](#). After you have enabled SSL, ACS begins using the SSL at the next administrator login. This change does not affect current administrator sessions. In the absence of a certificate, ACS displays an error message when you attempt to configure SSL.

To set up an ACS Access Policy:

-
- | | |
|--------|--|
| Step 1 | In the navigation bar, click Administration Control .
ACS displays the Administration Control page. |
| Step 2 | Click Access Policy .
The Access Policy Setup page appears. |
| Step 3 | Click the appropriate IP Address Filtering option. For information on these options, see Access Policy Setup Page, page 11-18 . |
| Step 4 | Type the appropriate IP address ranges in accordance with the IP Address Filtering option. |
| Step 5 | Click the appropriate HTTP Port Allocation option to allow all ports or restrict access to certain ports. If you restrict access, type the range of the restricted ports. For information on these options, see Access Policy Setup Page, page 11-18 . |
| Step 6 | Check this option if you want ACS to use the SSL. For information on this option, see Access Policy Setup Page, page 11-18 . |
| Step 7 | Click Submit .
ACS saves and begins enforcing the access policy settings. |
-

Configuring Session Policy

If you have the Administration Control privilege, you can use the Session Policy controls that enable or disable:

- Local logins
- Responses to invalid IP address connections

To set up ACS session policy:

-
- Step 1** In the navigation bar, click **Administration Control**.
ACS displays the Administration Control page.
- Step 2** Click **Session Policy**.
The Session Policy Setup page appears.
- Step 3** Click the appropriate policies and type the appropriate information to set up the policy. For information on these options and fields, see [Session Policy Setup Page, page 11-20](#).
- Step 4** Click **Submit**.
ACS saves and begins enforcing the session policy settings.
-

Configuring Password Policy

You can access the Administrator Password Policy page from the Password Policy button on the Add Administrator page. If you do not configure the password policy, any administrator can log in, create administrators, and assign privileges.

The Administrator Password Policy provides controls that:

- Constrain complexity
- Restrict lifetime
- Restrict inactive accounts
- Limit incorrect login attempts

To set up a password policy:

-
- Step 1** In the navigation bar, click **Administration Control**.
ACS displays the Administration Control page.
- Step 2** Click **Password Policy**.
The Administrator Password Policy page appears.
- Step 3** Click the appropriate options and type the appropriate values. For information on these options and fields, see [Administrator Password Policy Page, page 11-16](#).
- Step 4** Click **Submit**.
ACS saves and begins enforcing the password policy settings at the next login.
-

Administration Control Pages Reference

The following topics describe the pages accessed from the **Administration Control** button on the navigation bar:

- [Administration Control Page, page 11-10](#)
- [Add Administrator and Edit Administrator Pages, page 11-11](#)
- [Administrator Password Policy Page, page 11-16](#)
- [Access Policy Setup Page, page 11-18](#)
- [Session Policy Setup Page, page 11-20](#)

Administration Control Page

The Administration Control page is the starting point for configuring administrator accounts and policies. Only administrators with the Administration Control privilege can access this page.

To open this page, click the **Administration Control** button in the navigation bar.

Table 11-2 *Administration Control (Privileged Administrator)*

Option	Description
Administrators	Lists all configured administrators.
<administrator_name>	Opens the Edit Administrator <administrator_name> page. For information, see the Add Administrator and Edit Administrator Pages, page 11-11 .
Add Administrator	Opens the Add Administrator page. For information, see the Add Administrator and Edit Administrator Pages, page 11-11 .
Access Policy	Opens the Access Policy Setup page, which controls network access for browsers. For information, see the Administrator Password Policy Page, page 11-16 .
Session Policy	Opens the Session Policy Setup page, which provides configuration details for HTTP sessions. For information, see the Session Policy Setup Page, page 11-20 .
Password Policy	Opens the Administrator Password Policy page. For information, see the Administrator Password Policy Page, page 11-16 .

Related Topics

- [Adding or Editing Accounts, page 11-6](#)
- [Deleting an Account, page 11-7](#)
- [Configuring Access Policy, page 11-8](#)
- [Configuring Session Policy, page 11-8](#)
- [Configuring Password Policy, page 11-9](#)

Add Administrator and Edit Administrator Pages

Use the areas on the Add Administrator and Edit Administrator pages to:

- Add an administrator (Add Administrator page only)
- Add, edit, and monitor passwords
- Monitor and re-enable locked out accounts
- Enable or disable privileges

To open these pages, click **Administration Control**, and then click **Add Administrator** or click `<administrator_name>` to edit an administrator.

Table 11-3 describes the following options:

- [Administrator Details, page 11-11](#)
- [Administrator Privileges, page 11-12](#)
- [User & Group Setup, page 11-12](#)
- [Shared Profile Components, page 11-13](#)
- [Network Configuration, page 11-14](#)
- [System Configuration, page 11-14](#)
- [Interface Configuration, page 11-15](#)
- [Administration Control, page 11-15](#)
- [External User Databases, page 11-15](#)
- [Posture Validation, page 11-15](#)
- [Network Access Profiles, page 11-15](#)
- [Reports & Activity, page 11-15](#)

Table 11-3 *Add Administrator and Edit Administrator Pages*

Option	Description
Administrator Details	
Administrator Name (appears only on the Add Administrator page)	<p>The login name for the ACS administrator account. Administrator names can contain 1 to 32 characters, excluding the left angle bracket (<), the right angle bracket (>), and the backslash (\). An ACS administrator name does not have to match a network user name.</p> <p>The administrator name does not appear on the Edit Administrator page because ACS does not allow name changes for previously configured administrators. To change names, delete the account and configure an account with a new name. To disable an account, revoke all privileges.</p>
Password	<p>The password can match the password that the administrator uses for dial-in authentication, or it can be a different password. ACS enforces the options in the Password Validation Options section on the Administrator Password Policy page.</p> <p>Passwords must be at least four characters long and contain at least one numeric character. The password cannot include the username or the reverse username, must not match any of the previous four passwords, and must be in ASCII characters. For errors in passwords, ACS displays the password criteria.</p> <p>If the password policy changes and the password does not change, the administrator remains logged in. ACS enforces the new password policy at the next login.</p>

Table 11-3 **Add Administrator and Edit Administrator Pages (continued)**

Option	Description
Confirm Password	Verifies the password in the Password field. For errors in password typing, ACS displays an error message.
Last Password Change (Edit Administrator page only)	Displays the date of the change on which a password changes through administrative action on this page or through expiration of a password during login. (Read-only) Always displays the change date, not the expiration date. Does not appear until a new account has been submitted.
Last Activity (Edit Administrator page only)	Displays the date of the last successful login. (Read-only) Does not appear until a new account has been submitted.
Account Never Expires	Prevents account lockout by overriding the lockout options on the Administrator Password Policy page with the exception of manual lockout. Therefore, the account never expires but password change policy remains in effect. The default value is unchecked (disabled).
Account Locked	<p>Prevents an administrator, who was locked out due to the lockout options on the Password Policy page, from logging in. When unchecked (disabled), this option unlocks an administrator who was locked out.</p> <p>Administrators who have the Administration Control privilege can use this option to manually lock out an account or reset locked accounts. The system displays a message that explains the reason for a lockout.</p> <p>When an administrator unlocks an account, ACS resets the Last Password Change and the Last Activity fields to the day on which the administrator unlocks the account.</p> <p>The reset of a locked account does not affect the configuration of the lockout and unlock mechanisms for failed attempts.</p>
Administrator Privileges	<p>Contains the privilege options for the User Setup and Group Setup sections of the web interface.</p> <p>By default, a remote administrator does not have privileges.</p>
Grant All	<p>Enables all privileges. ACS moves all user groups to the Editable Groups list. A privileged administrator can also grant privileges to each ACS administrator by assigning privileges on an individual basis. In either case, the administrator can individually override options enabled by Grant All.</p> <p>By default, ACS restricts all privileges for new administrator accounts.</p>
Revoke All	<p>Clears (restricts) all privileges. ACS removes all user groups from the Editable Groups list. Revoking all privileges for an existing account effectively disables the account. The administrator can individually override options disabled by Revoke All.</p> <p>You can also disable an account by revoking all privileges.</p>
User & Group Setup	
Add/Edit users in these groups	<p>Enables an administrator to add or edit users, and to assign users to the groups in the Editable groups list.</p> <p>When enabled, this setting overrides the settings in the Read access to users in these groups option.</p>
Setup of these groups	<p>Enables an administrator to edit the settings for the groups in the Editable groups list.</p> <p>When enabled, this setting overrides the settings in the Read access of these groups option.</p>

Table 11-3 **Add Administrator and Edit Administrator Pages (continued)**

Option	Description
Read access to users in these groups	<p>Enables read-only access to users in the Editable groups.</p> <p>When the Add/Edit users in these groups option is enabled, it overrides the settings in the Read access to users in these groups option.</p> <p>If the Add/Edit users in these groups option is checked (enabled), it does not matter if this setting is enabled or disabled. The Add/Edit users in these groups setting overrides this setting, and the administrator can edit all users in the Editable groups.</p> <p>If the Add/Edit users in these groups option is unchecked (disabled):</p> <ul style="list-style-type: none"> • Check this check box to grant the administrator read access to the users in the Editable groups. In this case, the administrator cannot submit changes. • When unchecked, administrators cannot view users.
Read access of these groups	<p>Enables read-only access to users in the Editable groups.</p> <p>When the Add/Edit users in these groups option is enabled, it overrides the settings in the Read access to users in these groups option.</p> <p>If the Add/Edit users in these groups option is checked (enabled), it does not matter if this setting is enabled or disabled. The Add/Edit users in these groups setting overrides this setting, and the administrator can edit the Editable groups.</p> <p>If the Add/Edit users in these groups option is unchecked (disabled):</p> <ul style="list-style-type: none"> • Check this check box to grant the administrator read access to the Editable groups list. In this case, the administrator cannot submit changes. • When unchecked, administrators cannot view groups.
Available groups	Lists all user groups. Administrators do not have access to the groups in this list.
Editable groups	<p>Lists the user groups to which administrators have access. Other options in the User & Group Setup area determine the limits on administrator access to these groups and associated users in this list.</p> <p>Click >> to add all groups, or click << to remove all groups. Click > to add a single group, or click < to remove a single group.</p> <p>Note The access settings in this section do not apply to group mappings for external authenticators.</p>
Shared Profile Components	
Network Access Restriction Sets	Enables full access to the Network Access Restriction Sets feature.
Network Access Filtering Sets	Enables full access to the Network Access Filtering Sets feature.
Downloadable ACLs	Enables full access to the Downloadable PIX ACLs feature.
RADIUS Authorization Components	Enables full access to RACs.
Create new Device Command Set Type	Allows the administrator account to be used as valid credentials by another Cisco application for adding new device command set types. New device command set types that are added to ACS by using this privilege appear in the Shared Profile Components section of the web interface.

Table 11-3 Add Administrator and Edit Administrator Pages (continued)

Option	Description
Shell Command Authorization Sets	Enables full access to the Shell Command Authorization Sets feature.
PIX/ASA Command Authorization Sets	Enables full access to the PIX/ASA Command Authorization Sets feature. Note Additional command authorization set privilege options can appear if other Cisco network management applications, such as CiscoWorks, have updated the configuration of ACS.
Network Configuration	Enables full access to the features in the Network Configuration section of the web interface.
System Configuration	Contains the privilege options for the features in the System Configuration section of the web interface. For each of the features, enabling the option grants full access to the feature.
Service Control	Enables access to configuration of the service log files, and stop and restart of ACS services.
Date/Time Format Control	Enables access to control of date formats.
Logging Control	Enables access to report options associated with the Logging Configuration page. To access the Logging Configuration page, click System Configuration , then click Logging .
Administration Audit Configuration	Enables this administrator to change the Administration Audit report configuration.
Password Change Configuration	Enables this administrator to change the Password Change report configuration.
Password Validation	Enables access to validation parameters for user passwords.
DB Replication	Enables access to ACS internal database replication.
RDBMS Synchronization	Enables access to RDBMS synchronization.
IP Pool Address Recovery	Enables access to IP pool address recovery.
IP Pool Server Configuration	Enables access to the configuration of IP pools.
ACS Backup	Enables access to ACS backup.
ACS Restore	Enables access to ACS restore.
ACS Service Management	Enables access to system monitoring and event logging.
VoIP Accounting Configuration	Enables access to the VoIP accounting configuration.
ACS Certificate Setup	Enables access to ACS certificate setup.
Global Authentication Setup	Grants privilege for global authentication setup. Any administrator who requires access to the EAP-FAST Files Generation configuration page must have the Global Authentication Setup privilege enabled.
EAP-FAST PAC Files Generation (ACS SE)	Enable generation of PAC files for use with EAP-FAST authentication.
NAC Attributes management (ACS SE)	Enables access to NAC attribute management.
Appliance Configuration (ACS SE)	Enables access to appliance configuration.
Support Operations (ACS SE)	Enables access to support operations.

Table 11-3 Add Administrator and Edit Administrator Pages (continued)

Option	Description
View Diagnostic Logs (ACS SE)	Enables access to diagnostic logs.
Appliance Upgrade Status (ACS SE)	Enables access to appliance upgrade status reports.
Interface Configuration	Enables full access to the features in the Interface Configuration section of the web interface.
Administration Control	Enables full access to the features in the Administration Control section of the web interface.
External User Databases	Enables full access to the features in the External User Databases section of the web interface.
Posture Validation	Enables access to Network Admission Control (NAC) configuration.
Network Access Profiles	Enables access to service-based policy configuration by using NAPs.
Reports & Activity	Click the Reports and Activities button in the navigation bar to access these logs.
TACACS+ Accounting	Enables access to the TACACS+ Accounting log, which includes TACACS+ session information.
TACACS+ Administration	Enables access to the TACACS+ Administration log, which lists configuration commands.
RADIUS Accounting	Enables access to the RADIUS Accounting log, which includes RADIUS session information.
VoIP Accounting	Enables access to the VoIP Accounting log, which includes VoIP session information.
Passed Authentications	Enables access to the Passed Authentications log, which lists successful authentication requests.
Failed Attempts	Enables access to the Failed Attempts log, which lists authentication and authorization failures.
Logged-in Users	Enables access to the Logged-in Users log, which lists all users that receive services from AAA clients.
Purge of Logged-in Users	If users are listed as logged in but the connection to the AAA client has been lost and the users are no longer actually logged in, click Purge and that session's activity will be terminated. Purging the user from this list does not log the user off the AAA client, but terminates the session record in accounting. To print this list, right-click anywhere in the right window and print the window from the browser.
Disabled Accounts	Enables access to the Disabled Accounts log, which lists all disabled user accounts.
ACS Backup and Restore	Enables access to the ACS Backup and Restore log, which lists backup and restore activity.
DB Replication	Enables access to the Database Replication log, which lists database replication activity.
RDBMS Synchronization	Enables access to the RDBMS Synchronization log, which lists RDBMS synchronization activity.
Administration Audit	Enables access to the Administration Audit log, which lists system administrator actions.
ACS Service Monitor	Enables access to the ACS Service Monitoring log, which lists ACS service starts and stops.
User Change Password	Enables access to the User Password Changes log, which lists user-initiated password changes.
Entitlement Reports	Enables access to reports of user and administrator entitlements.

Table 11-3 *Add Administrator and Edit Administrator Pages (continued)*

Option	Description
Appliance Status (ACS SE)	Enables access to the Appliance Status log, which logs resource utilization.
Appliance Administration Audit (ACS SE)	Enables access to the Appliance Administration Audit log, which lists activity on the serial console.

Related Topics

- [Service Control, page 7-1](#)
- [Date and Time Format Control, page 7-3](#)
- [Local Password Management, page 7-4](#)
- [ACS Backup, page 7-8](#)
- [ACS System Restore, page 7-14](#)
- [ACS Active Service Management, page 7-18](#)
- [VoIP Accounting Configuration, page 7-21](#)
- [Appliance Configuration \(ACS SE Only\), page 7-22](#)
- [Support Page, page 7-25](#)
- [Viewing or Downloading Diagnostic Logs \(ACS SE Only\), page 7-27](#)
- [ACS Internal Database Replication, page 8-1](#)
- [RDBMS Synchronization, page 8-17](#)
- [IP Pools Server, page 8-39](#)
- [IP Pools Address Recovery, page 8-44](#)
- [Global Authentication Setup, page 9-21](#)
- [ACS Certificate Setup, page 9-22](#)
- [NAC Attribute Management \(ACS SE Only\), page 8-44](#)
- [Appliance Configuration \(ACS SE Only\), page 7-22](#)
- [About ACS Logs and Reports, page 10-1](#)
- [Password Expirations and Account Lockouts, page 11-3](#)
- [Adding, Editing, and Deleting Accounts, page 11-6](#)

Administrator Password Policy Page

Use the Administrator Password Policy page to set password validation, lifetime, inactivity, and incorrect attempt options. If you do not configure the password policy, any administrator can log in, create administrators, and assign privileges.

To open this page, click **Administration Control** and then click **Password Policy**.

ACS returns an error when:

- The specification is out of range.

- Users do not meet the criteria on this page.

Table 11-4 describes the following options:

- [Password Validation Options, page 11-17](#)
- [Password Lifetime Options, page 11-17](#)
- [Password Inactivity Options, page 11-17](#)
- [Incorrect Password Attempt Options, page 11-18](#)

Table 11-4 Administrator Password Policy

Option	Description
Password Validation Options	
Password may not contain the username	If enabled, the password cannot contain the username or the reverse username.
Minimum length n characters	n specifies the minimum length of the password (the default is 4, the range is 4 to 20).
Password must contain:	Use these options to determine password complexity constraints.
upper case alphabetic characters	If enabled, the password must contain uppercase alphabetic characters.
lower case alphabetic characters	If enabled, the password must contain lowercase alphabetic characters.
numeric characters	If enabled, the password must contain numeric characters.
non alphanumeric characters	If enabled, the password must contain nonalphanumeric characters (for example, @).
Password must be different from the previous n versions	If enabled, the password must be different from the previous n versions (the default is 1, the range is 1 to 99).
Password Lifetime Options	
Following a change of password:	Use these options to set restrictions on the lifetime of administrator passwords. The value n represents the number of days that passed since the last time the password was changed.
The password will require change after n days	Following a change of password, if enabled, n specifies the number of days before ACS requires a change of password due to password age (the default is 30). The range is 1 to 365. When checked (enabled), The Administrator will be locked after n days option, causes ACS to compare the two Password Lifetime Options and take the greater value.
The Administrator will be locked out after n days	Following a change of password, if enabled, n specifies the number of days before ACS locks out the associated administrator account due to password age (the default is 60, the range is 1 to 365).
Password Inactivity Options	
Following last account activity:	Use these options to place restrictions on the use of inactive administrator accounts. The value n represents the number of days that passed since the activity (administrator login).

Table 11-4 Administrator Password Policy (continued)

Option	Description
The password will require change after n days	<p>Following the last account activity, if enabled, n specifies the number of days before ACS requires a change of password due to password inactivity (the default is 30). The range is 1 to 365. When checked (enabled), The Administrator will be locked after n days option causes ACS to compare the two Password Inactivity Options and take the greater value.</p> <p>Note For additional security, ACS does not warn users who are approaching the limit for password inactivity.</p>
The Administrator will be locked out after n days	<p>Following the last account activity, if enabled, n specifies the number of days before ACS locks out the associated administrator account due to password inactivity (the default is 60, the range is 1 to 365).</p> <p>Note For additional security, ACS does not warn users who are approaching the limit for account inactivity.</p>
Incorrect Password Attempt Options	
Lock out Administrator after n successive failed attempts	<p>If enabled, n specifies the allowable number of incorrect password attempts. When checked, n cannot be set to zero. If disabled (not checked), ACS allows unlimited successive failed login attempts (the default is 3, the range is 1 to 98).</p> <p>Note For additional security, ACS does not warn users who are approaching the limit for failed attempts. If the Account Never Expires option is enabled for a specific administrator, this option is ignored.</p>

Access Policy Setup Page

Use the Access Policy Setup page to configure access for IP addresses and ranges, to configure HTTP access, and to set up the Secure Sockets Layer (SSL).

To open the Access Policy Setup page, click **Administration Control**, and then click **Access Policy**.

Table 11-5 describes the following options:

- [IP Address Filtering, page 11-18](#)
- [IP Address Ranges, page 11-19](#)
- [HTTP Configuration, page 11-19](#)
- [Secure Socket Layer Setup, page 11-20](#)

Table 11-5 Access Policy Options

Option	Description
IP Address Filtering	
Allow all IP addresses to connect	Enables remote access to the web interface from any IP address.
Allow only listed IP addresses to connect	Restricts remote access to the web interface to IP addresses within the specified IP Address Ranges.

Table 11-5 **Access Policy Options** *(continued)*

Option	Description
Reject connections from listed IP addresses	<p>Restricts remote access to the web interface to IP addresses outside of the specified IP Address Ranges.</p> <p>IP filtering operates on the IP address received in an HTTP request from a remote administrator's web browser. If the browser is configured to use an HTTP proxy server or the browser runs on a workstation behind a network device performing network address translation, IP filtering applies only to the IP address of the HTTP proxy server or the NAT device.</p>
IP Address Ranges	<p>The IP Address Ranges table contains ten rows for configuring IP address ranges. The ranges are always inclusive; that is, the range includes the Start and End IP addresses.</p> <p>Use dotted-decimal format. The IP addresses that define a range must differ only in the last octet (Class C format).</p>
Start IP Address	Defines the lowest included IP address in the specified range (up to 16 characters).
End IP Address	Defines the highest included IP address in the specified range (up to 16 characters).
HTTP Configuration	
HTTP Port Allocation	
Allow any TCP ports to be used for Administration HTTP Access	Enables ACS to use any valid TCP port for remote access to the web interface.
Restrict Administration Sessions to the following port range From Port <i>n</i> to Port <i>n</i>	<p>Restricts the ports that ACS can use for remote access to the web interface. Use the boxes to specify the port range (up to five digits per box). The range is always inclusive; that is, the range includes the start and end port numbers. The size of the specified range determines the maximum number of concurrent administrative sessions.</p> <p>ACS uses port 2002 to start all administrative sessions. Port 2002 does not need to be in the port range. Also, ACS does not allow definition of an HTTP port range that consists only of port 2002. The port range must consist of at least one port other than port 2002.</p> <p>A firewall configured to permit HTTP traffic over the ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port that a web browser must address to initiate an administrative session.</p> <p>We do not recommend allowing administration of ACS from outside a firewall. If access to the web interface from outside a firewall is necessary, keep the HTTP port range as narrow as possible. A narrow range can help to prevent accidental discovery of an active administrative port by unauthorized users. An unauthorized user would have to impersonate, or “spoof,” the IP address of a legitimate host to make use of the active administrative session HTTP port.</p>

Table 11-5 *Access Policy Options (continued)*

Option	Description
Secure Socket Layer Setup	
Use HTTPS Transport for Administration Access	<p>Enables ACS to use the secure socket layer (SSL) protocol to encrypt HTTP traffic between the CSAdmin service and the web browser that accesses the web interface. This option enables encryption of all HTTP traffic between the browser and ACS, as reflected by the URLs, that begin with HTTPS. Most browsers include an indicator for SSL-encrypted connections.</p> <p>To enable SSL, first install an a server certificate and a certification authority certificate. Choose System Configuration > ACS Certificate Setup to access the installation process. With SSL enabled, ACS begins using HTTPS at the next administrator login. Current administrator sessions are unaffected. In the absence of a certificate, ACS displays an error.</p>

Related Topics

- [Installing an ACS Server Certificate, page 9-22](#)
- [Adding a Certificate Authority Certificate, page 9-26](#)

Session Policy Setup Page

Use the Session Policy Setup page to configure session attributes that include timeout, automatic local logins (ACS for Windows only), and response to invalid IP address connections.

To open this page, click **Administration Control**, and then click **Session Policy**.

[Table 11-6](#) describes the session configuration options.

Table 11-6 *Session Policy*

Option	Description
Session Configuration	
Session idle timeout (minutes)	<p>Specifies the time, in minutes, that an administrative session must remain idle before ACS terminates the connection (four-digit maximum, 5 to 1439).</p> <p>When an administrative session terminates, ACS displays a dialog box asking whether the administrator wants to continue. If the administrator chooses to continue, ACS starts a new administrative session.</p> <p>This parameter only applies to the ACS administrative session in the browser. It does not apply to an administrative dial-up session.</p>

Table 11-6 Session Policy (continued)

Option	Description
Allow Automatic Local Login (ACS for Windows)	<p>Enables administrators to start an administrative session without logging in, if they are using a browser on the computer that runs ACS. ACS uses a default administrator account named <code>local_login</code> to conduct these sessions.</p> <p>When unchecked (disabled), administrators must log in using administrator names and passwords.</p> <p>Note To prevent accidental lockout when there are no defined administrator accounts, ACS does not require an administrator name and password for local access to ACS.</p> <p>The <code>local_login</code> administrator account requires the Administration Control privilege. ACS records administrative sessions that use the <code>local_login</code> account in the Administrative Audit report under the <code>local_login</code> administrator name.</p>
Respond to invalid IP address connections	<p>Enables ACS to send an error message in response to attempts to start a remote administrative session by using an IP address that is invalid according to the IP address Range settings in the Access Policy. If this check box is clear, ACS does not display an error message when an invalid remote connection attempt is made. (the default is Enabled)</p> <p>Disabling this option can help to prevent unauthorized users from discovering ACS.</p>



CHAPTER 12

User Databases

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, authenticates users against one of several possible databases, including its internal database. You can configure ACS to authenticate users with more than one type of database. With this flexibility you can use user account data that is collected in different locations without having to explicitly import the users from each external user database into the ACS internal database. You can also apply different databases to different types of users, depending on the security requirements that are associated with user authorizations on your network. For example, a common configuration is to use a Windows user database for standard network users and a token server for network administrators. For information about authentication protocols and the external database types that support them, see [Authentication Protocol-Database Compatibility, page 1-8](#).



Note

For information about the Unknown User Policy and group mapping features, see [Chapter 15, “Unknown User Policy”](#) and [Chapter 16, “User Group Mapping and Specification.”](#)

This chapter contains:

- [ACS Internal Database, page 12-1](#)
- [About External User Databases, page 12-3](#)
- [Windows User Database, page 12-5](#)
- [Generic LDAP, page 12-23](#)
- [ODBC Database \(ACS for Windows Only\), page 12-35](#)
- [LEAP Proxy RADIUS Server Database \(Both Platforms\), page 12-48](#)
- [Token Server User Databases, page 12-50](#)
- [Deleting an External User Database Configuration, page 12-57](#)

ACS Internal Database

The ACS internal database is crucial for the authorization process. Regardless of whether a user is authenticated by the internal user database or by an external user database, ACS authorizes network services for users based on group membership and specific user settings in the ACS internal database. For information about the types of authentication that the ACS internal database supports, see [Authentication Protocol-Database Compatibility, page 1-8](#).

About the ACS Internal Database

For users who are authenticated by using the ACS internal database, ACS stores user passwords in a database which is protected by an administration password and encrypted by using the AES 128 algorithm. For users who are authenticated with external user databases, ACS does not store passwords in the ACS internal database.

Unless you have configured ACS to authenticate users with an external user database, ACS uses usernames and passwords in the ACS internal database during authentication. For more information about specifying an external user database for authentication of a user, see [Adding a Basic User Account, page 6-3](#).

User Import and Creation

The following facilities can import or create user accounts:

- **RDBMS Synchronization**—You can use RDBMS Synchronization to create large numbers of user accounts and configure many settings for user accounts. RDBMS also supports import of user accounts from external sources. We recommend that you use this feature whenever you need to import users by bulk; however, setting up RDBMS Synchronization for the first time requires several important decisions and time to implement them. For more information, see [RDBMS Synchronization, page 8-17](#).
- **CSUtil.exe (ACS for Windows)**—The **CSUtil.exe** command-line utility provides a simple means of creating basic user accounts. **CSUtil.exe** also supports import of user accounts from external sources. When compared to RDBMS Synchronization, its functionality is limited; however, it is simple to prepare for importing basic user accounts and assigning users to groups. For more information, see [Appendix C, “CSUtil Database Utility.”](#)

The following facilities can create user accounts:

- **ACS web interface**—The web interface provides the ability to create user accounts manually, one user at a time. Regardless of how a user account was created, you can edit a user account by using the web interface. For detailed steps, see [Adding a Basic User Account, page 6-3](#).
- **Unknown User Policy**—The Unknown User Policy enables ACS to add users automatically when it finds a user without an account in an external user database. The creation of a user account in ACS occurs only when the user attempts to access the network and is successfully authenticated by an external user database. For more information, see [Chapter 15, “Unknown User Policy.”](#)

If you use the Unknown User Policy, you can also configure group mappings so that each time a user who was added to ACS by the Unknown User Policy is authenticated, the user group assignment is made dynamically. For some external user database types, user group assignment is based on group membership in the external user database. For other database types, all users who were authenticated by a given database are assigned to a single ACS user group. For more information about group mapping, see [Chapter 16, “User Group Mapping and Specification.”](#)

- **Database Replication**—Database Replication creates user accounts on a secondary ACS by overwriting all existing user accounts on a secondary ACS with the user accounts from the primary ACS. Any user accounts that are unique to a secondary ACS are lost in the replication. For more information, see [ACS Internal Database Replication, page 8-1](#).

About External User Databases

You can configure ACS to forward authentication of users to one or more external user databases. Support for external user databases means that ACS does not require that you create duplicate user entries in the user database. In organizations in which a substantial user database already exists, ACS can leverage the work already invested in building the database without any additional input.

In addition to performing authentication for network access, ACS can perform authentication for TACACS+ enabling privileges by using external user databases. For more information about TACACS+ enable passwords, see [Setting TACACS+ Enable Password Options for a User, page 6-23](#).

**Note**

You can only use external user databases to authenticate users and to determine the group to which ACS assigns a user. The ACS internal database provides all authorization services. With few exceptions, ACS cannot retrieve authorization data from external user databases. Exceptions are noted where applicable in the discussions of specific databases in this chapter. For more information about group mapping for unknown users, see [Chapter 16, “User Group Mapping and Specification.”](#)

Users can be authenticated when using the following databases:

- Windows User Database
- Generic LDAP Open Database Connectivity (ODBC)-compliant relational databases (ACS for Windows)
- LEAP Proxy Remote Authentication Dial-In User Service (RADIUS) servers
- RADIUS Token server
- RSA SecurID Token Server
- RSA Authentication with LDAP Group Mapping

For ACS to interact with an external user database, ACS requires an API for the third-party authentication source. Then ACS communicates with the external user database by using the API.

ACS for Windows

For RSA token servers, you can install the software components that RSA provides or you can use the RADIUS interface. For token servers by other vendors, the standard RADIUS interface serves as the third-party API.

For Open Database Connectivity (ODBC) authentication sources, in addition to the Windows ODBC interface, you must install the third-party ODBC driver on the ACS Windows server.

ACS SE

For RSA token servers, you must use the RADIUS interface.

For Windows user databases, you must install and configure the ACS Remote Agent for Windows. The Remote Agent interacts with the Windows operating system to provide authentication. See the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

Authenticating with External User Databases

Authenticating users with an external user database requires more than configuring ACS to communicate with an external user database. Performing one of the configuration procedures in this chapter for an external database does not, on its own, instruct ACS to authenticate any users with that database.

After you have configured ACS to communicate with an external user database, you can configure ACS to authenticate users with the external user database by:

- **Specific User Assignment**—You can configure ACS to authenticate specific users with an external user database. To do this, the user must exist in the ACS internal database and you must set the Password Authentication list in User Setup to the external user database that ACS should use to authenticate the user.

While setting the Password Authentication for every user account is time-consuming, this method of determining which users are authenticated with an external user database is secure because it requires explicit definition of who should authenticate by using the external user database. In addition, the users may be placed in the desired ACS group and thereby receive the applicable access profile.

- **Unknown User Policy**—You can configure ACS to attempt authentication of users who are not in the ACS internal database by using an external user database. You do not need to define new users in the ACS internal database for this method. For more information about the Unknown User Policy, see [About Unknown User Authentication, page 15-3](#).
- **Network access profiles (NAPs)**—You can configure NAPs to define which external databases are used to validate the credentials of the user for authentication. For more information about configuring authentication in NAPs, see [Authentication Policy Configuration for NAPs, page 14-27](#).

You can configure ACS with any or all of the previous methods; these methods are not mutually exclusive.

External User Database Authentication Process

When ACS attempts user authentication with an external user database, it forwards the user credentials to the external user database. The external user database passes or fails the authentication request from ACS. On receiving the response from the external user database, ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the external user database.

[Figure 12-1](#) shows a AAA configuration with an external user database.

Figure 12-1 A Simple AAA Scenario



For more information, see the section regarding the database type in which you are interested.

Windows User Database

You can configure ACS to use a Windows user database to authenticate users.

This section contains:

- [Windows User Database Support, page 12-5](#)
- [Authentication with Windows User Databases, page 12-6](#)
- [Trust Relationships, page 12-6](#)
- [Windows Dial-Up Networking Clients, page 12-6](#)
- [Usernames and Windows Authentication, page 12-7](#)
- [EAP and Windows Authentication, page 12-10](#)
- [User-Changeable Passwords with Windows User Databases, page 12-16](#)
- [Preparing Users for Authenticating with Windows, page 12-17](#)
- [Selecting Remote Agents for Windows Authentication \(Solution Engine Only\), page 12-17](#)
- [Windows User Database Configuration Options, page 12-18](#)
- [Configuring a Windows External User Database, page 12-21](#)
- [Machine Authentication Support in a Multi-Forest Environment, page 12-22](#)

Windows User Database Support

ACS supports the use of Windows external user databases for:

- **User Authentication**—For information about the types of authentication that ACS supports with Windows Security Accounts Manager (SAM) database or a Windows Active Directory database, see [Authentication Protocol-Database Compatibility, page 1-8](#).
- **Machine Authentication**—ACS supports machine authentication with EAP-TLS and PEAP (EAP-MS-CHAPv2). For more information, see [EAP and Windows Authentication, page 12-10](#).
- **Group Mapping for Unknown Users**— ACS supports group mapping for unknown users by requesting group membership information from Windows user databases. For more information about group mapping for users authenticated with a Windows user database, see [Group Mapping by Group Set Membership, page 16-3](#).
- **Password-Aging**— ACS supports password aging for users who are authenticated by a Windows user database. For more information, see [User-Changeable Passwords with Windows User Databases, page 12-16](#).
- **Dial-in Permissions**—ACS supports use of dial-in permissions from Windows user databases. For more information, see [Preparing Users for Authenticating with Windows, page 12-17](#).
- **Callback Settings**—ACS supports use of callback settings from Windows user databases. For information about configuring ACS to use Windows callback settings, see [Setting the User Callback Option, page 6-6](#).

Authentication with Windows User Databases

ACS forwards user credentials to a Windows database by passing the user credentials to the Windows operating system of the computer that is running ACS for Windows or the Solution Engine remote agent. The Windows database passes or fails the authentication request from ACS.

ACS for Windows only: When receiving the response from the Windows database agent ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the Windows database.

Solution Engine only: When receiving the response from the Windows database, the remote agent forwards the response to ACS, and ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the Windows database.

ACS grants authorization based on the ACS group to which the user is assigned. While you can determine the group to which a user is assigned information from the Windows database, it is ACS that grants authorization privileges.

To further control access by a user, you can configure ACS to also check the setting for granting dial-in permission to the user. This setting is labeled Grant dialin permission to user in Windows NT and **Allow access** in the Remote Access Permission area in Windows 2000 and Windows 2003 R2. If this feature is disabled for the user, access is denied; even if the username and password are typed correctly.

Trust Relationships

ACS can take advantage of trust relationships established between Windows domains. If the domain that contains ACS for Windows or the computer running the Windows remote agent (ACS SE) trusts another domain, ACS can authenticate users whose accounts reside in the other domain. ACS can also reference the **Grant dialin permission to user** setting across trusted domains.



Note

If ACS for Windows is running on a member server, rather than a domain controller, taking advantage of trust relationships depends on proper configuration of ACS for Windows at installation. For more information, see the *Installation Guide for Cisco Secure ACS for Windows Release 4.2*.

If the ACS SE remote agent is running on a member server, rather than a domain controller, taking advantage of trust relationships depends on proper configuration of the remote agent at installation. For more information, see “Configuring for Member Server Authentication” in the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

ACS can take advantage of indirect trusts for Windows authentication. Consider the example of Windows domains A, B, and C, where ACS for Windows or the remote agent resides on a server in domain A. Domain A trusts domain B, but no trust relationship is established between domain A and domain C. If domain B trusts domain C, ACS for Windows or the remote agent in domain A can authenticate users whose accounts reside in domain C, making use of the indirect trust of domain C.

For more information on trust relationships, refer to your Microsoft Windows documentation.

Windows Dial-Up Networking Clients

The dial-up networking clients for Windows NT/2000/2003 R2/XP Professional and Windows 95/98/Millennium Edition (ME)/XP Home enable users to connect to your network remotely; but the fields that are provided differ:

- [Windows Dial-Up Networking Clients with a Domain Field, page 12-7](#)
- [Windows Dial-Up Networking Clients without a Domain Field, page 12-7](#)

Windows Dial-Up Networking Clients with a Domain Field

If users dial in to your network by using the dial-up networking client that is provided with Windows NT, Windows 2000, Windows 2003 R2, or Windows XP Professional, three fields appear:

- **username**—Type your username.
- **password**—Type your password.
- **domain**—Type your valid domain name.



Note For more information about the implications of completing or leaving the domain box blank, see [Nondomain-Qualified Usernames, page 12-8](#).

Windows Dial-Up Networking Clients without a Domain Field

If users access your network by using the dial-up networking client that is provided with Windows 95, Windows 98, Windows ME, or Windows XP Home, two fields appear:

- **username**—Type your username.



Note You can also prefix your username with the name of the domain in to which you want to log. For more information about the implications of prefixing or not prefixing the domain name before the username, see [Nondomain-Qualified Usernames, page 12-8](#).

- **password**—Type your password.

Usernames and Windows Authentication

This section contains:

- [Username Formats and Windows Authentication, page 12-7](#)
- [Nondomain-Qualified Usernames, page 12-8](#)
- [Domain-Qualified Usernames, page 12-9](#)
- [UPN Usernames, page 12-9](#)

Username Formats and Windows Authentication

ACS supports Windows authentication for usernames in a variety of formats. When ACS attempts Windows authentication, it first determines the username format and submits the username to Windows in the applicable manner. To implement reliable Windows authentication with ACS, you must understand how ACS determines a username format, how it supports each of these formats, and how the types of support are related.

To determine the format of a username that is submitted for Windows authentication, ACS searches the username for the:

- At symbol (@)
- Backslash (\)

Based on the presence and position of these two characters in the username, ACS determines username format by using the following logic:

1. If the username does not contain a backslash (\) *and* does not contain an at symbol (@), ACS considers the username to be nondomain qualified. For example, the username *cyril.yang* is nondomain qualified. For more information, see [Nondomain-Qualified Usernames, page 12-8](#).
2. If the username contains a backslash (\) that precedes any at characters, ACS considers the username to be domain qualified. For example, ACS considers the following usernames to be domain qualified:

- *MAIN\cyril.yang*
- *MAIN\cyril.yang@central-office*

For more information, see [Domain-Qualified Usernames, page 12-9](#).

3. If the username contains an at symbol (@) that does not follow a backslash (\), ACS considers the username to be in User Principal Name (UPN) format. For example, ACS considers the following usernames to be UPN usernames:

- *cyril.yang@example.com*
- *cyril.yang@main.example.com*
- *cyril.yang@main*
- *cyril.yang@central-office@example.com*
- *cyril.yang@main\example.com*

For more information, see [UPN Usernames, page 12-9](#).

Nondomain-Qualified Usernames

ACS supports Windows authentication of usernames that are not domain qualified, provided the username does not contain an at symbol (@). Users with at symbols (@) in their usernames must submit the username in UPN format or in a domain-qualified format. Examples of nondomain-qualified usernames are *cyril.yang* and *msmith*.

In Windows environments with multiple domains, authentication results with nondomain-qualified usernames can vary. This variance occurs because Windows, not ACS, determines which domains are used to authenticate a nondomain-qualified username. If Windows does not find the username in its local domain database, it then checks all trusted domains. If ACS for Windows or the remote agent runs on a member server and the username is not found in trusted domains, Windows also checks its local accounts database. Windows attempts to authenticate a user with the first occurrence of the username that it finds.

When Windows authentication for a nondomain-qualified username succeeds, the privileges that are assigned during authentication will be those that are associated with the Windows user account in the first domain with a matching username and password. This condition also illustrates the importance of removing usernames from a domain when the user account is no longer needed.



Note

If the credentials that the user submits do not match the credentials that are associated with the first matching username that Windows finds, authentication fails. Thus, if different users in different domains share the same exact username, logging in with a nondomain-qualified username can result in inadvertent authentication failure.

Use of the Domain List is not required to support Windows authentication, but it can alleviate authentication failures that nondomain-qualified usernames cause. If you have configured the Domain List in the Windows User Database Configuration page of the External User Databases section, ACS submits the username and password to each domain in the list in a domain-qualified format until it successfully authenticates the user. If ACS has tried each domain in the Domain List or if no trusted domains have been configured in the Domain List, ACS stops attempting to authenticate the user and does not grant that user access.

**Note**

If your Domain List contains domains and your Windows Security Account Manager (SAM) or Active Directory user databases are configured to lock out users after a number of failed attempts, users can be inadvertently locked out because ACS tries each domain in the Domain List explicitly, resulting in failed attempts for identical usernames that reside in different domains.

Domain-Qualified Usernames

The most reliable method of authenticating users against a specific domain is to require users to submit the domains that they should be authenticated against along with their usernames. Authentication of a domain-qualified username is directed to a specific domain; rather than depending on Windows to attempt authentication with the correct domain or on using the Domain List to direct ACS to submit the username repeatedly in a domain-qualified format.

Domain-qualified usernames have the following format:

DOMAIN\user

For example, the domain-qualified username for user Mary Smith (*msmith*) in Domain10 would be *Domain10\msmith*.

For usernames containing an at symbol (@), such as *cyril.yang@central-office*, using a domain-qualified username format is required. For example, *MAIN\cyril.yang@central-office*. If a username containing an at symbol (@) is received in a nondomain-qualified format, ACS perceives it as a username in UPN format. For more information, see [UPN Usernames, page 12-9](#).

UPN Usernames

ACS supports authentication of usernames in UPN format, such as *cyril.yang@example.com* or *cyril.yang@central-office@example.com*.

If the authentication protocol is EAP-TLS, by default, ACS submits the username to Windows in UPN format. For all other authentication protocols that it can support with Windows databases, ACS submits the username to Windows that is stripped of all characters after and including the last at symbol (@). This behavior allows for usernames that contain an at symbol (@). For example:

- If the username received is *cyril.yang@example.com*, ACS submits to Windows an authentication request containing the username *cyril.yang*.
- If the username received is *cyril.yang@central-office@example.com*, ACS submits to Windows an authentication request containing the username *cyril.yang@central-office*.

**Note**

ACS cannot tell the difference between a nondomain-qualified username that contains an at symbol (@) and a UPN username; all usernames containing an at symbol (@) that do not follow a backslash (\) are submitted to Windows with the final at symbol (@) and the characters that follow it removed. Users with at symbols (@) in their usernames must submit the username in UPN format or in a domain-qualified format.

EAP and Windows Authentication

This section contains information about Windows-specific EAP features that you can configure on the Windows User Database Configuration page.

This section contains:

- [Machine Authentication, page 12-10](#)
- [Machine Access Restrictions, page 12-12](#)
- [Microsoft Windows and Machine Authentication, page 12-13](#)
- [Enabling Machine Authentication, page 12-15](#)

Machine Authentication

ACS supports the authentication of computers that are running the Microsoft Windows operating systems that support EAP computer authentication, such as Windows XP with Service Pack 1. 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 user database. If you use Active Directory and the matching computer account in Active Directory 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 logged in to the domain successfully from this computer.

- **User network authentication**—ACS authenticates the user, allowing the user to have network connectivity. If the user profile exists, the user database that is specified is used to authenticate the user. While the user database is not required to be the Windows user database, 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 has selected to shutdown or restart the computer; rather than just logging off.

ACS supports EAP-TLS, PEAP (EAP-MS-CHAPv2), and PEAP (EAP-TLS) for machine authentication. You can enable each separately on the Windows User Database Configuration page, which allows a mix of computers that authenticate with EAP-TLS or PEAP (EAP-MS-CHAPv2). Microsoft operating systems that perform machine authentication might limit the user authentication protocol to the same protocol that is used for machine authentication. For more information about Microsoft operating systems and machine authentication, see [Microsoft Windows and Machine Authentication, page 12-13](#).

The Unknown User Policy supports machine authentication. Computers that were previously unknown to ACS are handled similarly to users. If the Unknown User Policy is enabled and an Active Directory external user database is included on the Selected Databases list on the Configure Unknown User Policy page, machine authentication succeeds; provided that the machine credentials presented to Active Directory are valid.

On a computer that is configured to perform machine authentication, machine authentication occurs when the computer started. Provided that the AAA client sends RADIUS accounting data to ACS, when a computer is started and before a user logs in on that computer, the computer appears on the Logged-In Users List in the Reports and Activity section. Once user authentication begins, the computer no longer appears on the Logged-In Users List.

PEAP-based machine authentication uses PEAP (EAP-MS-CHAPv2) and the password for the computer established automatically when it was added to the Microsoft Windows domain. The computer sends its name as the username and the format is:

`host/computer.domain`

where *computer* is the name of the computer and *domain* is the domain to which the computer belongs. The domain segment might also include subdomains, if they are used; so that the format may be:

`host/computer.subdomain.domain`

The usernames of computers that are authenticated must appear in the ACS internal database. If you enable unknown user processing, ACS adds them automatically once they authenticate successfully. During authentication, the domain name is not used.

EAP-TLS-based machine authentication uses EAP-TLS to authenticate the computer that is using a client certificate. The certificate that the computer uses can be one installed automatically when the computer was added to the domain or one that was added to the local machine storage later. As with PEAP-based machine authentication, the computer name must appear in the ACS internal database in the format contained in the computer client certificate and the user profile corresponding to the computer name must be configured to authenticate by using the Windows external user database. If you enable unknown user processing, ACS adds the computer names to the ACS internal database automatically; once they authenticate successfully. It also automatically configures the user profiles that are created to use the external user database in which the user was found. For machine authentication, this will always be the Windows external user database.

Machine Access Restrictions

You can use the machine access restrictions (MAR) feature as an additional means of controlling authorization for Windows-authenticated EAP-TLS, EAP-FASTv1a, and Microsoft PEAP users, based on machine authentication of the computer used to access the network.

When you enable the feature:

- For every successful machine authentication, ACS caches the value that was received in the Internet Engineering Task Force (IETF) RADIUS `Calling-Station-Id` attribute (31) as evidence of the successful machine authentication. ACS stores each `Calling-Station-Id` attribute value for the number of hours that is specified on the Windows User Database Configuration page before deleting it from the cache.
- When a user authenticates with an EAP-TLS, EAP-FASTv1a, or Microsoft PEAP end-user client, ACS searches the cache of `Calling-Station-Id` values from successful machine authentications for the `Calling-Station-Id` value received in the user authentication request. Whether ACS finds the user-authentication `Calling-Station-Id` value in the cache affects how ACS assigns the user requesting authentication to a user group.
 - **Calling-Station-Id value found in the cache**—ACS assigns the user to a user group by normal methods, which include manual specification of a group in the user profile, group mapping, or RADIUS-based group specification. For example, if a user logs in with a computer that was successfully authenticated and the user profile indicates that the user is a member of group 137, ACS applies to the user session the authorization that were settings specified in group 137.
 - **Calling-Station-Id value not found in the cache**—ACS assigns the user to the user group specified by **Group map for successful user authentication without machine authentication** list. This can include the **<No Access>** group.



Note

User profile settings always override group profile settings. If a user profile grants an authorization that is denied by the group specified in the **Group map for successful user authentication without machine authentication** list, ACS grants the authorization.

The MAR feature supports full EAP-TLS, EAP-FASTv1a, and Microsoft PEAP authentication, as well as resumed sessions for EAP-TLS, EAP-FASTv1a, and Microsoft PEAP and fast reconnections for Microsoft PEAP.

The MAR feature has the following limitations and requirements:

- Machine authentication must be enabled.
- Users must authenticate with EAP-TLS, EAP-FASTv1a, or a Microsoft PEAP client. MAR does not apply to users who are authenticated by other protocols, such as LEAP, or MS-CHAP.
- The AAA client must send a value in the IETF RADIUS `Calling-Station-Id` attribute (31).
- ACS does not replicate the cache of `Calling-Station-Id` attribute values from successful machine authentications.
- Users that are authenticated through dial-up will always be treated according to the MAR configuration, since there is no machine authentication when by using dial up. A user will be mapped to a specific group, as defined in the External User Databases > Database Group Mappings > Windows Database settings, when machine authentication occurs. If group mapping is not configured, the user will be mapped to the default group.

Setting Up a MAR Exception List

You might need to set up a MAR exception list if you need to set up specific users (for example managers and administrators) to have access to the network; regardless of whether they pass machine authentication. This feature allows you to select user groups that would be exempt from the MAR.

Before You Begin

So that users can immediately authenticate as part of the MAR exception list, you should set up the required number of groups and permissions before changing your Windows database settings. To manage your group settings, see [Group TACACS+ Settings, page 5-2](#) and [Listing Users in a User Group, page 5-40](#).

To set up a MAR exception list for selected user groups:

-
- | | |
|---------------|--|
| Step 1 | From the navigation bar, choose External User Databases > Database Configuration > Windows Database . |
| Step 2 | Click Configure . |
| Step 3 | In the Windows User Database Configuration page, enable the correct machine authentication settings and move the user groups that you want to include in the MAR exemption list to the Selected Groups list. |
| Step 4 | Click Submit . |
-

The exception list is based on ACS user groups to which the relevant NT groups would map. You can create exceptions for several user groups, and map different authorization permission to each group.

Microsoft Windows and Machine Authentication

ACS supports machine authentication with Active Directory in Windows 2000 and 2003 R2. To enable machine authentication support in Windows Active Directory you must:

1. Apply Service Pack 4 to the computer that is running Active Directory.
2. Complete the steps in [Microsoft Knowledge Base Article 306260: Cannot Modify Dial-In Permissions for Computers That Use Wireless Networking](#).

Client operating systems that support machine authentication are:

- Microsoft Windows XP with Service Pack 1 applied.
- Microsoft Windows 2000 with:
 - Service Pack 4 applied.
 - Patch Q313664 applied (available from Microsoft.com).
- Microsoft Windows 2003 R2

The following list describes the essential details of enabling machine authentication on a client computer with a Cisco Aironet 350 wireless adapter. For more information about enabling machine authentication in Microsoft Windows operating systems, please refer to Microsoft documentation.

1. Ensure that the wireless network adapter is installed correctly. For more information, see the documentation that is provided with the wireless network adapter.

2. Ensure that the certification authority (CA) certificate of the CA that issued the ACS server certificate is stored in machine storage on client computers. User storage is not available during machine authentication; therefore, if the CA certificate is in user storage, machine authentication fails.
3. Select the wireless network:
 - In Windows XP, you can choose **Windows Network Connection > Properties > Network Connection Properties**.
 - In Windows 2000, you can manually enter the Service Set Identifier (SSID) of the wireless network. Use the Advanced tab of the properties dialog box for the wireless network adapter.
4. To enable PEAP machine authentication, configure the Authentication tab. In Windows XP, the Authentication tab is available from the properties of the wireless network. In Windows 2000, it is available from the properties of the wireless network connection. To configure the Authentication tab:
 - a. Check the **Enable network access control using IEEE 802.1X** check box.
 - b. Check the **Authenticate as computer when computer information is available** check box.
 - c. From the EAP type list, select **Protected EAP (PEAP)**.
 - d. On the **Protected EAP Properties** dialog box, you can enforce that ACS has a valid server certificate by checking the **Validate server certificate** check box. If you do check this check box, you must also select the applicable **Trusted Root Certification Authorities**.
 - e. Also open the PEAP properties dialog box, from the **Select Authentication Method** list, select **Secured password (EAP-MS-CHAP v2)**.
5. To enable EAP-TLS machine authentication, configure the Authentication tab. In Windows XP, the Authentication tab is available from the properties of the wireless network. In Windows 2000, it is available from the properties of the wireless network connection.
 - a. Check the **Enable network access control using IEEE 802.1X** check box.
 - b. Check the **Authenticate as computer when computer information is available** check box.
 - c. From the **EAP type** list, select **Smart Card or other Certificate**.
 - d. On the **Smart Card or other Certificate Properties** dialog box, select the **Use a certificate on this computer** option.
 - e. Also on the **Smart Card or other Certificate Properties** dialog box, you can enforce that ACS has a valid server certificate by checking the **Validate server certificate** check box. If you check this check box, you must also select the applicable Trusted Root Certification Authorities.

If you have a Microsoft certification authority server that is configured on the domain controller, you can configure a policy in Active Directory to produce a client certificate automatically when a computer is added to the domain. For more information, see the [Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows](#).

Enabling Machine Authentication

This procedure contains an overview of the detailed procedures required to configure ACS to support machine authentication.

**Note**

You must configure end-user client computers and the applicable Active Directory to support machine authentication. This procedure is specific to configuration of ACS only. For information about configuring Microsoft Windows operating systems to support machine authentication, see [Microsoft Windows and Machine Authentication, page 12-13](#).

**Note**

Solution Engine only: Windows authentication requires that you install at least one ACS Remote Agent for Windows and complete the steps in [Adding a Remote Agent, page 3-21](#). For information about installing the ACS Remote Agent for Windows, see the *Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2*.

To enable ACS to perform machine authentication:

- Step 1** Install a server certificate in ACS. PEAP (EAP-MS-CHAPv2) and EAP-TLS require a server certificate. ACS uses a single certificate to support both protocols. For detailed steps, see [Installing an ACS Server Certificate, page 9-22](#).

**Note**

If you have installed a certificate to support EAP-TLS or PEAP user authentication or to support HTTPS protection of remote ACS administration, you do not need to perform this step. A single server certificate will support all certificate-based ACS services and remote administration.

- Step 2** For EAP-TLS machine authentication, if certificates on end-user clients are issued by a different CA than the CA that issued the server certificate on ACS, you must edit the certification trust list so that CAs that issue end-user client certificates are trusted. If you do not perform this step and the CA of the server certificate is not the same as the CA of an end-user client certificate CA, EAP-TLS will operate normally; but reject the EAP-TLS machine authentication because it does not trust the correct CA. For detailed steps, see [Editing the Certificate Trust List, page 9-28](#).

- Step 3** Enable the applicable protocols on the Global Authentication Setup page:

- To support machine authentication with PEAP, enable the PEAP (EAP-MS-CHAPv2) protocol.
- To support machine authentication with EAP-TLS, enable the EAP-TLS protocol.

**Note**

Solution Engine only: If you are using a Network Access Profile (NAP), the same protocols must be enabled in the NAP configuration.

You can use ACS to complete this step only after you have successfully completed Step 1. For detailed steps, see [Configuring Authentication Options, page 9-21](#).

- Step 4** Configure a Windows external user database and enable the applicable types of machine authentication on the Windows User Database Configuration page:
- To support machine authentication with PEAP, check the **Enable PEAP machine authentication** check box.

- To support machine authentication with EAP-TLS, check the **Enable EAP-TLS machine authentication** check box.
- To require machine authentication in addition to user authentication, check the **Enable machine access restrictions** check box.



Note If you already have a Windows external user database configured, modify its configuration to enable the applicable machine authentication types.

For detailed steps, see [Configuring a Windows External User Database, page 12-21](#).



Note Solution Engine only: Windows authentication requires an ACS Remote Agent for Windows.

ACS is ready to perform machine authentication for computers whose names exist in the ACS internal database.

- Step 5** If you have not already enabled the Unknown User Policy and added the Windows external user database to the Selected Databases list, consider doing so to allow computers that are not known to ACS to authenticate. For detailed steps, see [Configuring the Unknown User Policy, page 15-8](#).



Note Enabling the Unknown User Policy to support machine authentication also enables the Unknown User Policy for user authentication. ACS makes no distinction in unknown user support between computers and users.

- Step 6** If you have users to whom you want to allow access to the network, even if they do not pass machine authentication, you might want to set up a list of user groups that are exempt from the MAR. For detailed steps, see [Machine Access Restrictions, page 12-12](#).

ACS is ready to perform machine authentication for computers; regardless of whether the computer names exist in ACS internal database.

User-Changeable Passwords with Windows User Databases

For network users who are authenticated by a Windows user database, ACS supports user-changeable passwords on password expiration. You can enable this feature in the MS-CHAP Settings and Windows EAP Settings tables on the Windows User Database Configuration page in the External User Databases section. The use of this feature in your network requires that:

- Users must be present in the Windows Active Directory or SAM user database.
- User accounts in ACS must specify the Windows user database for authentication.
- End-user clients must be compatible with MS-CHAP, PEAP (EAP-GTC), PEAP (EAP-MS-CHAPv2), or EAP-FAST.
- The AAA client that the end-user clients connect to must support the applicable protocols:
 - For MS-CHAP password aging, the AAA client must support RADIUS-based MS-CHAP authentication.
 - For PEAP (EAP-MS-CHAPv2), PEAP (EAP-GTC), and EAP-FAST password aging, the AAA client must support EAP.

When the previous conditions are met and this feature is enabled, users receive a dialog box prompting them to change their passwords on their first successful authentication after their passwords have expired. The dialog box is the same as Windows presents to users when a user with an expired password accesses a network via a remote-access server.

For more information about password aging support in ACS, see [Enabling Password Aging for the ACS Internal Database, page 5-15](#).

Preparing Users for Authenticating with Windows

Before using the Windows user database for authentication:

-
- Step 1** Ensure that the username exists in the Windows user database.
 - Step 2** In Windows, for each user account, clear the following **User Properties** check boxes:
 - User must change password at next logon
 - Account disabled
 - Step 3** If you want to control dial-in access from within Windows NT, click **Dial-in** and select **Grant dialin permission to user**. In Windows 2000 and Windows 2003 R2, access the **User Properties** dialog box, select the **Dial-In** tab, and in the Remote Access area, click **Allow access**. You must also configure the option to reference this feature under Database Group Mappings in the External User Databases section of ACS.
-

Selecting Remote Agents for Windows Authentication (Solution Engine Only)

Before you can configure ACS to authenticate users with a Windows external user database, you must select a primary remote agent that is to deliver authentication requests to the Windows operating system. You may also select a secondary remote agent for ACS to use if the primary remote agent is unavailable.

Before You Begin

To complete this procedure, you must have installed at least one ACS Remote Agent for Windows and completed the steps in [Adding a Remote Agent, page 3-21](#).

To select remote agents for Windows authentication:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Configuration**.

ACS displays a list of all possible external user database types.
 - Step 3** Click **Windows Database**.

ACS displays the External User Database Configuration page.
 - Step 4** Click **Configure**.

ACS displays the Windows Remote Agent Selection lists.
 - Step 5** From the **Primary** list, select the remote agent that ACS should always use to authenticate users, provided that the remote agent is available.

- Step 6** From the **Secondary** list, select the remote agent that ACS should use to authenticate users when the remote agent selected in the Primary list is unavailable.



Note If you do not want to use a secondary remote agent, from the **Secondary** list, choose **None**.

- Step 7** Click **Submit**.

ACS saves the remote agent selections that you made. The Windows User Database Configuration page appears.

Windows User Database Configuration Options

The Windows User Database Configuration page contains:

- **Dialin Permission**—You can restrict network access to users whose Windows accounts have Windows dial-in permission. The Grant dialin permission to user check box controls this feature.



Note This feature applies to all users when ACS authenticates with a Windows external user database; despite the name of the feature, it is not limited to users who access the network with a dial-up client but is applied regardless of client type. For example, if you have configured a PIX Firewall to authenticate Telnet sessions by using ACS as a RADIUS server, a user authenticated by a Windows external user database would be denied Telnet access to the PIX Firewall if the Dialin Permission feature is enabled and the Windows user account does not have dial-in permission.



Tip

Windows dial-in permission is enabled in the Dialin section of user properties in Windows NT and on the Dial-In tab of the user properties in Windows 2000 and Windows 2003 R2.

- **Windows Callback**—You should enable this setting if you have Windows users that require dial-up access with callback and the User Setup or Group Setup callback setting is configured for Windows Database Callback. If dial-in access with callback is not required or is not configured for Windows Database Callback, then do not enable this setting.



Note If you disable the Windows Callback option, be certain to disable the callback options in the User Setup or Group Setup callback settings. If the settings contain inconsistencies, the client will not receive the callback number.

- **Unknown User Policy**—If the unknown user policy contains additional external databases and the Windows database is not the last database on the Selected Databases list, you might enable this option. For example, If a user does not exist in the Windows database, or has typed an incorrect password, the error 1326 (bad username or password) is returned. ACS treats this error as a wrong password error and does not default to another external database. You should enable this option when additional external databases appear after the Windows database in the Selected Databases list. When enabled, ACS searches for the unknown user in the other external databases.

- **Configure Domain List**—ACS tries to authenticate to any domain listed in Available Domains. If your Windows users do not specify their domain when dialing up, ACS relies on Windows to try to locate the appropriate user account. However, Windows may not be able to authenticate a user properly if the same username exists in more than one trusted domain. We recommend that you ask users to enter their domains when dialing in. If this is not practical, you can define a Domain List. If ACS fails to authenticate a user because the account exists in more than one domain and a Domain List exists, ACS will then retry authentication for each domain in the list. The list order is significant: domains that appear earlier in the list will be tried first. Because of the delay (typically two seconds) for each domain that fails authentication, you should set your AAA client timeout accordingly.

The Domain List is only required if you have multiple user accounts with the same SAM username in more than one domain AND you are not using EAP/PEAP (for example, PAP/MSCHAP) and you cannot supply a domain prefix in the username.

Use this option only when *all* the following occur:

- You are using PAP or MSCHAP.
- Usernames are not domain-prefixed.
- There are duplicate usernames, for example, administrator.

When usernames are not domain-prefixed, and there are multiple occurrences of the same username across the entire network, if no domains are in the **Domain List**, Windows can try to authenticate the wrong credentials. When Windows rejects the initial user authentication request, ACS stops attempting to authenticate the user. For more information, see [Nondomain-Qualified Usernames, page 12-8](#). If domains are in the **Domain List**, ACS qualifies the username with a domain from the list and submits the domain-qualified username to Windows, once for each domain in the Domain List, until each domain has rejected the user or until one of the domains authenticates the user.

In all other cases, the **Domain List** should be left empty as it might cause performance problems if you use it when you do not need to. Also, each time ACS uses the Domain List and checks the wrong account, Windows counts that as a failed login for that user, which can cause an account lockout.

- **MS-CHAP Settings**—You can control whether ACS supports MS-CHAP-based password changes for Windows user accounts. You can use the Permit password changes by checking the MS-CHAP version *N* check boxes to specify which versions of MS-CHAP ACS supports.



Note The check boxes under MS-CHAP Settings do not affect password aging for Microsoft PEAP, EAP-FAST, or machine authentication.

For more information about Windows password changes, see [Enabling Password Aging for the ACS Internal Database, page 5-15](#).

- **Windows EAP Settings:**
 - **Enable password change inside PEAP or EAP-FAST**—The **Permit password change inside PEAP or EAP-FAST** check box controls whether ACS supports PEAP-based or EAP-FAST-based password changes for Windows user accounts. PEAP password changes are supported only when the end-user client uses PEAP (EAP-MS-CHAPv2) for user authentication. For EAP-FAST, ACS supports password changes in phase zero and phase two.
 - **Enable PEAP machine authentication**—This check box controls whether ACS performs machine authentication by using a machine name and password with PEAP (EAP-MS-CHAPv2). For more information about machine authentication, see [Machine Authentication, page 12-10](#).

- **Enable EAP-TLS machine authentication**—This check box controls whether ACS performs machine authentication by using a machine name and password with EAP-TLS. For more information about machine authentication, see [Machine Authentication, page 12-10](#).
- **Enable machine access restrictions**— This box determines whether ACS uses machine authentication as a condition for user authorization. The following protocols are supported for machine authentication: Microsoft PEAP EAP-TLS, EAP-FAST v1a, Cisco PEAP-TLS. If one of these protocols is used for machine authentication, the settings for MAR do not effect the user authentication. If a user tries to access the network with a computer that failed machine authentication, or with another protocol that does not support machine authentication, authorizations are implemented according to the machine access restriction configuration. For more information about the MAR feature, see [Machine Access Restrictions, page 12-12](#).

**Note**

Users that are authenticated through dial-up will always be treated according to the MAR configuration, since there is no machine authentication when using dial up. A user will be mapped to a specific group, as defined in the **External User Databases > Database Group Mappings > Windows Database** settings, when machine authentication occurs. If group mapping is not configured, the user will be mapped to the default group.

**Tip**

To enable machine access restrictions, you must specify a number greater than zero (0) in the **Aging time (hours)** box.

- **Aging time (hours)**—This box specifies the number of hours that ACS caches IETF RADIUS `Calling-Station-Id` attribute values from successful machine authentications, for use with the MAR feature. The default value is 12 hours, which means that ACS does not cache `Calling-Station-Id` values.

**Note**

If you do not change the value of the **Aging time (hours)** box to something other than zero (0), all EAP-TLS and Microsoft PEAP users whose computers perform machine authentication are assigned to the group that is specified in the **Group map for successful user authentication without machine authentication** list.

**Tip**

To clear the cache of `Calling-Station-Id` values, type zero (0) in the **Aging time (hours)** box and click **Submit**.

- **Group map for successful user authentication without machine authentication**—This list specifies the group profile that ACS applies to a user who accesses the network from a computer that has not passed machine authentication for longer than the number of hours specified in the Aging time (hours) box. To deny such users any access to the network, select **<No Access>** (which is the default setting).

**Note**

User profile settings always override group profile settings. If a user profile grants an authorization that is denied by the group that is specified in the Group map for successful user authentication without machine authentication list, ACS grants the authorization.

- **User Groups that are exempt from passing machine authentication**— The Selected User Group list controls what ACS does when machine authentication is not successfully completed. If the Selected User Group list contains no groups and Windows rejects the initial machine authentication, ACS stops attempting to authenticate the user. If the Selected User Group list contains groups, ACS will provide authentication and the privileges within that group to the user; even though their computers are unknown to Active Directory.



Note Configuring the User Group list is optional. For more information about the user group management, see [Chapter 5, “User Group Management.”](#)



Caution

If your User Group list contains groups and you configure your Windows SAM or Active Directory user databases to lock out users after a number of failed attempts, users can be inadvertently locked out. You should ensure that your group settings are configured properly.

- **Available User Groups**—This list represents the user groups for which ACS *requires* machine authentication.
- **Selected User Groups**—This list represents the user groups for which ACS *do not require* machine authentication to gain entry into the network.
- **Windows Authentication Configuration**—This option provides the capability of configuring a workstation name for ACS authentications to the Windows Active Directory.
 - **Default: "CISCO"**—Choose this option if you want CISCO as the workstation name.
 - **Local: machine-name**—Choose this option if you want to use your local machine name as the workstation name.
 - **User defined workstation name**—Choose this option to define your own workstation name. You can use alpha numeric characters, the hyphen(-), and the period(.).
 - **Enable nested group evaluation during group mapping** — When this option is enabled, you can create group mappings that use Active Directory groups that a user is an indirect member of. However, this option will not evaluate Domain Local groups in Active Directory so any group mapping that references Domain Local groups will not operate correctly. When this option is disabled, group mapping will not work if it references an Active Directory group of which a user is an indirect member. Only groups that users are direct members of should be used. However, this option will evaluate Domain Local groups in Active Directory and they can be used in group mappings.

Configuring a Windows External User Database



Note

Solution Engine only: You must have completed the steps in [Selecting Remote Agents for Windows Authentication \(Solution Engine Only\)](#), page 12-17.

For information about the options that are available on the Windows User Database Configuration page, see [Windows User Database Configuration Options](#), page 12-18.

To configure ACS to authenticate users against the Windows user database in the trusted domains of your network:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

ACS displays a list of all possible external user database types.

Step 3 Click **Windows Database**.

If no Windows database configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Step 4 Click **Configure**.

The Windows User Database Configuration page appears.

Step 5 As needed, configure the options in:

- Dialin Permission
- Windows Callback
- Unknown User Policy
- Domain List
- MS-CHAP Settings
- Windows EAP Settings
- Windows Authentication Configuration

For information about the options on the Windows User Database Configuration page, see [Windows User Database Configuration Options, page 12-18](#).



Note All the settings on the Windows User Database Configuration page are optional and need not be enabled; unless you want to permit and configure the specific features that they support.

Step 6 Click **Submit**.

ACS saves the Windows user database configuration that you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see [About Unknown User Authentication, page 15-3](#). For more information about configuring user accounts to authenticate by using this database, see [Chapter 6, "User Management."](#)

Machine Authentication Support in a Multi-Forest Environment

ACS supports machine authentication in a multi-forest environment. Machine authentications succeed as long as an appropriate trust relationship exists between the primary ACS forest and the requested domain's forest. When a requested user's or machine's domain is part of trusted forest, machine authentication will succeed.

User authentication between multiple forests is supported for EAP-FASTv1a with PEAP, MSPEAP, and for EAP-TLS.

**Note**

The multi-forest feature works only when the username contains the domain information.

Generic LDAP

For information about the types of authentication that ACS supports with generic LDAP databases, such as Netscape Directory Services, see [Authentication Protocol-Database Compatibility, page 1-8](#).

ACS supports group mapping for unknown users by requesting group membership information from LDAP user databases. For more information about group mapping for users who are authenticated with an LDAP user database, see [Group Mapping by Group Set Membership, page 16-3](#).

Configuring ACS to authenticate against an LDAP database has no effect on the configuration of the LDAP database. To manage your LDAP database, see your LDAP database documentation.

This section contains:

- [ACS Authentication Process with a Generic LDAP User Database, page 12-23](#)
- [Multiple LDAP Instances, page 12-24](#)
- [LDAP Organizational Units and Groups, page 12-24](#)
- [Domain Filtering, page 12-24](#)
- [LDAP Failover, page 12-25](#)
- [LDAP Admin Logon Connection Management, page 12-26](#)
- [Distinguished Name Caching, page 12-26](#)
- [LDAP Configuration Options, page 12-27](#)
- [Configuring a Generic LDAP External User Database, page 12-31](#)
- [Downloading a Certificate Database \(Solution Engine Only\), page 12-47](#)

ACS Authentication Process with a Generic LDAP User Database

ACS forwards the username and password to an LDAP database by using a Transmission Control Protocol (TCP) connection on a port that you specify. The LDAP database passes or fails the authentication request from ACS. When receiving the response from the LDAP database, ACS instructs the requesting AAA client to grant or deny the user access, depending on the response from the LDAP server.

ACS grants authorization based on the ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the LDAP server, ACS grants authorization privileges.

Multiple LDAP Instances

You can create more than one LDAP configuration in ACS. By creating more than one LDAP configuration 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 configuration instance.

ACS does not require that each LDAP instance corresponds to a unique LDAP database. You can have more than one LDAP configuration 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 configuration 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.

For each LDAP instance, you can add it to or omit it from the Unknown User Policy. For more information, see [About Unknown User Authentication, page 15-3](#).

For each LDAP instance, you can establish unique group mapping. For more information, see [Group Mapping by Group Set Membership, page 16-3](#).

Multiple LDAP instances are also important when you use domain filtering. For more information, see [Domain Filtering, page 12-24](#).

LDAP Organizational Units and Groups

LDAP groups do not need the same name as their corresponding ACS groups. You can map the LDAP group to an ACS group with any name that you want to assign. For more information about how your LDAP database handles group membership, see your LDAP database documentation. For more information on LDAP group mappings and ACS, see [Chapter 16, “User Group Mapping and Specification.”](#)

Domain Filtering

Using domain filtering, you can control which LDAP instance authenticates a user based on domain-qualified usernames. Domain filtering is based on parsing the characters at the beginning or end of a username that is submitted for authentication. Domain filtering provides you with greater control over the LDAP instance to which ACS submits any given user authentication request. You can also control whether usernames are submitted to an LDAP server with their domain qualifiers intact.

For example, when EAP-TLS authentication a Windows XP client initiates, ACS receives the username in `username@domainname` format. When PEAP authentication is initiated by a Cisco Aironet end-user client, ACS receives the username without a domain qualifier. If both clients are to be authenticated with an LDAP database that stores usernames without domain qualifiers, ACS can strip the domain qualifier. If separate user accounts are maintained in the LDAP database—domain-qualified and nondomain-qualified user accounts—ACS can pass usernames to the LDAP database without domain filtering.

If you choose to make use of domain filtering, each LDAP configuration that you create in ACS can perform domain filtering:

- **Limiting users to one domain**—Per each LDAP configuration in ACS, you can require that ACS only attempts to authenticate usernames that are qualified with a specific domain name. This corresponds to the Only process usernames that are domain qualified option on the LDAP Configuration page. For more information about this option, see [LDAP Configuration Options, page 12-27](#).

With this option, each LDAP configuration is limited to one domain and to one type of domain qualification. You can specify whether ACS strips the domain qualification before submitting the username to an LDAP server. If the LDAP server stores usernames in a domain-qualified format, you should not configure ACS to strip domain qualifiers.

Limiting users to one domain is useful when the LDAP server stores usernames differently per domain: by user context or how the username is stored in ACS—domain qualified or nondomain qualified. The end-user client or AAA client must submit the username to ACS in a domain-qualified format; otherwise ACS cannot determine the user's domain and does not attempt to authenticate the user with the LDAP configuration that uses this form of domain filtering.

- **Allowing any domain but stripping domain qualifiers**—Per each LDAP configuration in ACS, you can configure ACS to attempt to strip domain qualifiers based on common domain-qualifier delimiting characters. This method corresponds to the Process all usernames after stripping domain name and delimiter option on the LDAP Configuration page. For more information about this option, see [LDAP Configuration Options, page 12-27](#).

ACS supports prefixed and suffixed domain qualifiers. A single LDAP configuration can attempt to strip both prefixed and suffixed domain qualifiers; however, you can only specify one delimiting character each for prefixed and suffixed domain qualifiers. To support more than one type of domain-qualifier delimiting character, you can create more than one LDAP configuration in ACS.

Allowing usernames of any domain but stripping domain qualifiers is useful when the LDAP server stores usernames in a nondomain-qualified format but the AAA client or end-user client submits the username to ACS in a domain-qualified format.

**Note**

With this option, ACS submits usernames that are nondomain qualified, too. Usernames are not required to be domain qualified to be submitted to an LDAP server.

LDAP Failover

ACS 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, such as when the server is down or is otherwise unreachable by ACS. To use this feature, you must define the primary and secondary LDAP servers on the LDAP Database Configuration page. Also, you must check the **On Timeout Use Secondary** check box. For more information about configuring an LDAP external user database, see [Configuring a Generic LDAP External User Database, page 12-31](#).

If you check the **On Timeout Use Secondary** check box, 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 attempt and on the value that you enter in the **Failback Retry Delay** box.

Successful Previous Authentication with the Primary LDAP Server

If, on the previous LDAP authentication attempt, ACS successfully connected to the primary LDAP server, ACS attempts to connect to the primary LDAP server. If ACS cannot connect to the primary LDAP server, ACS attempts to connect to the secondary LDAP server.

If ACS cannot connect with LDAP server, ACS stops attempting LDAP authentication for the user. If the user is an unknown user, ACS tries the next external user database in the Unknown User Policy list. For more information about the Unknown User Policy list, see [About Unknown User Authentication, page 15-3](#).

Unsuccessful Previous Authentication with the Primary LDAP Server

If, on the previous LDAP authentication attempt, ACS could not connect to the primary LDAP server, whether ACS first attempts to connect to the primary server or secondary LDAP server for the current authentication attempt depends on the value in the Failback Retry Delay box. If the Failback Retry Delay box is set to zero (0), ACS always attempts to connect to the primary LDAP server first. And if ACS cannot connect to the primary LDAP server, ACS then attempts to connect to the secondary LDAP server.

If the Failback Retry Delay box is set to a number other than zero (0), ACS determines how many minutes have passed since the last authentication attempt by using the primary LDAP server. If more minutes have passed than the value in the Failback Retry Delay box, ACS attempts to connect to the primary LDAP server first. And if ACS cannot connect to the primary LDAP server, ACS then attempts to connect to the secondary LDAP server.

If fewer minutes have passed than the value in the Failback Retry Delay box, ACS attempts to connect to the secondary LDAP server first. And if ACS cannot connect to the secondary LDAP server, ACS then attempts to connect to the primary LDAP server.

If ACS cannot connect to either LDAP server, ACS stops attempting LDAP authentication for the user. If the user is an unknown user, ACS tries the next external user database in the Unknown User Policy list. For more information about the Unknown User Policy list, see [About Unknown User Authentication, page 15-3](#).

LDAP Admin Logon Connection Management

When ACS checks authentication and authorization of a user on an LDAP server, it uses a connection with the LDAP administrator account permissions. It uses the connection to search for the user and user groups on the Directory subtree. ACS retains the administrator connections that are open for successive use and additional administrator binds are not required for each authentication request. You can limit the maximum number of concurrent administrator connections per Generic LDAP External DB configuration (primary and secondary).

Distinguished Name Caching

Searching can be an expensive LDAP operation, which introduces an element of unpredictability into the authentication. ACS takes the username that the authentication process supplies, and asks the LDAP server to search a full subtree of unknown depth, over an unknown user population.

After successful authentication ACS caches the Distinguished Name (DN) that the search returns. Reauthentications can then use the cached DN to perform an immediate lookup of the user.

A cached DN cannot appear on a screen. If a bind to a cached DN fails, ACS falls back to a full search of the data base for authenticating a user.

LDAP Configuration Options

The LDAP Database Configuration page contains many options, presented in three tables:

- **Domain Filtering**—This table contains options for domain filtering. The settings in this table affect all LDAP authentication that is performed by using this configuration; regardless of whether the primary or secondary LDAP server handles the authentication. For more information about domain filtering, see [Domain Filtering, page 12-24](#)

This table contains:

- **Process all usernames**—When you select this option, ACS does not perform domain filtering on usernames before submitting them to the LDAP server for authentication.
- **Only process usernames that are domain qualified**—When you select this option, ACS only attempts authentication for usernames that are domain-qualified for a single domain. You must specify the type of domain qualifier and the domain in the **Qualified by** and **Domain** options. ACS only submits usernames that are qualified in the method that you specify in the **Qualified by** option and that are qualified with the username that is specified in the Domain Qualifier box. You can also specify whether ACS removes the domain qualifier from usernames before submitting them to an LDAP server.
- **Qualified by**—When you select **Only process usernames that are domain qualified**, this option specifies the type of domain qualification. If you select **Prefix**, ACS only processes usernames that begin with the characters that you specify in the Domain Qualifier box. If you select **Suffix**, ACS only processes usernames that end in the characters that you specify in the Domain Qualifier box.



Note

Regardless of the domain qualifier type that is selected, the domain name must match the domain that is specified in the Domain Qualifier box.

- **Domain Qualifier**—When Only process usernames that are domain qualified is selected, this option specifies the domain name and delimiting character that must qualify usernames so ACS can submit the username to an LDAP server. The Domain box accepts up to 512 characters; however, only one domain name and its delimiting character are permitted.

For example, if the domain name is *mydomain*, the delimiting character is the at symbol (@), and Suffix is selected on the Qualified by list, the Domain box should contain *@mydomain*. If the domain name is *yourdomain*, the delimiting character is the backslash (\), and Prefix is selected on the Qualified by list, the Domain Qualifier box should contain *yourdomain*.

- **Strip domain before submitting username to LDAP server**—When you select Only process usernames that are domain qualified, this option specifies whether ACS removes the domain qualifier and its delimiting character before submitting a username to an LDAP server. For example, if the username is *jwiedman@domain.com*, the stripped username is *jwiedman*.
- **Process all usernames after stripping domain name and delimiter**—When this option is selected, ACS submits all usernames to an LDAP server after attempting to strip domain names. Usernames that are not domain qualified are processed, too. Domain name stripping occurs as specified by the following two options:

- **Strip starting characters through the last X character**—When you select Process all usernames after stripping domain name and delimiter, this option specifies that ACS attempts to strip a prefixed domain qualifier. If, in the username, ACS finds the delimiter character that is specified in the X 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 X 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 X 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 X box contains any of these characters, stripping fails.

- **Strip ending characters through the first Y character**—When you select Process all usernames after stripping domain name and delimiter, this option specifies that ACS attempts to strip a suffixed domain qualifier. 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 Y 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 Y box contains any of these characters, stripping fails.

- **Common LDAP Configuration**—This table contains options that apply to all LDAP authentication that is performed by using this configuration. ACS uses the settings in this section; regardless of whether the primary or secondary LDAP server handles the authentication.

This table contains:

- **User Directory Subtree**—The distinguished name (DN) for the subtree that contains all users. For example:

ou=organizational unit[,ou=next organizational unit] o=corporation.com

If the tree containing users 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.

- **Group Directory Subtree**—The DN for the subtree that contains all groups. For example:

ou=organizational unit[,ou=next organizational unit] o=corporation.com

If the tree containing groups is the base DN, type:

`o=corporation.com`

or

`dc=corporation,dc=com`

as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

- **UserObjectType**—The name of the attribute in the user record that contains the username. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation. ACS contains default values that reflect the default configuration of a Netscape Directory Server. Confirm all values for these fields with your LDAP server configuration and documentation.
- **UserObjectClass**—The value of the LDAP `objectType` attribute that identifies the record as a user. Often, user records have several values for the `objectType` attribute, some of which are unique to the user, some of which are shared with other object types. This box should contain a value that is not shared.
- **GroupObjectType**—The name of the attribute in the group record that contains the group name.
- **GroupObjectClass**—A value of the LDAP `objectType` attribute in the group record that identifies the record as a group.
- **Group Attribute Name**—The name of the attribute of the group record that contains the list of user records that are a member of that group.
- **Server Timeout**—The number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server has failed.
- **On Timeout Use Secondary**—Determines whether ACS performs failover of LDAP authentication attempts. For more information about the LDAP failover feature, see [LDAP Failover, page 12-25](#).
- **Failback Retry Delay**—The number of minutes after the primary LDAP server fails to authenticate a user that ACS resumes sending authentication requests to the primary LDAP server first. A value of zero (0) causes ACS to always use the primary LDAP server first.
- **Max. Admin Connections**—The maximum number of concurrent connections (greater than zero (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.
- **Primary and Secondary LDAP Servers**—You can use the Primary LDAP Server table and the Secondary LDAP Server table to identify the LDAP servers and make settings that are unique to each. You do not need to complete the Secondary LDAP Server table if you do not intend to use LDAP failover.

These tables contain:

- **Hostname**—The name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.
- **Port**—The TCP/IP port number on which the LDAP server is listening. 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 those properties on the LDAP server. If you want to use secure authentication, port 636 is usually used.

- **LDAP Version**—ACS uses LDAP version 3 or version 2 to communicate with your LDAP database. If you check this check box, ACS uses LDAP version 3. If it is not checked, ACS uses LDAP version 2.
- **Security**—ACS uses SSL to encrypt communication between ACS and the LDAP server. If you do not enable SSL, user credentials are passed to the LDAP server in clear text. If you select this option, then you must select **Trusted Root CA** or **Certificate Database Path**. ACS supports only server-side authentication for SSL communication with the LDAP server. Solution Engine only: You must be sure that the Port box contains the port number used for SSL on the LDAP server.
- **Trusted Root CA**—LDAP over SSL includes the option to authenticate by using the certificate database files other than the Netscape *cert7.db* file. This option uses the same mechanism as other SSL installations in the ACS environment. Select the certification authority that issued the server certificate that is installed on the LDAP server.
- **Certificate DB Path**—Uses the path to the Netscape *cert7.db* file, which contains the certificates for the server to be queried, and the certificates for the trusted CA.

ACS for Windows

- The path to the Netscape *cert7.db* file. This file must contain the certificates for the server to be queried and the trusted CA. You can use a Netscape web browser to generate *cert7.db* files. For information about generating a *cert7.db* file, refer to Netscape documentation.

To perform secure authentication by using SSL with this option, you must provide a Netscape *cert7.db* certificate database file. ACS requires a certificate database so that it can establish the SSL connection because the certificate database must be local to the ACS Windows server.

ACS SE

- This option provides a link to the Download Certificate Database page. ACS displays information about whether the Netscape *cert7.db* certificate database file has been downloaded to support secure communication to the LDAP server that you specified. For information about the Download Certificate Database page, see [Downloading a Certificate Database \(Solution Engine Only\)](#), page 12-47.

To perform secure authentication by using SSL with this option, you must provide a Netscape *cert7.db* certificate database file. ACS requires a certificate database so that it can establish the SSL connection. Since the certificate database must be local to the Solution Engine, you must use FTP to transfer the certificate database to ACS.

ACS requires a *cert7.db* certificate database file for each LDAP server that you configure. For example, to support users distributed in multiple LDAP trees, you might configure two LDAP instances in ACS that can communicate with the same LDAP servers. Each LDAP instance then has a primary and a secondary LDAP server. Even though the two LDAP configurations share the same primary server, each LDAP configuration requires that you download a certificate database file to ACS.



Note

The database must be a Netscape *cert7.db* certificate database file. No other filename is supported.



Caution

TACACS+ authentications to the back-end LDAP database may not work properly when ACS is operating under a heavy load by using *cert7.db*. TACACS+ services may shut down and authentications cease. The third-party DLL may be unstable and cause exceptions. In addition, Netscape no longer

supports the third-party DLL. The recommended way to work around this problem is to use a secure connection with the OpenSSL infrastructure with a CA root certificate, instead of the *cert7.db*. In this ACS release, Cisco has fully tested and supports this method.

- **Admin DN**—The DN of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree. It must contain the following information about your LDAP server:

uid=*user id*,[*ou=organizational unit*,][*ou=next organizational unit*]o=*organization*

where *user id* is the username, *organizational unit* is the last level of the tree, and *next organizational unit* is the next level up the tree.

For example:

`uid=joesmith,ou=members,ou=administrators,o=cisco`

You can use anonymous credentials for the administrator username if the LDAP server is configured to make the group name attribute visible in searches by anonymous credentials. Otherwise, you must specify an administrator username that permits the group name attribute to be visible to searches.



Note

If the administrator username that you specify does not have permission to see the group name attribute in searches, group mapping fails for users that LDAP authenticates.

- **Password**—The password for the administrator account that you specified in the **Admin DN** box. The LDAP server determines case sensitivity.

Configuring a Generic LDAP External User Database

Creating a generic LDAP configuration provides ACS information that enables it to pass authentication requests to an LDAP database. This information reflects the way that you have implemented your LDAP database and does not dictate how your LDAP database is configured or functions. For information about your LDAP database, refer to your LDAP documentation.

Before You Begin

For information about the options on the LDAP Database Configuration page, see [LDAP Configuration Options, page 12-27](#).

To configure ACS to use the LDAP User Database:

- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration**.
ACS displays a list of all possible external user database types.
- Step 3** Click **Generic LDAP**.



Note

The user authenticates against only one LDAP database.

If no LDAP database configuration exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.

Step 4 If you are creating a configuration:

- a. Click **Create New Configuration**.
- b. Type a name for the new configuration for generic LDAP in the box provided.
- c. Click **Submit**.

ACS lists the new configuration in the External User Database Configuration table.

Step 5 Under External User Database Configuration, select the name of the LDAP database that to configure.



Note If only one LDAP configuration exists, the name of that configuration appears instead of the list. Proceed to Step 6.

Step 6 Click **Configure**.



Caution If you click **Delete**, the configuration of the selected LDAP database is deleted.

Step 7 If you do not want ACS to filter LDAP authentication requests by username, under Domain Filtering, select **Process all usernames**.

Step 8 If you want to limit authentications processed by this LDAP configuration to usernames with a specific domain qualification:



Note For information about domain filtering, see [Domain Filtering, page 12-24](#).

- a. Under Domain Filtering, select **Only process usernames that are domain qualified**.
- b. From the **Qualified by** list, select the applicable type of domain qualification, either **Suffix** or **Prefix**. Only one type of domain qualification is supported per LDAP configuration.

For example, if you want this LDAP configuration to authenticate usernames that begin with a specific domain name, select **Prefix**. If you want this LDAP configuration to authenticate usernames that end with a specific domain name, select **Suffix**.

- c. In the **Domain Qualifier** box, type the name of the domain for which you this LDAP configuration should authenticate usernames. Include the delimiting character that separates the user ID from the domain name. Ensure that the delimiting character appears in the applicable position: at the end of the domain name if **Prefix** is selected on the **Qualified by** list; at the beginning of the domain name if **Suffix** is selected on the **Qualified by** list.

Only one domain name is supported per LDAP configuration. You can type up to 512 characters.

- d. If you want ACS to remove the domain qualifier before submitting it to the LDAP database, check the **Strip domain before submitting username to LDAP server** check box.
- e. If you want ACS to pass the username to the LDAP database *without* removing the domain qualifier, clear the **Strip domain before submitting username to LDAP server** check box.

Step 9 If you want to enable ACS to strip domain qualifiers from usernames before submitting them to an LDAP server:

**Note**

For information about domain filtering, see [Domain Filtering, page 12-24](#).

- a. Under Domain Filtering, select **Process all usernames after stripping domain name and delimiter**.
- b. If you want ACS to strip prefixed domain qualifiers, check the **Strip starting characters through the last X character** check box, and then type the domain-qualifier delimiting character in the X box.

**Note**

The X 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 X box contains any of these characters, stripping fails.

- c. If you want ACS to strip suffixed domain qualifiers, check the **Strip ending characters from the first X character** check box, and then type the domain-qualifier delimiting character in the X box.

**Note**

The X 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 X box contains any of these characters, stripping fails.

- Step 10** Under Common LDAP Configuration, in the **User Directory Subtree** box, type the DN of the tree containing all your users.
- Step 11** In the **Group Directory Subtree** box, type the DN of the subtree containing all your groups.
- Step 12** In the **User Object Type** box, type the name of the attribute in the user record that contains the username. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation.

**Note**

The default values in the UserObjectType and following fields reflect the default configuration of the Netscape Directory Server. Confirm all values for these fields with your LDAP server configuration and documentation.

- Step 13** In the **User Object Class** box, type the value of the LDAP `objectType` attribute that identifies the record as a user. Often, user records have several values for the `objectType` attribute, some of which are unique to the user, some of which are shared with other object types. Select a value that is not shared.
- Step 14** In the **GroupObjectType** box, type the name of the attribute in the group record that contains the group name.
- Step 15** In the **GroupObjectClass** box, type a value of the LDAP `objectType` attribute in the group record that identifies the record as a group.
- Step 16** In the **GroupAttributeName** box, type the name of the attribute of the group record that contains the list of user records who are a member of that group.
- Step 17** In the **Server Timeout** box, type the number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server has failed.
- Step 18** To enable failover of LDAP authentication attempts, check the **On Timeout Use Secondary** check box. For more information about the LDAP failover feature, see [LDAP Failover, page 12-25](#).

- Step 19** In the **Failback Retry Delay** box, type the number of minutes after the primary LDAP server fails to authenticate a user that ACS resumes sending authentication requests to the primary LDAP server first.



Note To specify that ACS should always use the primary LDAP server first, type zero (0) in the **Failback Retry Delay** box.

- Step 20** In the **Max. Admin Connection** box, enter the number of maximum concurrent connections with LDAP administrator account permissions.

- Step 21** For the Primary LDAP Server and Secondary LDAP Server tables:



Note If you did not check the On Timeout Use Secondary check box, you do not need to complete the options in the Secondary LDAP Server table.

- a. In the **Hostname** box, type the name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.
- b. In the **Port** box, type the TCP/IP port number on which the LDAP server is listening. 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 those properties on the LDAP server. If you want to use secure authentication, port 636 is usually used.
- c. To specify that ACS should use LDAP version 3 to communicate with your LDAP database, check the **LDAP Version** check box. If the LDAP Version check box is not checked, ACS uses LDAP version 2.
- d. If you want ACS to use SSL to connect to the LDAP server, check the **Use secure authentication** check box and complete the next three steps. If you do not use SSL, the username and password credentials are normally passed over the network to the LDAP directory in clear text.
- e. Solution Engine only: If you checked the **Use Secure authentication** check box, perform one of the following procedures:
 - Check the **Trusted Root CA** check box, and in the adjacent drop-down list, select a **Trusted Root CA**.
 - Check the **Certificate Database Path** check box, and download a *cert7.db* file.



Note To download a *cert7.db* certificate database file to ACS now, complete the steps in [Downloading a Certificate Database \(Solution Engine Only\)](#), page 12-47, and then continue with step f. You can download a certificate database later. Until a certificate database is downloaded for the current LDAP server, secure authentication to this LDAP server fails.

- f. ACS for Windows only: If you checked the **Use Secure authentication** check box, perform one of the following procedures:
 - Click the **Trusted Root CA** button, and in the adjacent drop-down list, select a **Trusted Root CA**.
 - Click the **Certificate Database Path** button, and in the adjacent box, type the path to the Netscape *cert7.db* file, which contains the certificates for the server to be queried and the trusted CA.
- g. The Admin DN box requires the fully qualified (DN) of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree.

In the **Admin DN** box, type the following information from your LDAP server:

```
uid=user id, [ou=organizational unit, ]
[ou=next organizational unit] o=organization
```

where *user id* is the username

organizational unit is the last level of the tree

next organizational unit is the next level up the tree.

For example:

```
uid=joesmith,ou=members,ou=administrators,o=cisco
```



Tip

If you are using Netscape DS as your LDAP software, you can copy this information from the Netscape console.

- h. In the **Password** box, type the password for the administrator account that is specified in the Admin DN box. The server determines password case sensitivity.

Step 22 Click **Submit**.

ACS saves the generic LDAP configuration that you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see [About Unknown User Authentication, page 15-3](#). For more information about configuring user accounts to authenticate by using this database, see [Chapter 6, “User Management.”](#)

ODBC Database (ACS for Windows Only)

As with Windows user database support, you can use ACS ODBC-compliant relational database support to use existing user records in an external ODBC-compliant relational database. Configuring ACS to authenticate against an ODBC-compliant relational database does not affect the configuration of the relational database. To manage your relational database, refer to your relational database documentation.



Note

As with all other external databases that ACS supports, the ODBC-compliant relational database is not supplied as part of ACS. For general guidance with setting up your ODBC external user database, see [Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 12-37](#).

You can use the Windows ODBC feature to create a data source name (DSN), which specifies the database and other important parameters that are necessary for communicating with the database. Among the parameters that you provide are the username and password that are required for the ODBC driver to gain access to your ODBC-compliant relational database.

This section contains:

- [What is Supported with ODBC User Databases, page 12-36](#)
- [ACS Authentication Process with an ODBC External User Database, page 12-36](#)
- [Preparing to Authenticate Users with an ODBC-Compliant Relational Database, page 12-37](#)
- [Implementation of Stored Procedures for ODBC Authentication, page 12-38](#)
- [Microsoft SQL Server and Case-Sensitive Passwords, page 12-39](#)

- [Sample Routine for Generating a PAP Authentication SQL Procedure, page 12-39](#)
- [Sample Routine for Generating an SQL CHAP Authentication Procedure, page 12-40](#)
- [Sample Routine for Generating an EAP-TLS Authentication Procedure, page 12-40](#)
- [PAP Authentication Procedure Input, page 12-40](#)
- [PAP Procedure Output, page 12-41](#)
- [CHAP/MS-CHAP/ARAP Authentication Procedure Input, page 12-41](#)
- [CHAP/MS-CHAP/ARAP Procedure Output, page 12-42](#)
- [EAP-TLS Authentication Procedure Input, page 12-42](#)
- [EAP-TLS Procedure Output, page 12-43](#)
- [Result Codes, page 12-43](#)
- [Configuring a System Data Source Name for an ODBC External User Database, page 12-44](#)
- [Configuring an ODBC External User Database, page 12-44](#)

What is Supported with ODBC User Databases

ACS supports the use of ODBC external user databases for:

- **Authentication**—For information about the types of authentication that ACS supports by using a relational database via the ODBC authenticator feature, see [Authentication Protocol-Database Compatibility, page 1-8](#).
- **Group Specification**—ACS supports group assignment for users who are authenticated by an ODBC user database. Authentication queries to the ODBC database must contain the group number to which you want to assign a user. For unknown users authenticated by an ODBC user database, group specification overrides group mapping.

For more information about expected query output, see [PAP Procedure Output, page 12-41](#), [CHAP/MS-CHAP/ARAP Procedure Output, page 12-42](#), and [EAP-TLS Procedure Output, page 12-43](#).

- **Group Mapping for Unknown Users**—ACS supports group mapping for unknown users by requesting group membership information from Windows user databases. For more information about group mapping for users who are authenticated with a Windows user database, see [Group Mapping by Group Set Membership, page 16-3](#).

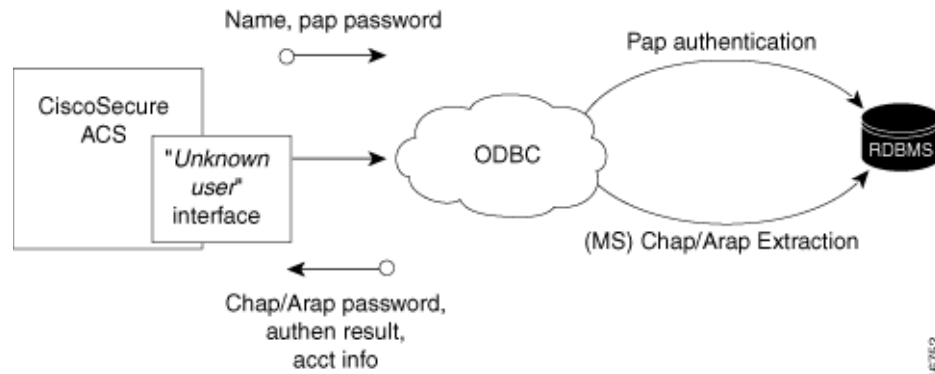
ACS Authentication Process with an ODBC External User Database

ACS forwards user authentication requests to an ODBC database when the user:

- Account in the ACS internal database lists an ODBC database configuration as the authentication method.
- Is unknown to the ACS internal database, and the Unknown User Policy dictates that an ODBC database is the next external user database to try.

In either case, ACS forwards user credentials to the ODBC database via an ODBC connection. The relational database must have a stored procedure that queries the appropriate tables and returns values to ACS. If the returned values indicate that the user credentials that were provided are valid, ACS instructs the requesting AAA client to grant the user access; otherwise, ACS denies the user access ([Figure 12-2](#)).

Figure 12-2 Using the ODBC Database for Authentication





ACS grants authorization based on the ACS group to which the user is assigned. While the group to which a user is assigned can be determined by information from the ODBC database by using a process known as “group specification,” it is ACS that grants authorization privileges.

Preparing to Authenticate Users with an ODBC-Compliant Relational Database

Authenticating users with an ODBC-compliant relational database requires that you complete several significant steps that are external to ACS before configuring ACS with an ODBC external user database.

To prepare for authenticating with an ODBC-compliant relational database:

-
- Step 1** Install your ODBC-compliant relational database on its server. For more information, refer to the relational database documentation.
-
-  **Note** The relational database that you use is not supplied with ACS.
-
- Step 2** Create the database to hold the usernames and passwords. The database name is irrelevant to ACS, so that you can name the database however you like.
- Step 3** Create the table or tables that will hold the usernames and passwords for your users. The table names are irrelevant to ACS, so you can name the tables and columns however you like.
-
-  **Note** For SQL database columns that hold user passwords, we recommend using **varchar** format. If you define password columns as **char**, password comparison might fail if the password does not use the full length of the field. For example, if a password column is 16 characters wide but the password is only ten characters long, the database might append six spaces. The value used for password comparison then grows to 16 characters, causing comparison to the actual password that the user submitted to fail.
-
- Step 4** Write the stored procedures that are intended to return the required authentication information to ACS. For more information about these stored procedures, see [Implementation of Stored Procedures for ODBC Authentication](#), page 12-38.
- Step 5** Set up a system DSN on the computer that is running ACS. For steps, see [Configuring a System Data Source Name for an ODBC External User Database](#), page 12-44.

- Step 6** Configure ACS to authenticate users with an ODBC database. For steps, see [Configuring an ODBC External User Database, page 12-44](#).
-

Implementation of Stored Procedures for ODBC Authentication

When you configure ACS to authenticate users against an ODBC-compliant relational database, you must create a stored procedure to perform the necessary query and return the values that ACS expects. The values that are returned and the tasks that are required of the stored procedure vary depending on the authentication protocol used.

Authentication for PAP, or PEAP (EAP-GTC) occurs within the relational database; that is, if the stored procedure finds a record with the username and the password matching the input, the user is considered authenticated.

Authentication for CHAP, MS-CHAP, ARAP, LEAP, or EAP-MD5 occurs within ACS. The stored procedure returns the fields for the record with a matching username, including the password. ACS confirms or denies authentication based on the values that are returned from the procedure.

Authentication for EAP-TLS occurs within ACS. The stored procedure returns the field for the record, indicating whether it found the username in the ODBC database. ACS confirms or denies authentication based on the values that are returned from the procedure and on the validity of the user certificate. For more information about ACS support for the EAP-TLS protocol, see [EAP-TLS Authentication, page 9-2](#).

To support the three sets of protocols, ACS provides different input to, and expects different output from, the ODBC authentication request. This feature requires a separate stored procedure in the relational database to support each of the three sets of protocols.

The ACS product CD contains **stub** routines for creating a procedure in Microsoft SQL Server or an Oracle database. You can modify a copy of these routines to create your stored procedure or write your own. You can see example routines for creating PAP and CHAP/MS-CHAP/ARAP authentication stored procedures in SQL Server in [Sample Routine for Generating a PAP Authentication SQL Procedure, page 12-39](#), and [Sample Routine for Generating an SQL CHAP Authentication Procedure, page 12-40](#).

The following sections provide reference information about ACS data types versus SQL data types, PAP/PEAP (EAP-GTC) authentication procedure input and output, CHAP/MS-CHAP/ARAP authentication procedure input and output, EAP-TLS authentication procedure input and output, and expected result codes. You can use this information while writing your authentication stored procedures in your relational database.



Note

Two stored procedures are required when using EAP-FAST; MS-CHAP (used for phase zero provisioning) and PAP (used for phase two authentication).

Type Definitions

The ACS types and their matching SQL types are:

- **Integer**—SQL_INTEGER
- **String**—SQL_CHAR or SQL_VARCHAR

**Note**

For SQL database columns that hold user passwords, we recommend using **varchar** format. If you define password columns as **char**, password comparison might fail if the password does not use the full length of the field. For example, if a password column is 16 characters wide but the password is only ten characters long, the database might append six spaces. The value used for password comparison then grows to 16 characters, causing comparison to the actual password that the user submitted to fail.

Microsoft SQL Server and Case-Sensitive Passwords

If you want your passwords to be case sensitive and are using Microsoft SQL Server as your ODBC-compliant relational database, configure your SQL Server to accommodate this feature. If your users are authenticating by using PPP via PAP or Telnet login, the password might not be case sensitive, depending on how you set the case-sensitivity option on the SQL Server. For example, an Oracle database will default to case sensitive, whereas Microsoft SQL Server defaults to case insensitive. However, in the case of CHAP/ARAP, the password is case sensitive if you configured the CHAP stored procedure.

For example, with Telnet or PAP authentication, the passwords **cisco** or **CISCO** or **CiScO** will all work if you configure the SQL Server to be case insensitive.

For CHAP/ARAP, the passwords **cisco** or **CISCO** or **CiScO** are not the same, regardless of whether the SQL Server is configured for case-sensitive passwords.

Sample Routine for Generating a PAP Authentication SQL Procedure

The following example routine creates a procedure named **CSNTAuthUserPap** in Microsoft SQL Server, the default procedure that ACS uses for PAP authentication. Table and column names that could vary for your database schema appear in variable text. For your convenience, the ACS product CD includes a stub routine for creating a procedure in SQL Server or Oracle. For more information about data type definitions, procedure parameters, and procedure results, see [ODBC Database \(ACS for Windows Only\), page 12-35](#).

```
if exists (select * from sysobjects where id = object_id ('dbo.CSNTAuthUserPap') and
sysstat & 0xf = 4)drop procedure dbo.CSNTAuthUserPap
GO
```

```
CREATE PROCEDURE CSNTAuthUserPap
@username varchar(64), @pass varchar(255)
AS
SET NOCOUNT ON
IF EXISTS( SELECT  username
FROM  users
WHERE  username  = @username
AND   csntpassword = @pass )
SELECT 0,csntgroup,csntacctinfo,"No Error"
FROM  users
WHERE  username  = @username
ELSE
SELECT 3,0,"odbc","ODBC Authen Error"
GO

GRANT EXECUTE ON dbo.CSNTAuthUserPap TO ciscosecure
GO
```

Sample Routine for Generating an SQL CHAP Authentication Procedure

The following example routine creates in Microsoft SQL Server a procedure named **CSNTExtractUserClearTextPw**, the default procedure that ACS uses for CHAP/MS-CHAP/ARAP authentication. Table and column names that could vary for your database schema appear in variable text. For more information about data type definitions, procedure parameters, and procedure results, see [ODBC Database \(ACS for Windows Only\), page 12-35](#).

```
if exists (select * from sysobjects where id = object_id('dbo.CSNTExtractUserClearTextPw')
and sysstat & 0xf = 4) drop procedure dbo.CSNTExtractUserClearTextPw
GO

CREATE PROCEDURE CSNTExtractUserClearTextPw
@username varchar(64)
AS
SET NOCOUNT ON
IF EXISTS( SELECT  username
FROM  users
WHERE  username  = @username )
SELECT  0,csntgroup,csntacctinfo,"No Error",csntpassword
FROM  users
WHERE  username  = @username
ELSE
SELECT  3,0,"odbc","ODBC Authen Error"
GO

GRANT EXECUTE ON dbo.CSNTExtractUserClearTextPw TO ciscosecure
GO
```

Sample Routine for Generating an EAP-TLS Authentication Procedure

The following example routine creates in Microsoft SQL Server a procedure named **CSNTFindUser**, the default procedure that ACS uses for EAP-TLS authentication. Table and column names that could vary for your database schema appear in variable text. For more information about data type definitions, procedure parameters, and procedure results, see [ODBC Database \(ACS for Windows Only\), page 12-35](#).

PAP Authentication Procedure Input

[Table 12-1](#) details the input that ACS provides to the stored procedure that supports PAP authentication. The stored procedure should accept the named input values as variables.

Table 12-1 *PAP Stored Procedure Input*

Field	Type	Explanation
CSNTusername	String	0-64 characters
CSNTpassword	String	0-255 characters

The input names are for guidance only. Procedure variables that are created from them can have different names; however, you must define them in the procedure in the order shown: the username must precede the password variable.

PAP Procedure Output

The stored procedure must return a single row that contains the nonnull fields.

Table 12-2 lists the procedure results that ACS expects as output from stored procedure.

Table 12-2 PAP Stored Procedure Results

Field	Type	Explanation
CSNTresult	Integer	See Table 12-7.
CSNTgroup	Integer	The ACS group number for authorization. You use 0xFFFFFFFF to assign the default value. Values other than 0-499 are converted to the default. Note The group that is specified in the CSNTgroup field overrides group mapping that is configured for the ODBC external user database.
CSNTacctInfo	String	0-16 characters. A customer-defined string that ACS adds to subsequent account log file entries.
CSNTerrorString	String	0-255 characters. A customer-defined string that ACS writes to the CSAuth service log file if an error occurs.

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The CSNTerrorString file is logged only after a failure (if the result is greater than or equal to 4).



Note

If the ODBC database returns data in **recordset** format rather than in parameters, the procedure must return the result fields in the order previously listed.

CHAP/MS-CHAP/ARAP Authentication Procedure Input

ACS provides a single value for input to the stored procedure that supports CHAP/MS-CHAP/ARAP authentication. The stored procedure should accept the named input value as a variable.



Note

Because ACS performs authentication for CHAP/MS-CHAP/ARAP, the user password is not an input (Table 12-3).

Table 12-3 CHAP Stored Procedure Input

Field	Type	Explanation
CSNTusername	String	0-64 characters

The input name is for guidance only. A procedure variable that is created from it can have a different name.

CHAP/MS-CHAP/ARAP Procedure Output

The stored procedure must return a single row that contains the nonnull fields.

[Table 12-4](#) lists the procedure results that ACS expects as output from a stored procedure.

Table 12-4 CHAP/MS-CHAP/ARAP Stored Procedure Results

Field	Type	Explanation
CSNTresult	Integer	See Table 12-7 Result Codes.
CSNTgroup	Integer	The ACS group number for authorization. You use 0xFFFFFFFF to assign the default value. Values other than 0-499 are converted to the default. Note The group that is specified in the CSNTgroup field overrides group mapping that is configured for the ODBC external user database.
CSNTacctInfo	String	0-15 characters. A customer-defined string that ACS adds to subsequent account log file entries.
CSNTerrorString	String	0-255 characters. A customer-defined string that ACS writes to the CSAuth service log file if an error occurs.
CSNTpassword	String	0-255 characters. ACS authenticates the password. Note If the password field in the database is defined by using a char datatype rather than varchar , the database might return a string that is 255 characters long; regardless of actual password length. We recommend using the varchar datatype for the CHAP password field in your ODBC database.

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The CSNTerrorString file is logged only after a failure (if the result is greater than or equal to 4).



Note

If the ODBC database returns data in **recordset** format rather than in parameters, the procedure must return the result fields in the order previously listed.

EAP-TLS Authentication Procedure Input

ACS provides a single value for input to the stored procedure that supports EAP-TLS authentication. The stored procedure should accept the named input value as a variable.



Note

Because ACS performs authentication for EAP-TLS, the user password is not an input ([Table 12-3](#)).

Table 12-5 EAP-TLS Stored Procedure Input

Field	Type	Explanation
CSNTusername	String	0-64 characters

The input name is for guidance only. A procedure variable that is created from it can have a different name.

EAP-TLS Procedure Output

The stored procedure must return a single row that contains the nonnull fields.

Table 12-4 lists the procedure results that ACS expects as output from stored procedure.

Table 12-6 *EAP-TLS Stored Procedure Results*

Field	Type	Explanation
CSNTresult	Integer	See Table 12-7 Result Codes.
CSNTgroup	Integer	The ACS group number for authorization. You use 0xFFFFFFFF to assign the default value. Values other than 0-499 are converted to the default. Note The group that is specified in the CSNTgroup field overrides group mapping that is configured for the ODBC external user database.
CSNTacctInfo	String	0-15 characters. A customer-defined string that ACS adds to subsequent account log file entries.
CSNTerrorString	String	0-255 characters. A customer-defined string that ACS writes to the CSAuth service log file if an error occurs.

The CSNTGroup and CSNTacctInfo fields are processed only after a successful authentication. The CSNTerrorString file is logged only after a failure (if the result is greater than or equal to 4).



Note

If the ODBC database returns data in **recordset** format, rather than in parameters, the procedure must return the result fields in the order previously listed.

Result Codes

You can set the result codes that are listed in Table 12-7.

Table 12-7 *Result Codes*

Result Code	Meaning
0 (zero)	Authentication successful
1	Unknown username
2	Invalid password
3	Unknown username or invalid password
4+	Internal error—authentication not processed

The SQL procedure can decide among 1, 2, or 3 to indicate a failure, depending on how much information that you want the failed authentication log files to include.

A return code of 4 or higher results in an authentication error event. These errors do not increment per-user failed attempt counters. Additionally, error codes are returned to the AAA client so it can distinguish between errors and failures and, if configured to do so, fall back to a backup AAA server.

Successful or failed authentications are not logged; general ACS logging mechanisms apply. In the event of an error (CSNTresult equal to or less than 4), the contents of the CSNTerrorString are written to the Windows Event Log under the Application Log.

Configuring a System Data Source Name for an ODBC External User Database

On the computer that is running ACS, you must create a system DSN for ACS to communicate with the relational database.

To create a system DSN for use with an ODBC external user database:

-
- Step 1** Using the local administrator account, log in to the computer that is running ACS.
 - Step 2** In the Windows Control Panel, double-click the **ODBC Data Sources** icon.
 - Step 3** Choose **Start > Settings > Control Panel > Administrative Tools > Data Sources (ODBC)**.



Tip If the Control Panel is not expanded on the **Start** menu, choose **Start > Settings > Control Panel**, double-click **Administrative Tools**, and then double-click **Data Sources (ODBC)**.

The ODBC Data Source Administrator window appears.

- Step 4** Click the **System DSN** tab.
- Step 5** Click **Add**.
- Step 6** Select the driver that you use with your new DSN, and then click **Finish**.
A dialog box displays fields that require information that is specific to the ODBC driver that you selected.
- Step 7** Type a descriptive name for the DSN in the **Data Source Name** box.
- Step 8** Complete the other fields that the ODBC driver that you selected requires. These fields might include information such as the IP address of the server on which the ODBC-compliant database runs.
- Step 9** Click **OK**.

The name that you assigned to the DSN appears in the System Data Sources list.

- Step 10** Close the ODBC Data Source Administrator window and the Windows Control Panel.

The system DSN that ACS will use for communication with the relational database is created on the computer that is running ACS.


Configuring an ODBC External User Database


Creating an ODBC database configuration provides ACS with information that it uses to pass authentication requests to an ODBC-compliant relational database. This information reflects the way that you have implemented your relational database, and does not dictate how your relational database is configured or functions. For information about your relational database, refer to your relational documentation.




Note Before performing this procedure, you should have completed the steps in [Preparing to Authenticate Users with an ODBC-Compliant Relational Database](#), page 12-37.

To configure ACS for ODBC authentication:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration**.
ACS lists all possible external user database types.
- Step 3** Click **External ODBC Database**.
- Step 4** If you are creating a configuration:
- Click **Create New Configuration**.
 - Type a name for the new configuration for ODBC authentication in the box provided, or accept the default name in the box.
 - Click **Submit**.
- ACS lists the new configuration in the External User Database Configuration table.
- Step 5** Click **Configure**.
- Step 6** From the System DSN list, select the DSN that is configured to communicate with the ODBC-compliant relational database that you want to use.
- 

Note If you have not configured the computer that is running ACS with a DSN for the relational database, do so before completing these steps. For more information about creating a DSN for ACS ODBC authentication, see [Configuring a System Data Source Name for an ODBC External User Database, page 12-44](#).
-
- Step 7** In the **DSN Username** box, type the username that is required to perform transactions with your ODBC database.
- Step 8** In the **DSN Password** box, type the password that is required to perform transactions with your ODBC database.
- Step 9** In the **DSN Connection Retries** box, type the number of times that ACS should try to connect to the ODBC database before timing out. The default is 3.
- 

Note If you have connection problems when Windows starts, increase the default value.
-
- Step 10** To change the ODBC worker thread count, in the **ODBC Worker Threads** box, type the number of ODBC worker threads. The maximum thread count is 10. The default is 1.
- 

Note Increase the ODBC worker thread count only if the ODBC driver that you are using is certified thread safe. For example, the Microsoft Access ODBC driver is not thread safe and can cause ACS to become unstable if multiple threads are used. Where possible, ACS queries the driver to find out if it is thread safe. The thread count to use is a factor of how long the DSN takes to execute the procedure and the rate at which authentications are required.
-
- Step 11** From the DSN Procedure Type list, select the type of output that your relational database provides. Different databases return different output:
- Returns Recordset**—The database returns a raw record set in response to an ODBC query. Microsoft SQL Server responds in this manner.

- **Returns Parameters**—The database returns a set of named parameters in response to an ODBC query. Oracle databases respond in this manner.

Step 12 To support PAP or PEAP (EAP-GTC) authentication with the ODBC database:

- Check the **Support PAP authentication** check box.
- In the **PAP SQL Procedure** box, type the name of the PAP SQL procedure routine that runs on the ODBC server. The default value in this box is **CSNTAuthUserPap**. If you named the PAP SQL procedure something else, change this entry to match the name given to the PAP SQL procedure. For more information and an example routine, see [Sample Routine for Generating a PAP Authentication SQL Procedure](#), page 12-39.



Note

If you enabled PAP authentication, the PAP authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the **PAP SQL Procedure** box. If it does not, be certain to create it in the ODBC database before attempting to authenticate users against the ODBC database.

Step 13 To support CHAP, MS-CHAP, ARAP, EAP-MD5, or LEAP authentication with the ODBC database:

- Check the **Support CHAP/MS-CHAP/ARAP Authentication** check box.
- In the **CHAP SQL Procedure** box, type the name of the CHAP SQL procedure routine on the ODBC server. The default value in this box is **CSNTExtractUserClearTextPw**. If you named the CHAP SQL procedure something else, change this entry to match the name given to the CHAP SQL procedure. For more information and an example routine, see [Sample Routine for Generating an SQL CHAP Authentication Procedure](#), page 12-40.



Note

If you enabled CHAP/MS-CHAP/ARAP authentication, the CHAP authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the **PAP SQL Procedure** box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

Step 14 To support EAP-TLS authentication with the ODBC database:

- Check the **Support EAP-TLS Authentication** check box.
- In the **EAP-TLS SQL Procedure** box, type the name of the EAP-TLS SQL procedure routine on the ODBC server. The default value in this box is **CSNTFindUser**. If you named the EAP-TLS SQL procedure something else, change this entry to match the name given to the EAP-TLS SQL procedure. For more information and an example routine, see [Sample Routine for Generating an EAP-TLS Authentication Procedure](#), page 12-40.



Note

If you enabled EAP-TLS authentication, the EAP-TLS authentication SQL procedure must exist on the ODBC database and must have the exact name specified in the **EAP-TLS SQL Procedure** box. If it does not, be sure to create it in the ODBC database before attempting to authenticate users against the ODBC database.

Step 15 To configure the RADIUS behavior if the database fails:

- Choose **Send an access reject** for the devices to retry the same server.
- Choose **Discard the access request** for the devices to try to access other servers.

**Note**

This option is useful in the event of an external ODBC database failure, whereas ACS can deny the authentication (access-reject), or, not respond at all. Conversely, if ACS discards an access-request, the network access device can fail over to another ACS server. A drawback to this approach is that discards can cause excessive network traffic and load on the network access devices as requests continue to travel from network access devices to the ACS servers.

Step 16 Click **Submit**.

ACS saves the ODBC configuration that you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see [About Unknown User Authentication, page 15-3](#). For more information about configuring user accounts to authenticate by using this database, see [Chapter 6, “User Management.”](#)

Downloading a Certificate Database (Solution Engine Only)

Before You Begin

The database must be a Netscape *cert7.db* certificate database file generated by a Netscape web browser. No other filename is supported. For information about generating a Netscape *cert7.db* file, refer to Netscape documentation.

To download a certificate database for a primary or a secondary LDAP server:

**Note**

Downloading a certificate database is a part of the larger process that configures an LDAP external user database. For more information, see [Configuring a Generic LDAP External User Database, page 12-31](#).

Step 1 To access the Download Certificate Database page:

- a. Open the LDAP Database Configuration page that contains the information for the LDAP server whose certificate database file you want to download.

**Note**

If you are already on the applicable LDAP Database Configuration page, go to Step b.

- b. For the LDAP server whose certificate database file you want to download, click **Download Certificate Database**.

**Note**

ACS lists a primary and secondary LDAP server for each LDAP database configuration. To support secure authentication to both servers, you must download a certificate database file twice, once for the primary LDAP server and once for the secondary LDAP server.

Step 2 In the **FTP Server** box, enter the IP address or hostname of the FTP server. The FTP Server box accepts a maximum of 512 characters.**Note**

Providing the hostname requires that DNS is correctly operating on your network.

- Step 3** In the **Login** box, enter a valid username to enable ACS to access the FTP server. The Login box accepts a maximum of 512 characters.
- Step 4** In the **Password** box, enter the password for the username provided in the Login box. The Password box accepts a maximum of 512 characters.
- Step 5** In the **Directory** box, enter the path to the Netscape *cert7.db* file. The path is relative to the starting directory at login to the FTP server.
- For example, if the Netscape *cert7.db* file is located in `c:\ACS-files\LDAPcertdb` and the user provided in the Login box starts its FTP sessions in `c:\`, you then type `ACS-files\LDAPcertdb`.
- The Directory box accepts a maximum of 512 characters.
- Step 6** Click **Download**.
- ACS downloads the Netscape *cert7.db* file from the FTP server. ACS displays the LDAP Database Configuration page.
-

LEAP Proxy RADIUS Server Database (Both Platforms)

For ACS-authenticated users who access your network via Cisco Aironet devices, ACS supports authentication with a proxy RADIUS server. For information about the types of authentication that ACS supports with a proxy RADIUS server, see [Authentication Protocol-Database Compatibility, page 1-8](#). This feature is useful if your own RADIUS-based user database can support MS-CHAP but not LEAP/EAP-FAST. ACS manages the LEAP/EAP-FAST protocol handling and forwards just the MS-CHAP authentication to your server.

ACS uses MS-CHAP Version 1 for LEAP Proxy RADIUS Server authentication. With LEAP Proxy, only the MS-CHAP authentication is proxied to the remote server in a separate RADIUS access request. To manage your proxy RADIUS database, refer to your RADIUS database documentation.

You can use the LEAP proxy RADIUS server authentication to authenticate users against existing Kerberos databases that support MS-CHAP authentication. You can use the LEAP Proxy RADIUS Server database to authenticate users with any third-party RADIUS server that supports MS-CHAP authentication.



Note

The third-party RADIUS server must return Microsoft Point-to-Point Encryption (MPPE) keys in the Microsoft RADIUS vendor-specific attribute (VSA) `MS-CHAP-MPPE-Keys` (VSA 12). If the third-party RADIUS server does not return the MPPE keys, the authentication fails and is logged in the Failed Attempts log.

ACS supports RADIUS-based group specification for users who are authenticated by LEAP Proxy RADIUS Server databases. The RADIUS-based group specification overrides group mapping. For more information, see [RADIUS-Based Group Specification, page 16-8](#).

ACS supports group mapping for unknown users who are authenticated by LEAP Proxy RADIUS Server databases. Group mapping is only applied to an unknown user if RADIUS-based group specification did not occur. For more information about group mapping of users who are authenticated by a LEAP Proxy RADIUS Server database, see [Group Mapping by External User Database, page 16-1](#).

Configuring a LEAP Proxy RADIUS Server External User Database

You should install and configure your proxy RADIUS server before configuring ACS to authenticate users with it. For information about installing the proxy RADIUS server, refer to the documentation that is included with your RADIUS server.

To configure LEAP proxy RADIUS authentication:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration**.
ACS lists all possible external user database types.
- Step 3** Click **LEAP Proxy RADIUS Server**.
If no LEAP Proxy RADIUS Server configuration exists, only the Database Configuration Creation table appears. Otherwise, in addition to the Database Configuration Creation table, the External User Database Configuration table appears.
- Step 4** If you are creating a configuration:
- Click **Create New Configuration**.
 - Type a name for the new configuration for the LEAP Proxy RADIUS Server in the box provided, or accept the default name in the box.
 - Click **Submit**.
ACS lists the new configuration in the External User Database Configuration table.
- Step 5** Under External User Database Configuration, select the name of the LEAP Proxy RADIUS Server database that you configure.



Note If only one LEAP Proxy RADIUS Server configuration exists, the name of that configuration appears instead of the list. Proceed to Step 6.

- Step 6** Click **Configure**.
- Step 7** In the following boxes, type the required information:
- **Primary Server Name/IP**—IP address of the primary proxy RADIUS server.
 - **Secondary Server Name/IP**—IP address of the secondary proxy RADIUS server.
 - **Shared Secret**—The shared secret of the proxy RADIUS server. This must be identical to the shared secret with which the proxy RADIUS server is configured.
 - **Authentication Port**—The UDP port over which the proxy RADIUS server conducts authentication sessions. If the LEAP Proxy RADIUS server is installed on the same Windows server as ACS, this port should not be the same port that ACS uses for RADIUS authentication. For more information about the ports that ACS uses for RADIUS, see [RADIUS, page 1-4](#).
 - **Timeout (seconds)**—The number of seconds that ACS waits before sending notification to the user that the authentication attempt has timed out.
 - **Retries**—The number of authentication attempts ACS makes before failing over to the secondary proxy RADIUS server.
 - **Failback Retry Delay (minutes)**—The number of minutes after which ACS attempts authentications by using a failed primary proxy RADIUS server.

**Note**

If the primary and the secondary servers fail, ACS alternates between the servers until one responds.

Step 8 Click **Submit**.

ACS saves the proxy RADIUS token server database configuration that you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see [About Unknown User Authentication, page 15-3](#). For more information about configuring user accounts to authenticate by using this database, see [Chapter 6, “User Management.”](#)

Token Server User Databases

ACS supports the use of token servers for the increased security that one-time passwords (OTPs) provide.

This section contains:

- [About Token Servers and ACS, page 12-50](#)
- [RADIUS-Enabled Token Servers, page 12-51](#)
- [Using RSA Token-Card Client Software, page 12-54](#)

About Token Servers and ACS

For information about the types of authentication that ACS supports with token servers, see [Authentication Protocol-Database Compatibility, page 1-8](#).

Requests from the AAA client are first sent to ACS. If ACS has been configured to authenticate against a token server and finds the username, it forwards the authentication request to the token server. If it does not find the username, ACS checks the database that is configured to authenticate unknown users. If the request for authentication is passed, the appropriate authorizations are forwarded to the AAA client along with the approved authentication. ACS then maintains the accounting information.

ACS for Windows Only

ACS acts as a client to the token server. For all token servers except RSA SecurID, ACS acts as a client by using the RADIUS interface of the token server. For more information about ACS support of token servers with a RADIUS interface, see [RADIUS-Enabled Token Servers, page 12-51](#).

For RSA SecurID, ACS uses an RSA proprietary API. For more information about ACS support of RSA SecurID token servers, see [Using RSA Token-Card Client Software, page 12-54](#).

Solution Engine Only

ACS acts as a client to the token server. For all token servers, ACS acts as a client by using the RADIUS interface of the token server. For more information about ACS support of token servers with a RADIUS interface, see [RADIUS-Enabled Token Servers, page 12-51](#).

Token Servers and ISDN

ACS supports token caching for ISDN terminal adapters and routers. One inconvenience of using token cards for OTP authentication with ISDN is that each B channel requires its own OTP. Therefore, a user must enter at least 2 OTPs, plus any other login passwords, such as those for Windows networking. If the terminal adapter supports the ability to turn on and off the second B channel, users might have to enter many OTPs each time the second B channel comes into service.

ACS caches the token to help make the OTPs easier for users. Therefore, if a token card is being used to authenticate a user on the first B channel, you can set a specified period during which the second B channel can come into service without requiring the user to enter another OTP. To lessen the risk of unauthorized access to the second B channel, you can limit the time that the second B channel is up. Furthermore, you can configure the second B channel to use the CHAP password that is specified during the first login to further lessen the chance of a security problem. When the first B channel is dropped, the cached token is erased.

RADIUS-Enabled Token Servers

This section describes support for token servers that provide a standard RADIUS interface.

This section contains:

- [About RADIUS-Enabled Token Servers, page 12-51](#)
- [Token Server RADIUS Authentication Request and Response Contents, page 12-51](#)
- [Configuring a RADIUS Token Server External User Database, page 12-52](#)

About RADIUS-Enabled Token Servers

ACS supports token servers by using the RADIUS server that is built into the token server. Rather than using a vendor-proprietary API, ACS sends standard RADIUS authentication requests to the RADIUS authentication port on the token server. This feature enables ACS to support any IETF RFC 2865-compliant token server.

You can create multiple instances of RADIUS token servers. For information about configuring ACS to authenticate users with one of these token servers, see [Configuring a RADIUS Token Server External User Database, page 12-52](#).

ACS provides a means for specifying a user group assignment in the RADIUS response from the RADIUS-enabled token server. Group specification always takes precedence over group mapping. For more information, see [RADIUS-Based Group Specification, page 16-8](#).

ACS also supports mapping users who are authenticated by a RADIUS-enabled token server to a single group. Group mapping only occurs if group specification does not occur. For more information, see [Group Mapping by External User Database, page 16-1](#).

Token Server RADIUS Authentication Request and Response Contents

When ACS forwards an authentication request to a RADIUS-enabled token server, the RADIUS authentication request contains the following attributes:

- `User-Name` (RADIUS attribute 1)
- `User-Password` (RADIUS attribute 2)
- `NAS-IP-Address` (RADIUS attribute 4)

- `NAS-Port` (RADIUS attribute 5)
- `NAS-Identifier` (RADIUS attribute 32)

ACS expects to receive one of the following three responses:

- **access-accept**—No attributes are required; however, the response can indicate the ACS group to which the user should be assigned. For more information, see [RADIUS-Based Group Specification, page 16-8](#).
- **access-reject**—No attributes required.
- **access-challenge**—Attributes required, per IETF RFC, are:
 - `State` (RADIUS attribute 24)
 - `Reply-Message` (RADIUS attribute 18)


Configuring a RADIUS Token Server External User Database

Use this procedure to configure RADIUS Token Server external user databases.

Before You Begin

You should install and configure your RADIUS token server before configuring ACS to authenticate users with it. For information about installing the RADIUS token server, refer to the documentation included with your token server.

To configure ACS to authenticate users with a RADIUS Token Server:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration**.
- ACS lists all possible external user database types.
- Step 3** Click **RADIUS Token Server**.
- The Database Configuration Creation table appears. If at least one RADIUS token server configuration exists, the External User Database Configuration table also appears.
- Step 4** If you are creating a configuration:
- Click **Create New Configuration**.
 - Type a name for the new configuration for the RADIUS-enabled token server in the box provided, or accept the default name in the box.
 - Click **Submit**.
- ACS lists the new configuration in the External User Database Configuration table.
- Step 5** Under External User Database Configuration, select the name of the RADIUS-enabled token server that you configure.
-  **Note** If only one RADIUS-enabled token server configuration exists, the name of that configuration appears instead of the list. Proceed to [Step 6](#).
- Step 6** Click **Configure**.
- Step 7** In the RADIUS Configuration table, type the required information in the following boxes:

- **Primary Server Name/IP**—The hostname or IP address of the primary RADIUS token server. If you provide the hostname, the hostname must be resolvable by DNS.
- **Secondary Server Name/IP**—The hostname or IP address of the secondary RADIUS token server. If you provide the hostname, the hostname must be resolvable by DNS.
- **Shared Secret**—The shared secret of the RADIUS server. This must be identical to the shared secret with which the RADIUS token server is configured.
- **Authentication Port**—The UDP port over which the RADIUS server conducts authentication sessions. If the RADIUS token server is installed on the same Windows server as ACS, this port should not be the same port that ACS uses for RADIUS authentication. For more information about the ports that ACS uses for RADIUS, see [RADIUS, page 1-4](#).



Note For ACS to send RADIUS OTP messages to a RADIUS-enabled token server, you must ensure that gateway devices between the RADIUS-enabled token server and ACS allow communication over the UDP port that is specified in the Authentication Port box.

- **Timeout (seconds)**—The number of seconds that ACS waits for a response from the RADIUS token server before retrying the authentication request.
- **Retries**—The number of authentication attempts that ACS makes before failing over to the secondary RADIUS token server.
- **Failback Retry Delay (minutes)**—The number of minutes that ACS sends authentication requests to the secondary server when the primary server has failed. When this duration elapses, ACS reverts to sending authentication requests to the primary server.



Note If the primary and the secondary servers fail, ACS alternates between the servers until one responds.

Step 8 If you want to support token users who perform a shell login to a TACACS+ AAA client, you must configure the options in the TACACS+ Shell Configuration table. Perform one of the following procedures:

- If you want ACS to present a custom prompt for tokens, select **Static (sync and async tokens)**, and then type in the **Prompt** box the prompt that ACS will present.

For example, if you type **Enter your PassGo token** in the **Prompt** box, users receive an **Enter your PassGo token** prompt rather than a password prompt.



Note If some tokens that are submitted to this server are synchronous tokens, you must click the **Static (sync and async tokens)** option.

- If you want ACS to send the token server a password to trigger a challenge, select **From Token Server (async tokens only)**, and then, in the **Password** box, type the password that ACS will forward to the token server.

For example, if the token server requires the string **challenge** in order to evoke a challenge, you should type **challenge** in the **Password** box. Users will receive a username prompt and a challenge prompt.



Tip Most token servers accept a blank password as the trigger to send a challenge prompt.



Note You should only click the **From Token Server (async tokens only)** option if all tokens that are submitted to this token server are asynchronous tokens.

Step 9 Click **Submit**.

ACS saves the RADIUS token server database configuration that you created. You can add it to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see [About Unknown User Authentication, page 15-3](#). For more information about configuring user accounts to authenticate by using this database, see [Chapter 6, “User Management.”](#)

Using RSA Token-Card Client Software

ACS supports mapping users who are authenticated by a RSA token server to a single group. For more information, see [Group Mapping by External User Database, page 16-1](#).

ACS supports PPP (ISDN and async) and Telnet for RSA SecurID token servers by acting as a token-card client to the RSA SecurID token server. To use this client you must install the RSA token-card client software on the computer that is running ACS. The following procedure includes the steps that you follow to install the RSA client correctly on the computer that is running ACS.

ACS supports the RSA SecurID token server custom interface for authentication of users. You can create only one RSA SecurID configuration within ACS.

ACS for Windows

Before You Begin

You should install and configure your RSA SecurID token server before configuring ACS to authenticate users with it. For information about installing the RSA SecurID server, refer to the documentation for your token server.

Ensure that you have the applicable RSA ACE Client.

To configure ACS to authenticate users with an RSA token server:

- Step 1** Install the RSA client on the computer that is running ACS:
- With a username that has administrative privileges, log in to the computer that is running ACS.
 - Run the Setup program of the ACE Client software, following the setup instructions that RSA provides.



Note Do not restart Windows when installation is complete.

- Locate the ACE Server data directory, for example, `/sdi/ace/data`.
- Get the file named `sdconf.rec` and place it in the following Windows directory:
`%SystemRoot%\system32`
 For example:
`\winnt\system32`
- Ensure that the ACE server hostname is in the Windows local host file:

`\Windows directory\system32\drivers\etc\hosts`

- f. Restart the computer that is running ACS.
- g. Verify connectivity by running the Test Authentication function of your ACE client application. You can run this from the Control Panel.

Step 2 In the navigation bar, click **External User Databases**.

Step 3 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 4 Click **RSA SecurID Token Server**.

If no RSA SecurID token server configuration exists, the Database Configuration Creation table appears. Otherwise, the External User Database Configuration page appears.

Step 5 If you are creating a configuration:

- a. Click **Create New Configuration**.
- b. Type a name for the new configuration for the RSA SecurID token server in the box provided, or accept the default name in the box.
- c. Click **Submit**.

ACS lists the new configuration in the External User Database Configuration table.

Step 6 Click **Configure**.

ACS displays the name of the token server and the path to the authenticator dynamic link library (DLL). This information confirms that ACS can contact the RSA client. You can add the RSA SecurID external user database to your Unknown User Policy or assign specific user accounts to use this database for authentication. For more information about the Unknown User Policy, see [About Unknown User Authentication, page 15-3](#). For more information about configuring user accounts to authenticate by using this database, see [Chapter 6, "User Management."](#)

ACS for Solution Engine

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 3 Click **RSA SecurID Token Server**.

The CiscoSecure ACS to RSA SecurID Configuration page appears.

Step 4 Select **Upload sdconf.rec** to upload the token server file from the ACE Server data directory.

The FTP Setup Page appears. Enter the:

- a. **FTP Server** address.
- b. **Login** name.
- c. **Password**.
- d. **Directory** where the *sdconf.rec* file is located.
- e. **Decryption Password**.

**Note**

The decryption password must exactly match the password that you specified in the Encryption Password box for the FTP Server.

- f. Click **Submit**.

- Step 5** Choose **Purge Node Secret** to delete any existing configuration settings.
ACS lists the new configuration in the External User Database Configuration table.

RSA Authentication with LDAP Group Mapping

You can perform authentication with RSA in native mode and group mapping by using the LDAP group mapping configuration. Authorization is controlled based on the user's LDAP group membership. When RSA native mode authentication succeeds, group mapping is performed with LDAP. The user's group is applied based on the group mapping configuration.

**Note**

Before you configure RSA Authentication with LDAP Group Mapping, be certain that you have the correct installation or configuration of the third-party DLLs required to support this type of external database.

ACS for Windows

To configure RSA authentication with LDAP Group Mapping:

- Step 1** Install the RSA client for windows.

**Note**

Cisco recommends that you do not install the RSA client on a local PC.

- Step 2** Copy the *sdconf.rec* file into the */system32* directory.
- Step 3** Restart **CSAuth** and **CSAdmin**.
- Step 4** In the navigation bar, click **External User Databases**.
- Step 5** Click **Database Configuration**.
ACS lists all possible external user database types.
- Step 6** Click **RSA SecurID Token and LDAP Group Mapping**.
The External Database Configuration page appears.
- Step 7** Click **Configure**.

Solution Engine Only

You need to upload the RSA client DLL to the Solution Engine image to configure RSA authentication with LDAP Group Mapping. The *sdconf.rec* file interacts with the RSA ACE Server through the *aceclnt.dll* interface. After you upload the dll file, you can purge the node secret. Purging the node secret is useful when configuration changes are made in the RSA server.

The RSA server client software version. 6.1 [*aceclnt.dll*] is included in appliance image. The server client software allows authentication via the RSA Native token card without installing the RSA client software. You can make changes to the *sdconf.rec* file and the node secret through the ACS web interface. RSA client software is unnecessary.

**Note**

ACS assumes the delivery of the node secret is set to automatic in the RSA server.

To configure RSA Authentication with LDAP Group Mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration**.
ACS lists all possible external user database types.
- Step 3** Click **RSA SecurID Token and LDAP Group Mapping**.
The External Database Configuration page appears.
- Step 4** Click **Configure**.
- Step 5** Click **Configure Native RSA**.
- Step 6** Choose **Upload sdconf.rec** to upload the token server file from the ACE Server data directory.
The FTP Setup Page appears. Enter the:
- FTP Server** address.
 - Login** name.
 - Password**.
 - Directory** where the *sdconf.rec* file is located.
 - Decryption Password**.

**Note**

The decryption password must exactly match the password that you specified in the Encryption Password box for the FTP Server.

-
- Step 7** Chose **Purge Node Secret** to delete any existing configuration settings.
- Step 8** Update the port mapper.
-

Deleting an External User Database Configuration

If you no longer need a particular external user database configuration, you can delete it from ACS.
To delete an external user database configuration:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Configuration**.
ACS lists all possible external user database types.
- Step 3** Click the external user database type for which you want to delete a configuration.

The External User Database Configuration table appears.

Step 4 If a list appears in the External User Database Configuration table, select the configuration to delete. Otherwise, proceed to Step 5.

Step 5 Click **Delete**.

A confirmation dialog box appears.

Step 6 Click **OK** to confirm that you want to delete the selected external user database configuration. The external user database configuration that you selected is deleted from ACS.



CHAPTER 13

Posture Validation

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, supports posture validation when ACS is deployed as part of a broader Cisco Network Access Control (NAC) solution.

This chapter contains:

- [What is Posture Validation?, page 13-1](#)
- [Posture Validation in Network Access Control, page 13-2](#)
- [Posture Validation and Network Access Profiles, page 13-3](#)
- [Posture Tokens, page 13-3](#)
- [The Posture Validation Process, page 13-4](#)
- [Policy Overview, page 13-5](#)
- [Internal Policies, page 13-7](#)
- [External Policies, page 13-8](#)
- [External Posture Validation Audit Servers, page 13-9](#)
- [Configuring NAC in ACS, page 13-13](#)
- [Configuring ACS in a NAC/NAP Environment, page 13-15](#)
- [Configuring Policies, page 13-15](#) (including internal, external, and audit server)
- [Posture Validation Pages Reference, page 13-30](#)

What is Posture Validation?

The term *posture* refers to the collection of attributes that play a role in the conduct and “health” of an endpoint device that is seeking access to the network. Some of these attributes relate to the endpoint device-type and operating system; other attributes belong to various security applications that might be present on the endpoint, such as antivirus (AV) scanning software.

Posture validation applies a set of rules to the posture data associated with an endpoint. The result is an assessment of the level of trust associated with the endpoint. A posture token, such as **Healthy** or **Infected**, represents the state of the endpoint.

The posture token becomes one of the conditions in the authorization rules for network access. Posture validation, together with the traditional user authentication, provides a complete security assessment of the endpoint and the user.

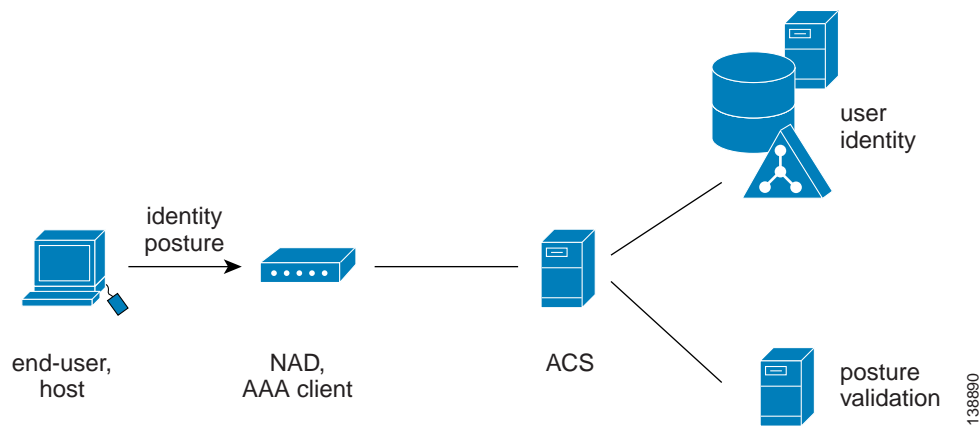
Posture Validation in Network Access Control

Posture validation can work with Network Access Control (NAC). NAC uses the network infrastructure to enforce-security policy compliance on all devices seeking access to network computing resources.

Security-policy compliance limits damage from emerging security threats. By using NAC, customers can allow network access only to compliant and trusted endpoint devices (such as PCs, servers, and PDAs), and can restrict the access of noncompliant devices. For more information about the NAC solution, see <http://www.cisco.com/go/NAC>.

Figure 13-1 shows the components of a typical NAC deployment, including posture validation.

Figure 13-1 Components of a Typical NAC Deployment



Typical NAC components are:

- **End-user or host**—Also known as the endpoint. The endpoint is a device such as a PC, workstation or server that is connected to a switch, access point, or router through a direct connection. In a NAC deployment, the host that is running the Cisco Trust Agent application, collects posture data from the computer and from any NAC-compliant applications that are installed on the computer. For more information about posture credentials, see [Posture Validation Attribute Data Types](#), page 13-6.

Examples of NAC-compliant applications are the CSA and antivirus programs from Network Associates, Symantec, or Trend Micro. These applications provide the Cisco Trust Agent with attributes about themselves, such as the version number of a virus definition file.

A NAC agentless host (NAH) is an endpoint that is not running the Cisco Trust Agent application.

- **Network Access Device (NAD)**—In a NAC deployment the AAA client is called a NAD. The NAD is a Cisco network access device, such as a router or switch, which acts as a NAC enforcement point.
- **ACS**—ACS performs the validation of the endpoint device by using internal policies, external policy servers, or both, to which the posture credentials are forwarded.
- **External posture validation servers**—These perform posture validation and return a posture token to ACS. In a NAC deployment with agentless hosts, you can configure ACS to invoke the services of a special type of posture validation server, called an audit server. An audit server uses out-of-band methods, such as port scans, to validate the health of the endpoint device, and reports the result as a posture token to ACS.
- **Remediation servers**—Provide repair and upgrade services to hosts that do not comply with network admission requirements.

Posture Validation and Network Access Profiles

To understand the profile-based policy paradigm, you should understand network access profiles (NAPs). A profile is essentially a classification of network access requests for applying a common policy. Profile-based policies include rules for authentication, authorization, and posture validation.

Authorization rules are no longer set in Posture Validation but in the Network Access Profiles tab. By using authorization in NAP, you can provision the same RADIUS attribute to have different values for different users, groups and profiles. The one-user-one-group-one-profile is now more flexible by using profile-based policies instead.

After configuring posture validation rules, you must associate those rules to a network access profile. For detailed instructions, see [Setting a Posture-Validation Policy, page 14-30](#).

For more detailed information on policy-based profiles, see [Overview of NAPs, page 14-1](#).

Posture Tokens

Posture tokens represent the state of an endpoint device or a NAC-compliant application that is installed on the computer. ACS recognizes two types of posture tokens:

- System posture tokens (SPTs) represent the state of the computer.
- Application posture tokens (APTs) represent the state of a NAC-compliant application.

ACS determines the SPT of each request by comparing the APTs from all policies that are applied to the request. The most severe APT becomes the SPT.

[Table 13-1](#) describes the six predefined, non-configurable posture tokens, used for system and application posture tokens. They are listed in order from least to most severe.

Table 13-1 ACS Posture Tokens

Token	Description
Healthy	The endpoint device complies with the currently required credentials so you do not have to restrict this device.
Checkup	The endpoint device is within the policy but does not have the latest security software; update recommended. Use to proactively remediate a host to the <code>Healthy</code> state.
Transition	The endpoint device is in the process of having its posture checked and is given interim access pending a result from a full posture validation. Applicable during host boot where all services may not be running or while audit results are not yet available.
Quarantine	The endpoint device is out of policy and needs to be restricted to a remediation network. The device is not actively placing a threat on other hosts; but is susceptible to attack or infection and should be updated as soon as possible.
Infected	The endpoint device is an active threat to other hosts; network access should be severely restricted and placed into remediation or totally denied all network access.
Unknown	The posture credentials of the endpoint device cannot be determined. Quarantine the host and audit, or remediate until a definitive posture can be determined.

From the perspective of ACS, the actions that you set in your authorization rule determine the meaning of an SPT. These actions associate a token with RADIUS authorization components (RACs), DACLs, or both. The authorization rule may also specify a user group as part of the condition. For details on

configuring RACs, see [Adding RADIUS Authorization Components, page 4-10](#). For details on setting up your authorization rules as part of network access profiles, see [Classification of Access Requests, page 14-2](#).

Posture validation requests resulting in an SPT for which access is not strictly denied are logged in the Passed Authentications log. Posture validation requests resulting in an SPT for which access is denied are logged in the Failed Attempts log. For more information on logging and reports, see [Update Packets in Accounting Logs, page 10-37](#).

ACS only uses APTs to determine the SPT; but the endpoint device receiving the results of the posture validation can use them based on their meanings to the relevant NAC-compliant application.

The Posture Validation Process

ACS evaluates the posture attributes that it receives from an endpoint computer. The following overview describes the steps and systems involved in posture validation. Details about various concepts, such as posture tokens and policies, are provided in topics that follow.

1. Following a network event (for example, traffic captured by the EoU ACL on the NAD), the NAD initiates an EAP conversation with the endpoint and forwards EAP messages from the endpoint to ACS.
2. ACS establishes a secure conversation with the host by using PEAP or EAP-FAST (depending on the ACS configuration and endpoint support).
3. (EAP-FAST only and optional) ACS authenticates the end user.
4. ACS queries the endpoint for posture attributes. In response, the endpoint sends posture attributes to ACS.
5. ACS performs the evaluation of the posture attributes internally and/or uses external posture validation servers. The evaluation results in a set of application posture tokens (APTs). ACS then evaluates the system posture token (SPT) by using the most severe APT.
6. Based on authorization rules that you set in Network Access Profiles, ACS sends the endpoint computer the system posture token and the results of each policy that is applied to the posture validation request, and then ends the EAP session. Based on the evaluation, ACS grants the client network access based on access limitations; or the noncompliant device can be denied access, placed in a quarantined network segment, or given restricted access to computing resources.

You can set up many types of restrictions in authorization rules by using various RADIUS attributes in the RAC (which might be combined with the user's group), downloadable ACL, and url-redirect or status-query-timeout.

7. ACS sends the AAA client the RADIUS attributes as configured in the shared RAC, including ACLs and attribute-value pairs that are configured in the Cisco IOS/PIX 6.0 RADIUS attribute `Cisco-AV-Pair`.
8. ACS logs the results of the posture validation request. If the request was not denied, ACS logs the results in the Passed Authentications log (if enabled). If the request was denied (for instance by the authorization policy or if no posture validation rule with matched required credential types was present), then ACS logs the results in the Failed Attempts log.

The endpoint handles the results of the posture validation request according to its configuration. The AAA client enforces network access as dictated by ACS in its RADIUS response. By configuring profiles, you define authorizations and, therefore, network access control, based on the system posture token that is determined as a result of posture validation.

Policy Overview

This section contains:

- [About Posture Credentials and Attributes, page 13-5](#)
- [Extended Attributes, page 13-6](#)
- [Posture Validation Attribute Data Types, page 13-6](#)

You can use ACS to set up internal or external posture validation policies that return a posture token and an action after checking the rules that you (or the external server) set for the policy.

Policies are reusable; that is, you can associate a single policy with more than one network access profile. For example, if your NAC implementation requires two profiles, one for endpoints using NAI software and one for endpoints using Symantec software, you may need to apply the same rules about the operating system of the endpoint; regardless of which antivirus application is installed. You can create a single policy that enforces rules about the operating system and associate it with the Symantec and the NAI server information.

The results of applying a policy are:

- **Posture Assessment**—The credential type and, therefore, the NAC-compliant application to which the policy evaluation result applies.
- **Token**—One of six predefined tokens that represents the posture of the endpoint and, specifically, the application that the result credential type defines.
- **Notification String**—An optional text string that is sent in the posture validation response to the application that the posture assessment defines.

About Posture Credentials and Attributes

For posture validation, credentials are the sets of attributes sent from the endpoint to ACS. Also known as inbound attributes, these attributes contain data that is used during posture validation to determine the posture of the computer. ACS considers attributes from each NAC-compliant application and from the Cisco Trust Agent to be different types of credentials.

With policies that ACS creates for validation, the rules that you create use the content of inbound attributes to determine the APT returned by applying the policy. With policies that are created for validation by an external server, ACS forwards the credential types that you specify to the external NAC server. In either case, the contents of inbound attributes provide the information that is used to determine posture and, thus, to control network admission for the computer.

ACS uses NAC attributes in its response to the endpoint. These attributes are called outbound attributes. For example, APTs and the SPT are sent to the endpoint in attributes.

Credential types are uniquely identified by two identifiers: vendor ID and application ID. The vendor ID is the number that is assigned to the vendor in the [IANA Assigned Numbers RFC](#). For example, vendor ID 9 corresponds to Cisco Systems, Inc. Vendors assign numbers to the NAC applications that they provide. For example, with Cisco applications, application ID 1 corresponds to the Cisco Trust Agent. In the web interface, when you specify result credential types for a policy, the names that you assign to the vendor and application identify the credential types for the Cisco Trust Agent. For example, the credential type for the Cisco Trust Agent is *Cisco:PA* (where PA refers to posture agent, another term for the Cisco Trust Agent). In a posture validation response, ACS would use the numeric identifiers 9 and 1, which are the identifiers for Cisco and the Cisco Trust Agent, respectively.

Attributes are uniquely identified by three identifiers: vendor ID, application ID, and attribute ID. For each unique combination of vendor and application, there are set of attributes that each have numbers as well. When ACS communicates with an endpoint, the identifiers are numerical. In the web interface, when you define rules for internal policies, attributes are identified by the names that are assigned to vendor, application, and attribute. For example, the Cisco Trust Agent attribute for the version of the operating system is `Cisco:PA:OS-Version`. The data that ACS receives identifies the attribute with the numeric identifiers 9, 1, and 6, which are the identifiers for Cisco, the Cisco Trust Agent, and the sixth attribute of the Cisco Trust Agent, respectively.

For more information about attributes, including data types and operators that are used in rules for internal policies, see [Posture Validation Attribute Data Types, page 13-6](#). You can use **CSUtil.exe** to add and configure custom RADIUS vendor and VSA configurations. For information about using **CSUtil.exe** to export, add, or delete posture validation attributes, see [User-Defined RADIUS Vendors and VSA Sets, page C-17](#).

Extended Attributes

You use extended attributes to configure conditions that support Linux clients, and are specific for different Linux packages. For example, you can configure a condition for the version of the **openssl** package.

You input values for these Linux packages in the Entity field. When you input an extended attribute from the attribute drop-down list, the entity field is enabled. You can then select an entity from the drop-down list.

For example, if you select the `Cisco:Host:Package:Version` attribute, which is an extended attribute, the Entity drop-down list displays all the Linux packages that are configured in the system (ACS).

You can add or delete extended attributes.

ACS for Windows: You use the **CSUtil.exe** command. For details, see [Posture-Validation Attributes, page C-29](#).

ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see [NAC Attribute Management \(ACS SE Only\), page 8-44](#).

Posture Validation Attribute Data Types

Posture validation attributes can be one of the following data types:

- **boolean**—The attribute can contain a value of 1 or 0 (zero). In the HTML interface, when you define a rule element with a boolean attribute, the words `false` and `true` are valid input. Valid operators are `=` (equal to) and `!=` (not equal to). When a rule element using a Boolean attribute is evaluated, `false` corresponds to a value of 0 (zero) and `true` corresponds to 1.

For example, if a rule element for a Boolean attribute requires that the attribute is not equal to `false` and the attribute in a specific posture validation request was 1, ACS would evaluate the rule element to be true; however, to avoid confusion, you can express the rule element more clearly by requiring that the attribute is equal to `true`.

- **string**—The attribute can contain a string. Valid operators are `=` (equal to), `!=` (not equal to), `contains`, `starts-with`, and `regular-expression`.
- **integer**—The attribute can contain an integer, including a signed integer. Valid operators are `=` (equal to), `!=` (not equal to), `>` (greater than), `<` (less than), `<=` (less than or equal to), `>=` (greater than or equal to). Valid input in rule elements is an integer between -65535 and 65535.

- **unsigned integer**—The attribute can contain only an integer without a sign. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), and >= (greater than or equal to). Valid input in rule elements is a whole number between 0 and 4294967295.
- **ipaddr**—The attribute can contain an IPv4 address. Valid operators are = (equal to), != (not equal to), and `mask`. Valid format in rule elements is dotted decimal format. If the operator is `mask`, the format is the `mask/IP`. For more information, see [Configuring Policies, page 13-15](#).
- **date**—The attribute can contain a date. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), >= (greater than or equal to), and `days-since-last-update`. Valid format in rule elements:

mm/dd/yyyy
hh:mm:ss

- **version**—The attribute can contain an application or data file version. Valid operators are = (equal to), != (not equal to), > (greater than), < (less than), <= (less than or equal to), and >= (greater than or equal to). Valid format in rule elements:

n.n.n.n

where each *n* can be an integer from 0 to 65535.

- **octet-array**—The attribute can contain data of arbitrary type and variable length. Valid operators are = (equal to) and != (not equal to). Valid input in rule elements is any hexadecimal number, such as 7E (the hexadecimal equivalent of 126).

Internal Policies

This section contains:

- [About Internal Policies, page 13-7](#)
- [About Rules, Rule Elements, and Attributes, page 13-8](#)

About Internal Policies

Internal policies comprise one or more rules that you define in ACS. When ACS applies an internal policy, it uses the policy rules to evaluate credentials that are received with the posture validation request. Each rule is associated with an APT, a credential type, and an action. The credential type determines which NAC-compliant application with which the APT and action are associated.

ACS applies each rule in the order they appear on the Posture Validation Policies page (from top to bottom), resulting in one of the following two possibilities:

- **A configurable rule matches**—When all elements of a rule are satisfied by the credentials that are received in a posture validation request, the result of applying the policy is the condition, posture assessment, and notification string that are associated with the rule. ACS does not evaluate the credentials with any additional rules.
- **No configurable rule matches**—When the attributes that are included in the posture validation request satisfy no policy rules, ACS uses the condition, posture assessment, and notification string that are associated with the default rule as the result of the policy.

**Note**

Applying a policy to a posture validation request always results in a match, to one of the configurable rules or to the default rule.

When you specify the order of rules in a policy, determine the likelihood of each rule to be true and then order the rules so that the rule most likely to be true is first and the rule least likely to be true is last. Doing so makes rule processing more efficient; however, determining how likely a rule is to be true can be challenging. For example, one rule may be true for the posture of twice as many endpoints as a second rule, but posture validation may occur more than twice as often for endpoints whose posture matches the second rule; therefore, the second rule should be listed first.

About Rules, Rule Elements, and Attributes

A rule is a set of one or more rule elements. A rule element is a logical statement which comprises:

- A posture validation attribute
- An operator or posture token
- A value or notification string

ACS uses the operator to compare the contents of an attribute to the value. Each rule element of a rule must be true for the whole rule to be true. In other words, all rule elements of a rule are joined with a Boolean AND.

For detailed descriptions of rules, see [Classification of Access Requests, page 14-2](#).

For information on configuration, see [Creating an Internal Policy, page 13-17](#), and [Internal Posture Validation Setup Pages, page 13-30](#)

External Policies

External policies are policies that an external NAC server defines, usually from an antivirus vendor and a set of credential types to be forwarded to the external database. You also have the option of defining a secondary external NAC server. The presence of a secondary server allows the secondary or failover server to evaluate any policies from the primary server.

ACS does not determine the result of applying an external policy; instead, it forwards the selected credentials to the external NAC server and expects to receive the results of the policy evaluation: an APT, a result credential type, and an action.

Each external policy that is associated with a external server must return a result; otherwise, ACS rejects policy validation requests that are evaluated with a profile whose external policies do not return a result. For example, if ACS evaluates a posture validation request by using a profile that has 10 internal policies and one external policy, but the external NAC servers associated with the external policy are not online, it is irrelevant that the 10 internal policies all return SPTs. The failure of the single external policy causes ACS to reject the posture validation request.

For information on external policy configuration options see [Editing an External Posture Validation Server, page 13-23](#), and [External Posture Validation Setup Pages, page 13-33](#).

External Posture Validation Audit Servers

This section contains:

- [About External Audit Servers, page 13-9](#)
- [Auditing Device Types, page 13-10](#)
- [Configuring NAC in ACS, page 13-13](#)

About External Audit Servers

Audit servers are Cisco and third-party servers that determine posture information about a host without relying on the presence of a Posture Agent (PA). The Cisco PA is also known as the Cisco Trust Agent. Audit servers are used to assess posture validation with an organization's security policy. You can also define a secondary external audit server. The presence of a secondary audit server allows the second or failover server to evaluate any policies from the primary server when the primary server rejects a policy.

An audit policy is a set of processing rules for evaluating the posture of a Agentless Host through an audit server. Audit policies are used to retrieve posture decisions for hosts that do not have an EAP supplicant. When a host accesses the network through a NAD that is acting as a NAC enforcement point, the NAD sends information to ACS so that ACS can trigger auditing. If ACS is configured correctly, it queries the audit server for the result (posture token) of the audit and then determines the authorization based on the audit result.

Your network-management security strategy may include external audit servers that work with ACS to control access to your network.

ACS will use the **GAME** protocol to communicate with audit servers. In each audit request, ACS forwards the following information to the audit server:

- `host id`
- `ip-address`
- `mac-address` (optional)

The name of the System-Posture-Token is dynamically sent (without requiring any configuration) to the device.

[Table 13-2](#) defines the details required in applying the results of an audit.

Table 13-2 *Audit Policy Requirements*

Audit Policy	Description
auditServerConfiguration	A pointer to the audit server configuration that defines how to communicate with the audit server.
exemptionList	A list of MAC or IP addresses (or both), and groups that are exempt from audit.
inverseExemptionFlag	If this flag is set, the meaning of the exemption list will be inversed. That is, only the hosts specified in the list will be audited; all others will be exempt.
exemptionToken	The token to assign to hosts who are exempt.
defaultInProgressToken	The token to use when the audit is in progress and we have no cached token.

Table 13-2 Audit Policy Requirements (continued)

Audit Policy	Description
staticAttributes	These name value pairs will be sent to the audit server when this policy is invoked. For this release, this list of attributes will be used to pass the policy name.
tokenMappings	The token to user group mapping. Note that this scheme assumes that there is only one audit policy per service.

How an External Audit Gets Triggered

An endpoint failure triggers an external audit. This failure occurs when the enforcement point detects that the endpoint is not responding as required. The enforcement point sends the `aaa:event` failure message to indicate that a device failure has occurred.

The current release of ACS supports this event type and provides configuration in the out-of-band posture policy about which event should activate the policy (may be more than one).

ACS must be able to recognize the following events that may or may not trigger an audit, depending on policy configuration:

- NAS detects lack of a functioning Cisco Trust Agent and sends NRH notification in the `aaa:event` attribute
- Endpoint device (or supplicant) is unable to respond to a posture request
- An explicit audit request from the device

Once ACS recognizes that an audit will occur, the audit server is queried. The audit server responds with results or an audit-in-progress message, which may contain a polling timeout hint to pass on to the NAD. At this point, ACS evaluates the enforcement policy for the given host based on the default APT that is associated with the posture validation policies. Part of the enforcement policy must be a session-timeout value that is used to trigger the NAD to reauthenticate the host. ACS receives the request and queries the audit server. This process repeats itself until the audit server responds with an APT. Once the audit response is received, enforcement policies are reevaluated and returned to the NAD.

The NAD caches the posture token that will be sent along with any subsequent access requests occurring during the host's session; for instance, as a result of session timeout (reauthentication). ACS uses this token for default policy evaluation during the audit for these subsequent authentications, thereby avoiding session downgrade for the connected host.

Exemption List Support

ACS supports exemption lists of groups and hosts. The exemption list contains a list of IP or MAC addresses to include or exclude from the audit. When a host is exempted, it is assigned an exemption token that determines its posture status. The exemption list is defined in the out-of-band audit policy. The IP list may contain single IP addresses or IP mask ranges. The MAC lists may be MAC ranges in the form of partial MAC strings that are matched with the hosts MAC address by using the ***begins with*** operator.

Auditing Device Types

As an extra security check on MAC authentication, you can configure an audit policy that checks for device type and handles assignment of the device to an appropriate destination user group. For example, a questionable device might be assigned to a user group called *Mismatch*; or, if the process does not

assign a group, the device might be assigned to a user group called *Quarantine*. In the case where MAC authentication and the audit policy return the same device type, such as printer, your audit policy can assign the device to the printer group.

Policy Formation

You use options on the External Posture Validation Audit Server Setup page to define the audit policy. These options can enable a request for device-type from the audit server or assign a group in the absence of the device-type. The options on this page also provide for construction of rules that can specifically manage group assignment based on logical comparisons.

The complete audit policy also depends on the elements that you have previously configured on the External Posture Validation Server Setup page, which include setup of the host(s), audit server(s), and audit flow. In addition, the policy includes an option for configuration of a secondary audit server that can function in a failover scenario.

ACS uses the **GAME** protocol in a conversation with an audit server. The conversation includes a request for device type, which the audit server determines by scanning the device. If the protocol or audit policy flows return errors, the system displays an error message.

When configuring policy, remember that:

- ACS does not allow configuration of this feature for vendors who do not have the device-type attribute. Qualys is the only vendor tested against this attribute and currently supporting it.
- If an audit server does not return a device-type attribute, policy evaluation continues as though the attribute was not requested.
- ACS logs the device-type attribute in the Passed and Failed logs.

User Groups and Device Types

MAC authentication returns a device type in the form of a user group, such as Printer or PC. Audit policy relies on a list of NAC attribute device definitions, which include Printer and PC, for comparison with the MAC user group. Alternatively, the audit policy can rely on a user-defined device-type string.

When looking at the MAC user group, the policy supports a user group of *Any*, which ACS interprets to mean that the group returned can be any group or no group. When looking at the device type, the policy supports **Match-all** when interpreting the device type returned by the audit.

Group Assignment

Group assignment depends on the configuration of your network. Your network might support multiple devices or only certain devices. To support the audit policy, you should add a destination device group such as **Mismatch** or **Quarantine**. Your particular configuration might require additional groups.

Assignment to a destination user group is based on the following conditions:

- **Device-Type Returned**—Group assignment is based on a rule that compares a MAC device type with a NAC device-type attribute.
- **No Device-Type**—Group assignment is based on a group that you chose.
- **No Device-Type or Group**—Group assignment is based on a group that you chose.
- **No Token or Group**—Group assignment is based on the Fail Open Configuration, which contains a posture token, timeout, and group. In the absence of a Fail Open Configuration, the system returns an error.

Group Mapping Rules

Each group-mapping rule uses an operator, which compares the device user group that MAC authentication returns with the device type that an audit server returned. Any one of the following operators can be defined in a comparison:

- Match all device types (ACS performs a wildcard match on all device types)
- Device type equals
- Device type does not equal
- Contains
- Starts with
- Regular expression

For example:

- If group equals *printers* and device-type not equals *Printer* assign group *Mismatch* (or *Quarantine*).
- If group equals *NotKnown* and device-type equals *Printer* assign group *printers*.
- If group equals *embedded-os* and device-type not equals *Printer* assign group *quarantine*.
- If group equals *Any* and device-type equals *PC* assign group *reject* (maybe this is a LAN where the admin does not allow computers).
- If group equals *Any* and device-type equals *unknown* assign *quarantine*.

Policy List

Each rule definition appears on a list of policies that is orderable by priority.

Layer 2 Audit for Network Access Control

ACS first admits the device to a quarantined network, where the device can receive an IP address. The audit cannot begin until the device has received the IP address. When the audit begins, the audit is the same as an audit of a Layer 3 (L3) host.

The NAD must be pre-configured to learn the host's IP address. Then ACS responds to an initial access-request with a notification to the NAD to issue another access-request when the NAD has learned the IP address. If the NAD does not learn the host's IP address, ACS invokes a failure condition, and policy flow follows the audit fail-open policy. Using the audit fail-open policy, administrators can choose to reject the user, or assign a posture token and an optional user-group.

Audit policy can serve as a backup verification when MAC Authentication Bypass (MAB) fails. The audit policy tests whether MAB failed by applying policy conditions that test the ACS user group assigned to the current session. For example, you can test whether the user-group is equal to the user-group that MAB assigns to failed authentications, and, if so, only then continue the audit.

For configuration information, see [Chapter 14, "Network Access Profiles"](#).

Configuring NAC in ACS

This section provides an overview of the steps to configure posture validation in ACS, with references to more detailed procedures for each step.

**Note**

To design your posture policies, click the Posture Validation tab. You can assign those policies to profiles by clicking the Posture Validation link inside the Network Access Profiles tab.

Before You Begin

Before ACS can perform posture validation, you must complete several configuration steps. An overview of the steps follows. For information on finding detailed instructions on Cisco.com, see [Posture Validation in Network Access Control, page 13-2](#).

To implement posture validation:

Step 1

Install a server certificate. ACS requires a server certificate for NAC because an EAP tunnel protects NAC communication with an end-user client. You can use a certificate that is acquired from a third-party certificate authority (CA) or you can use a self-signed certificate.

For detailed steps about installing a server certificate, see [Installing an ACS Server Certificate, page 9-22](#). For detailed steps about generating and installing a self-signed certificate, see [Generating a Self-Signed Certificate, page 9-35](#).

**Note**

If you use a self-signed certificate, you may need to export the certificate from ACS and import it as a trusted root CA certificate into local storage on the endpoint computers.

Step 2

For posture credentials from a third-party vendor, you must import the corresponding NAC attribute definition file (ADF).

You must add your audit vendor to the ACS internal dictionary.

ACS for Windows: You use the **CSUtil.exe** command before configuring an external posture validation audit server. For detailed instructions, see [Importing External Audit Posture-Validation Servers, page C-34](#).

ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see [NAC Attribute Management \(ACS SE Only\), page 8-44](#).

**Note**

To set up external policies or use external policy audit servers, you should plan on configuring ACS to communicate with the external server over HTTPS; although ACS also supports HTTP communication.

ACS authenticates the audit servers and posture validation servers by using certificates. You must choose the certificate from ACS or configure the Certificate Trust List (CTL). If the external servers use a different CA than the CA that issued the ACS server certificate, then you must configure the CTL. For detailed steps, see [Editing the Certificate Trust List, page 9-28](#).

If your external server uses a self-signed certificate, you do not need to alter the CTL.

Step 3

On the Advanced Options page, check the check box for **Microsoft Network Access Protection Settings**.

- Step 4** Enable the Passed Authentications log. ACS uses this log to log all posture validation credentials whenever access is not strictly denied. If the requests were denied, then ACS logs the results in the Failed Attempts log. When you enable the Passed Authentications log, be sure to move NAC-related attributes to the Logged Attributes column on the Passed Authentications File Configuration page.

For detailed steps about configuring this type of log, see [Configuring a CSV Log, page 10-24](#).

- Step 5** Configure the Failed Attempts log to include NAC attributes. Posture validation requests that were denied are logged to the Failed Attempts log. Including NAC attributes in this log can help you debug errors in your NAC implementation. For example, if none of the posture validation rules is matched, the request is logged here. Using the Failed Attempts log, you can see the contents of the attributes that are received in the request from the endpoint and sent in the reply to the endpoint.

For detailed steps about configuring this type of log, see [Configuring a CSV Log, page 10-24](#).

- Step 6** On the Global Authentication Setup page, enable posture validation by selecting **Allow Posture Validation** under EAP. Complete the steps for layer 2 or layer 3 support.

For detailed steps, see [Configuring Authentication Options, page 9-21](#).

- Step 7** If you have not already configured the AAA clients supporting NAC in the Network Configuration section, do so now.

For detailed steps, see [Adding AAA Clients, page 3-12](#).

- Step 8** From **Network Access Profiles**, set up the user groups that you want to use for posture validation. You are likely to want a separate user group for each possible SPT; therefore, select six user groups. If possible, choose groups that have not been configured to authorize users. Additionally, consider using groups that are widely separated from groups that authorize users. For example, assuming that the lowest numbered groups have been used for user authorization, consider using groups 494 through 499.

- Step 9** For detailed steps on setting up profiles, see [Workflow for Configuring NAPs and Profile-based Policies, page 14-3](#).



Tip

To avoid confusion between groups that are intended to authorize users and groups that are intended to authorize endpoints, consider renaming the groups with an easily understood name. For example, if you selected group 499 to contain authorizations that are related to the Unknown SPT, you could rename the group *NAC Unknown*. For detailed steps, see [Renaming a User Group, page 5-41](#).

- Step 10** For each posture validation rule, assign a posture token and an SPT, which you can later associate with a profile that contains downloadable IP ACL sets, RACs, or both that limit network access appropriately.

For detailed steps on creating rules, see [Creating an Internal Policy, page 13-17](#). For detailed steps, see [Adding a Downloadable IP ACL, page 4-15](#) (and [Adding RADIUS Authorization Components, page 4-10](#).) To associate posture rules to profiles, see [Posture-Validation Policy Configuration for NAPs, page 14-29](#).

- Step 11** For each profile, you can create several different posture validation policies that contain any number of rules to validate your endpoint device. You can:

- Create a policy and its associated rules, including configuring mandatory credential types and policies.

For detailed steps, see [Configuring Policies, page 13-15](#).

- Use **Network Access Profiles** to assign posture validation policies to profiles to validate your endpoint devices.

For detailed steps, see [Posture-Validation Policy Configuration for NAPs, page 14-29](#).

Configuring ACS in a NAC/NAP Environment

ACS 4.2 provides configuration options that you can use to configure ACS to work in a Cisco Network Access Control and Microsoft Network Access Protection (NAC/NAP) environment:

- Configuration of External AAA servers

In the Microsoft NAP environment, these are NAP servers that send Statements of Health (SoHs) to ACS or other AAA servers. You can configure ACS to grant or deny access or levels of access based on processing of the SoHs. For more information on configuring external AAA servers, see [Setting Up an External AAA Server, page 13-23](#).

- Configuration of Statement of Health Posture Validation Rules

You can set up SoH posture validation rules to enable ACS to make decisions about user access based on SoH attributes. For more information on setting up SoH posture validation rules, see [Setting a Posture-Validation Policy to Process Statements of Health, page 14-32](#).



Note

For detailed information on configuring ACS for a NAC/NAP environment, see Chapter 9 of the *Configuration Guide for Cisco Secure ACS, 4.2*, “NAC/NAP Configuration Scenario.”

Configuring Policies

If you plan to use NAC in your network, you will need to define the manner in which posture validation will be performed. Policies are sets of rules that are used to determine a posture token for a posture validation request.

This section contains:

- [Posture Validation Options, page 13-15](#)
- [Setting Up Posture Validation Policies, page 13-16](#)
- [Setting Up an External Policy Server, page 13-22](#)
- [Setting Up an External Audit Posture Validation Server, page 13-25](#)
- [Audit Processing with MAC Authentication Bypass, page 13-27](#)

Posture Validation Options

You can configure the following posture validation options:

- Internally within ACS. See [Setting Up Posture Validation Policies, page 13-16](#).
- Externally by using the Host Credential Authorization Protocol (HCAP) protocol to one or more Posture Validation Servers (PVSs). See [Setting Up an External Policy Server, page 13-22](#).
- Externally by using the GAME protocol to an audit server for NAC agentless host (NAH) support. See [Setting Up an External Audit Posture Validation Server, page 13-25](#).

[Table 13-3](#) describes the setup options for posture validation.

Table 13-3 Posture Validation Options

Component	Description	Notes
Internal Posture Validation	Policy requirements for the network are internally (or locally) validated in ACS.	NAC policies for the Cisco Trust Agent, Windows, the CSA, and antivirus software applications are among recommended internal policies. See Creating an Internal Policy, page 13-17
External Posture Validation	An outside posture validation server validates policies.	Externalizing the posture validation to an AV server allows you to handle proprietary AV posture credentials and antivirus policy administration by an AV administrator separate from the ACS administrator.
External Audit Posture Validation	Cisco and third-party servers that determine posture information about a host without relying on the presence of a PA. These types of hosts are also referred to as <i>agentless</i> . Audit servers are used to assess posture validation with an organization's security policy.	The Cisco PA is also known as the Cisco Trust Agent. If no Cisco Trust Agent is on the host, then an audit server can be used.

**Note**

You can perform internal and external posture validation at the same time; but not for the same NAC credential types (vendor-application combinations).

To configure a policy for internal or external posture validation:

-
- Step 1** In the navigation bar, click **Posture Validation**.
- Step 2** Select one of the components to set up your posture validation servers:
- **Internal Posture Validation Setup**—See [Internal Policies, page 13-7](#) or [Creating an Internal Policy, page 13-17](#)
 - **External Posture Validation Setup**—See [External Policies, page 13-8](#) or [Setting Up an External Policy Server, page 13-22](#)
 - **External Posture Validation Audit Setup**—See [External Posture Validation Audit Servers, page 13-9](#) or [Setting Up an External Audit Posture Validation Server, page 13-25](#)
- Step 3** Complete the required steps to set up internal or external posture validation.
-

Setting Up Posture Validation Policies

This section contains:

- [Creating an Internal Policy, page 13-17](#)
- [Cloning a Policy or Policy Rule, page 13-20](#)
- [External Posture Validation Audit Servers, page 13-9](#)

- [Editing a Policy, page 13-19](#)
- [Deleting a Policy or Rule, page 13-21](#)

Creating an Internal Policy

Use internal posture validation to write your own policies for access in your network. After you have created policies, you can then profile rules to use these policies.

You can select internal policies for more than one profile. To add the policy to a profile, use the Network Access Profiles page.

For descriptions of the options available on the Internal Posture Validation Setup page, see [Configuring Policies, page 13-15](#).

For details on how to set up your third-party component policies, see the related documentation on the Go NAC website on Cisco.com. For information on adding internal policies to your profiles, see [Posture-Validation Policy Configuration for NAPs, page 14-29](#).

Once you have set up at least one policy, you can use the clone rule option to save time by copying a policy and customizing it. For details on how to use cloning, see [Cloning a Policy or Policy Rule, page 13-20](#).

To create your internal posture validation policy:

-
- Step 1** Access the Internal Policy Validation Setup page:
- In the navigation bar, click **Posture Validation**.
 - Click **Internal Posture Validation Setup**.
ACS displays a list of posture validation policies, if available.
 - Click **Add Policy**.
- Step 2** In the **Name** box, type a descriptive name for the policy.
- Step 3** In the **Description** box, type a useful description of the policy.
- Step 4** Click **Submit**.
- Step 5** Click **Add Rule**.
- Step 6** For each condition set that you want to add to the rule:
- Select an attribute. For more information about attribute types, see [Posture Validation Attribute Data Types, page 13-6](#).
 - Select an entity (only available for extended attributes).
 - Select an operator.
 - Type a value.
 - Click **Enter** and then **Submit**.

For example, if you create a policy for the CSA, you might create the following condition sets:

- *Cisco:PA:PA-Version >= 2.0.0.0 AND Cisco:PA:Machine-Posture-State = 1 with a Posture token=Healthy.*
- *Cisco:PA:PA-Version >= 2.0.0.0 AND Cisco:PA:Machine-Posture-State = 2 with a Posture Token=Transition.*
- Match OR inside Condition and AND between Condition Sets to allow ACS to choose between tokens.

For more information about operators, see [Configuring Policies, page 13-15](#).

For information on the Cisco Trust Agent posture plug-in attributes and values, see the Cisco Trust Agent documentation.

The condition set appears in the Conditions Sets table.

Step 7 Select which Boolean condition to add to this condition set:

- **Match OR inside Condition and AND between Condition Set**—Select if you want to be less stringent with your conditions.
- **Match AND inside Condition and OR between Condition Sets**—Select if you want to be more secure with your posture validation.

Step 8 Verify that the condition sets are configured as intended.



Tip If you want to change a condition set that you have already added, select the condition element, click **Remove**, and update its attribute, entity, operator, or value, then click **Enter**.

Step 9 For the new rule, do each of the following:

- a. Select a credential type.
- b. Select a token.
- c. Type an action (in the form of a notification string).

For more information about tokens, see [Posture Tokens, page 13-3](#).

If the rule matches the posture validation request, ACS associates with the policy the result credential type, token, and action that you specify.



Tip If you want to create another condition set that is identical to one that is already created, click **Clone**. Then change the condition set as needed.

Step 10 Click **Submit**.

The Policy Validation Rules page appears again. The new condition set appears at the bottom of the Condition Sets table.



Tip You can return to the Posture Validation Rules page by clicking the rule.

Step 11 After you create the rules that define the policy, order the rules as needed. ACS applies a policy by attempting to match rules in the order that they appear on the Policy Validation Rules page, from top to bottom. Policy processing stops at the first successful rule match; so order is important. To move a rule:

- a. Select the rule. To do so, click the radio button to the left of the rule.
- b. Click the **Up** or **Down** button as needed until the rule is positioned properly.

Step 12 Configure the Default Rule at the bottom of the Posture Validation Rules page by clicking **Default**:

- a. Select a credential type.
- b. Select a token.
- c. Type an action (in the form of a notification string).

When ACS applies this policy to a posture-validation request and none of the configurable rules matches the request, ACS associates the default credential type, token, and action that you specify with the policy.

- Step 13** Click **Submit**.
The Posture Validation Rules page displays the new rule.
- Step 14** Click **Done**.
The current configuration has been changed.
- Step 15** Click **Apply and Restart** for your changes to take effect.
-

Editing a Policy

You can only edit a policy by accessing it through the Posture Validation pages.

To edit a policy or posture validation rule:

-
- Step 1** In the navigation bar, click **Posture Validation**.
- Step 2** Click **Internal Posture Validation Setup**.
- Step 3** Click on the policy name of the rule that you want to edit.
The applicable policy rules page appears.
- Step 4** To edit a policy:
- Click **Add Rule to add more condition sets**.
 - To change a condition set that you have already added:
 - Select the condition element.
 - Click **Remove**.
 - Update its attribute, entity, operator, or value; then click **Enter**.
 - To add a new condition:
 - Select the attribute, entity, and operator from the drop-down lists.
 - Enter a value.
 - Click **Enter**.
 - Click **Clone** to copy an existing condition set or policy rule.
 - Click **Delete** to remove policy rule. You can also remove a condition set or an element from a condition set. See [Deleting a Condition Component or Condition Set](#), page 13-21.
 - To move a rule:
 - Select the rule by clicking the button to the left of the rule.
 - Click the **Up** or **Down** button as needed until the rule is positioned properly.
 - If you want to add or change a Boolean condition to this condition set, select one of the options:
 - Match OR inside Condition and AND between Condition Set**—Select if you want to be less stringent with your conditions.
 - Match AND inside Condition and OR between Condition Sets**—Select if you want to be more secure with your posture validation.
 - Click **Rename** to change the existing name.
- ACS creates a new policy. ACS stores the new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.

- Step 5** When finished with editing, click **Submit**. Then click **Done**.
- Step 6** Click **Apply and Restart** for your changes to take effect.
-

Cloning a Policy or Policy Rule

This option creates a policy or rule that is identical to the selected one. You can then easily modify the settings.

To clone an internal posture validation policy or policy rule:

- Step 1** If you have not already done so, access the Internal Policy Validation Setup page. To do so:
- In the navigation bar, click **Posture Validation**.
 - Click **Internal Posture Validation Setup**.
ACS displays a list of posture validation policies.
 - Select a policy name from the list.



Tip If no policies are configured, click **Add Policy** and follow the instructions in [Creating an Internal Policy](#), page 13-17.

- Step 2** To make a copy of the current policy, click **Clone**.
For example, if you selected *VPNmgt1* as the policy, the copy would be *Copy-of-VPNmgt1*.
- Step 3** To make a copy of one of the policy rules inside the current policy, click the condition name. Then click **Clone**.
The Policy Validation Rule page appears again. The new condition set appears in the Condition Sets table.
- Step 4** Click **Rename** to change the existing name to a more meaningful name or description.
ACS creates a new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.
- Step 5** When you finish with editing, click **Submit**.
- Step 6** Click **Done** if you are finished adding clones.
- Step 7** Click **Apply and Restart** for your changes to take effect.
-

Renaming a Policy

Use the renaming feature to change the name or description of an existing or cloned policy to something more meaningful.

To rename a policy:

- Step 1** If you have not already done so, access the Internal Policy Validation Setup page. To do so:
- In the navigation bar, click **Posture Validation**.

- b. Click **Internal Posture Validation Setup**.
ACS displays a list of posture validation policies.
 - c. Select a policy name from the list.
 - Step 2** Click **Rename** to change the existing policy name or make the description more meaningful.
 - Step 3** Enter the changes to the policy name or description. When you finish editing, click **Submit**.
ACS creates a new policy. ACS stores the new policy and does not change the configuration of the old policy. The old policy remains in the Posture Validation Policies table.
 - Step 4** Click **Done**.
The renamed policy appears at the bottom of the Posture Validation Policies page.
 - Step 5** Click **Apply and Restart** for your changes to take effect.
-

Deleting a Policy or Rule

To delete a policy or rule:

-
- Step 1** If you have not already done so, access the Internal Policy Validation Setup page. To Access the Internal Policy Validation Setup page:
 - a. In the navigation bar, click **Posture Validation**.
 - b. Click **Internal Posture Validation Setup**.
ACS displays a list of posture validation policies.
 - Step 2** To delete a rule or policy, select a policy name from the list of posture validation policies.
The Posture Validation Rules page appears.
 - Step 3** To delete an entire policy and all its rules, click **Delete**.
This deletes the policy from the policy validation list; but does not remove the policy from any profiles with which it may be associated. A warning message prompts you to cancel or click **OK**.
 - Step 4** To delete an element or condition set, see [Deleting a Condition Component or Condition Set, page 13-21](#).
ACS deletes the policy rule. The policies page reappears and the policies table no longer lists the deleted policy. All profiles that were configured to use the policy no longer include the deleted policy.
-

Deleting a Condition Component or Condition Set

A condition component is the list of elements that a condition set comprises. To delete a condition component from a condition set or an entire condition set:

-
- Step 1** If you have not already done so, access the Internal Policy Validation Setup page. To Access the Internal Policy Validation Setup page:
 - a. In the navigation bar, click **Posture Validation**.
 - b. Click **Internal Posture Validation Setup**.
ACS displays a list of posture validation policies.

- Step 2** Select a policy name from the list of posture validation policies.
The Posture Validation Rules page appears.
- Step 3** Select a blue link in the Condition list on the Posture Validation Rules page.
- Step 4** To delete the entire condition set, click **Delete**. Then click **Done**.
- Step 5** To delete a selected condition component from the set, select a blue link in the Condition Sets list, then click **Delete**. Click **Submit** when you have deleted all condition components desired.
ACS deletes the condition set or condition component.
- Step 6** Click **Done**.
-

Setting Up an External Policy Server

This procedure describes how you can create an external policy.

Before You Begin

You can choose external policies for more than one profile. To create external policies, use the External Posture Validation Setup pages. To add the policy to a profile, use the Network Access Profiles page. See [Classification of Access Requests, page 14-2](#).

The external server that you use to access the External Policy Validation page does not limit which profiles can select the new external policy.

For descriptions of the options available on the External Policy Configuration page, see [Configuring Policies, page 13-15](#).

-
- Step 1** After you choose **External Posture Validation Setup**, the External Posture Validation Servers page displays.
- Step 2** Click **Add Server**.
The Add/Edit External Posture Validation Server page appears.
- Step 3** Name the server and provide a description if necessary.
- Step 4** Provide addressing information for the primary and secondary servers.
- Check the **Primary Server configuration** check box.



Note If you do not select the **Primary Server Configuration** check box, ACS uses the secondary server configuration. If no secondary server configuration exists or if the secondary server is unreachable, the posture validation request is rejected.

- Provide configuration details about the primary NAC server. For more information about the boxes and list in this area, see [Configuring Policies, page 13-15](#).
- Step 5** (Optional) In the **Secondary Server configuration** pane:
- Check the **Secondary Server configuration** check box
 - Enter configuration details about the secondary NAC server. For more information about the boxes and list in this area, see [Configuring Policies, page 13-15](#).

- Step 6** Determine credentials to forward to the primary or secondary external server by moving the available credentials to the selected credentials column.
 - Step 7** Click **Submit** to save your changes.
 - Step 8** Click **Apply and Restart** to submit your changes to ACS.
-

Editing an External Posture Validation Server

You can edit an external posture validation server by accessing it through the Posture Validation pages.
To edit an external posture validation server:

- Step 1** In the navigation bar, click **Posture Validation**.
 - Step 2** Click **External Posture Validation Setup**.
 - Step 3** Click the server name that you want to edit.
The Add/Edit External Posture Validation Server page appears.
 - Step 4** Edit the fields and click **Submit**.
-

Deleting an External Posture Validation Server

You can remove an external posture validation server by accessing it through the Posture Validation pages.

To delete an external posture validation server:

- Step 1** In the navigation bar, click **Posture Validation**.
 - Step 2** Click **External Posture Validation Setup**.
 - Step 3** Click the server name that you want to delete.
The Add/Edit External Posture Validation Server page appears.
 - Step 4** Click **Delete**.
-

Setting Up an External AAA Server

This procedure describes how you can create an external policy that uses an external AAA server.

Before You Begin

You can choose external policies for more than one profile. To create external policies, use the External Posture Validation Setup pages. To add the policy to a profile, use the Network Access Profiles page. See [Classification of Access Requests, page 14-2](#).

The external server that you use to access the External Policy Validation page does not limit which profiles can choose the new external policy.

For descriptions of the options available on the External Policy Configuration page, see [Configuring Policies, page 13-15](#).

You can also set up an external AAA server that is used to evaluate SoHs from networks that include Microsoft Vista clients (NAC/NAP networks).

To set up an external posture validation server:

-
- Step 1** After you choose **External Posture Validation Setup**, the External Posture Validation Servers page displays.
 - Step 2** Under the External Posture AAA Servers table, click **Add Server**.
The Add/Edit External Posture AAA Server page appears.
 - Step 3** Name the server and provide a description if necessary.
 - Step 4** Provide addressing information for the primary and secondary servers:
 - a. Check the **Primary Server configuration** check box.



Note

If you do not choose the **Primary Server Configuration** check box, ACS uses the secondary server configuration. If no secondary server configuration exists or the secondary server is unreachable, ACS rejects the posture validation request.

- b. Provide configuration details about the primary external AAA server. For more information about the boxes and list in this area, see [Configuring Policies, page 13-15](#).
 - Step 5** (Optional) In the **Secondary Server configuration** pane:
 - a. Check the **Secondary Server configuration** check box
 - b. Enter configuration details about the secondary external AAA server. For more information about the boxes and list in this area, see [Configuring Policies, page 13-15](#).
 - Step 6** Determine the forwarding attributes to send to the primary or secondary external server by moving the available forwarding attributes to the chosen forwarding attributes column.
 - Step 7** Click **Submit** to save your changes.
 - Step 8** Click **Apply and Restart** to submit your changes to ACS.
-

Editing an External Posture AAA Server

You can edit an external posture AAA server by accessing it through the Posture Validation pages.

To edit an external posture validation server:

-
- Step 1** In the navigation bar, click **Posture Validation**.
 - Step 2** Click **External Posture Validation Setup**.
 - Step 3** Click the server name that you want to edit.
The Add/Edit External Posture AAA Server page appears.
 - Step 4** Edit the fields and click **Submit**.
-

Deleting an External Posture AAA Server

You can remove an external posture validation server by accessing it through the Posture Validation pages.

To delete an external posture validation server:

-
- | | |
|---------------|--|
| Step 1 | In the navigation bar, click Posture Validation . |
| Step 2 | Click External Posture Validation Setup . |
| Step 3 | Click the server name that you want to delete.
The Add/Edit External Posture AAA Server page appears. |
| Step 4 | Click Delete . |
-

Setting Up an External Audit Posture Validation Server

Use External Posture Validation Audit Server Setup page to add, edit, and delete external posture validation audit servers. Policies are reusable; you can associate an audit policy with more than one network access profile.

ACS does not include any non-Cisco attributes by default. Therefore, you must import a NAC Attribute Definition File (ADF) from each vendor application that you would like to validate in your NAC posture-validation policies. You can use the attributes that you add to create conditions for internal policies.

NAC introduces the ability to authorize network hosts not only based on user or machine identity; but also on a host's posture validation. The posture validation is determined by comparing the host's credentials to a posture-validation policy that you create from attribute-value pairs (AVPs), which Cisco and other vendors who are NAC partners define. Since the range of NAC attributes extends across many vendors and applications, you must import the non-Cisco attributes.

Before You Begin

Before you begin, you must:

- Add your audit vendor to the ACS internal dictionary.

ACS for Windows: You use the **CSUtil.exe** command. For detailed instructions, see [Importing External Audit Posture-Validation Servers](#), page C-34.

ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see [NAC Attribute Management \(ACS SE Only\)](#), page 8-44.

- Define destination user groups. See [Auditing Device Types](#), page 13-10.
- Configure RACs, if needed. See [RADIUS Authorization Components](#), page 4-6.

Adding an External Posture Validation Audit Server

To add an audit server for external posture validation:

-
- | | |
|---------------|---|
| Step 1 | Click Posture Validation in the navigation bar.
The Posture Validation Components Setup page appears. |
|---------------|---|

- Step 2** Click **External Posture Validation Audit Setup**.
The External Posture Validation Audit Server page appears.
- Step 3** Click **Add Server**.
The External Posture Validation Audit Server Setup page appears.
- Step 4** Type the **Name** that identifies the audit policy. See [Table 13-13 on page 13-37](#) for complete information on all options in this procedure.
- Step 5** Type a **Description** of the audit policy.
- Step 6** Select the appropriate options in the **Which Groups and Hosts are Audited** area. If necessary, identify hosts by using IP and MAC addresses.
- Step 7** Choose a **Posture Token**.
- Step 8** Choose an **Audit Server Vendor** in the **Use These Audit Servers** area.
- Step 9** Check the **Primary Server Configuration** option to configure a primary server.
- Step 10** Provide the configuration information for the primary server.

If your audit vendor does not appear, you must define an audit APT for the vendor in the internal ACS dictionary.

ACS for Windows: You use the **CSUtil.exe** command. For detailed instructions, see [Posture-Validation Attributes, page C-29](#).

ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see [NAC Attribute Management \(ACS SE Only\), page 8-44](#).
- Step 11** Check the **Secondary Server Configuration** option to configure a secondary server.
- Step 12** Provide the configuration information for the secondary server.
- Step 13** Choose a temporary posture token from the drop-down list in the **Audit Flow Settings** area.
- Step 14** Choose a timeout option.
- Step 15** Type a polling interval.
- Step 16** Choose the **Maximum amount of times the Audit Server should be polled**.
- Step 17** Type a **Policy string to be sent to the Audit Server**.
- Step 18** Check the **Request Device Type from Audit Server** option in the **Audit Policy** area if you want to cross-check the device types that the audit server and MAC authentication return.

If this check box is not available (greyed out), define an audit device type attribute for the vendor in the internal ACS dictionary.

ACS for Windows: You use the CSUtil.exe command. See [Posture-Validation Attributes, page C-29](#) for information.

ACS SE: You use the NAC Attributes Management page in the web interface. See [NAC Attribute Management \(ACS SE Only\), page 8-44](#) for more information.
- Step 19** Check the **Assign This Group if Audit Server Did not Return a Device-Type** option if you want to configure a default destination group.
- Step 20** Click **Add** to add a device-type feedback rule.
- Step 21** Choose a device type.
- Step 22** Choose the **User Group** that will be initially compared with the device type that MAC authentication returned.

- Step 23** Complete the **Device Type** comparison logic by choosing an operator and a device type. If the device type does not appear in the drop-down box, type a device type in the text box.
- Step 24** Choose the user group that ACS will assign based on the outcome of the device type comparison logic.
- Step 25** Click **Submit** to save your external posture validation audit server setup.
-

Editing an External Posture Validation Audit Server

You can edit an external posture validation audit server by accessing it through the Posture Validation pages.

To edit an external posture validation server:

-
- Step 1** In the navigation bar, click **Posture Validation**.
- Step 2** Click **External Posture Validation Audit Setup**.
- Step 3** Click the server name that you want to edit.
- The External Posture Validation Audit Server page appears.
- Step 4** Edit the fields and click **Submit**.
-

Deleting an External Posture Validation Server

You can remove an external posture validation audit server by accessing it through the Posture Validation pages.

To delete an external posture validation audit server:

-
- Step 1** In the navigation bar, click **Posture Validation**.
- Step 2** Click **External Posture Validation Audit Setup**.
- Step 3** Click the server name that you want to delete.
- The External Posture Validation Audit Server page appears.
- Step 4** Click **Delete**.
-

Audit Processing with MAC Authentication Bypass

An audit request can include a check against Agentless Host authentication. Audit server processing can double-check an audit request against a MAB authentication policy and an audit policy, and then combine the evaluation of the two policies.

Evaluating the combined policies is only possible in Layer 2 IP and Layer 3 NAC deployments because the audit request must contain the MAC address and IP address of an endpoint.

ACS requires the following key attributes for MAB and audit interoperability:

- [10] Service-type = 10

- [31] Calling-Station-ID = Endpoint *MAC Address*
- [8] Framed-IP-Address = Endpoint *IP address*
- [26:9:1] Cisco-AV-Pair = audit-session-id = *Id*
- [26:9:1] Cisco-AV-Pair = aaa:service = ip_admission

Workflow

This feature requires the following configuration options:

- A NAP using the Agentless Host template
- MAB authentication
- External posture validation audit
 - A GAME group feedback policy
 - User groups that will be audited
- Association of the audit serve with the network access profile

Processing

When the request is processed:

1. The audit request is evaluated against the Agentless Host policy.
2. The Agentless Host policy assigns a user group for the audit request.
3. The audit policy compares the assigned user group to its configured set of groups.
4. If the assigned group matches the configured set of groups, a GAME request is generated and the response is processed. If the assigned group does not match, a GAME request is not generated.
5. If there is a match, the authorization policy is processed and the resulting audit response is sent to the originating network access device.

Policy Configurations

ACS supports a number of configurations and capabilities for authenticating and authorizing agentless hosts. [Table 13-4](#) summarizes the policy combinations, capabilities, and configurations.

Table 13-4 Agentless Host Authentication and Authorization Support

Use Case		Audit			Authorization Based On	
Description	MAB	Grp Filter	Posture	Device Type	Token	Group from
MAB only.	Y	N	N	N	N	MAB
Audit for posture only.	N	N	Y	N	Y	None
Audit for posture and device type only. For example, differentiated azn based on the device type.	N	N	Y	Y	Y	None* or device type

Table 13-4 Agentless Host Authentication and Authorization Support (continued)

Use Case		Audit			Authorization Based On	
Description	MAB	Grp Filter	Posture	Device Type	Token	Group from
MAB and audit for posture. For example, even if MAB fails, healthy can be assigned.	Y	N	Y	N	Y	MAB
MAB and audit for posture and device type. For example, even if the MAC is not authenticated, printers get in.	Y	N	Y	Y	Y	MAB or device type
MAB and audit for posture. MAB success is mandatory. There is no need to audit if the MAC is not authenticated.	Y	Audit all but MAB failure group	Y	N	Y	MAB
MAB, Audit for posture and device type. MAB success is mandatory. There is no need to audit if the MAC is not authenticated.	Y	Audit all but MAB failure group	Y	Y	Y	MAB or device type
MAB, but if the MAC is not authenticated, then audit for posture. For example, MAB or a healthy token can be admitted to the network.	Y	Audit only MAB failure group	Y	N	Y	MAB
MAB, but if the MAC is not authenticated, audit for posture and device type. For example, managed devices are admitted to the network. Otherwise, azn is based on the device type or a token.	Y	Audit only MAB failure group	Y	Y	Y	MAB or device type

*In this case, group assignment depends on matching a device. Without matching, the group assignment policy for device types does not produce a user group.

You use the following procedure to configure Agentless Hosts and Audit interoperability.

- Step 1** In the navigation bar, click **Network Access Profiles**.
- Step 2** Click **Add Template Profile**.
- Step 3** Type a Name and Description for the profile.
- Step 4** Select the **Agentless Host** template.
- Step 5** Check **Active** to activate the profile, or leave it inactive.
- Step 6** In the navigation bar, click **Network Access Profiles**.
- Step 7** In the Protocols for the agentless host <profile_name>, check **Allow Agentless Request Processing**.
- Step 8** In Authentication for the agentless host <profile_name>, fill in the **Authenticate MAC With** section. See [Agentless Request Processing, page 14-24](#).
- Step 9** In the navigation bar, click **Posture Validation** and select External Posture validation Audit Setup.
- Step 10** Set up the Game Group Feedback Features. See [“Adding an External Posture Validation Audit Server” procedure on page 13-25](#).
- Step 11** Associate the Audit server to the Network Access Profile. See [Configuring Posture Validation for Agentless Hosts, page 14-33](#).

Posture Validation Pages Reference

The following topics describe the pages that you access from the **Posture Validation** button on the navigation bar:

- [Posture Validation Components Setup Page, page 13-30](#)
- [Internal Posture Validation Setup Pages, page 13-30](#)
- [External Posture Validation Setup Pages, page 13-33](#)
- [External Posture Validation Audit Setup Pages, page 13-36](#)

Posture Validation Components Setup Page

Use this page to access the posture validation pages.

To display the Posture Validation Components Setup page, click **Posture Validation** on the navigation bar.

Table 13-5 *Posture Validation Components Setup Page*

Option	Description
Internal Posture Validation Setup	Opens the Posture Validation Policies page. Internal policies contain rules that determine the posture token that ACS applies to a posture validation request.
External Posture Validation Setup	Opens the External Posture Validation Servers page. ACS forwards credentials to external posture validation servers, and the server then returns a posture token.
External Posture Validation Audit Setup	Opens the External Posture Validation Audit Server page. Audit servers return posture information for agentless hosts.

Internal Posture Validation Setup Pages

The following topics describe the Internal Validation Setup pages:

- [Posture Validation Policies Page, page 13-30](#)
- [Posture Validation Policy Page, page 13-31](#)
- [Posture Validation Rules for <policy_name> Page, page 13-31](#)
- [Posture Validation Rule - <policy_name> Page, page 13-32](#)
- [Add/Edit Condition Page, page 13-33](#)

Posture Validation Policies Page

Use this page to add policies or to access existing policies for editing.

To display the Posture Validation Policies page, click **Posture Validation** on the navigation bar, then choose **Internal Posture Validation Setup**.

Table 13-6 *Posture Validation Policies Page*

Option	Description
Posture Validation Policies	The Name and Description identify the policy. The Policy Details list the rules associated with the policy, by ID number.
Name <i><policy_name></i>	Opens the Posture Validation Policy page for editing.
Add Policy	Opens the Posture Validation Policy page for creation of a new policy.

Posture Validation Policy Page

Use this page to specify the name and description for a new policy.

To display the Posture Validation Policy page, choose **Posture Validation > Internal Posture Validation Setup > Add Policy**.

Table 13-7 *Posture Validation Policy Page*

Option	Description
Name	Defines the policy name. The name should be descriptive because the Descriptions do not appear when a policy name is selected. The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the left bracket ([), the right bracket (]), the comma (,), or the slash (/).
Description	Provides a text description of the policy, up to 255 characters. Because the same policy can apply to more than one profile, a useful description helps to prevent accidental configuration errors when someone modifies a policy without understanding the servers that use it.
Submit	Opens the Posture Validation Rules for <i><policy_name></i> page, where <i><policy_name></i> is the name of the new policy.

Posture Validation Rules for *<policy_name>* Page

Use this page to display and order rules.

To display the Posture Validation Rules for *<policy_name>* page when editing a rule, choose **Posture Validation > Internal Posture Validation Setup > *<policy_name>***.

Table 13-8 *Posture Validation Rules for <policy_name> Page*

Option	Description
Posture Validation Rules for <Name>	Lists each rule by ID number. Provides the rule Conditions and Actions (as Posture Token and Notification String). The Description (if specified) provides information about the policy.
Condition <condition_name>	<p>Opens the Posture Validation Rule - <policy_name> page, where you can edit an existing condition.</p> <p>If no configurable rule is true, the Default Rule specifies the posture assessment, token, and notification string (if specified) that ACS uses as the result of applying the policy.</p> <p>Under the Default Rule, the meanings of the Posture Assessment list, Token list, and Notification String box are identical to the options of the same name in the Posture Validation Rules table; except that the default rule is automatically true, provided that no rule in the Posture Validation Rules table is true.</p>
Add Rule	Opens the Posture Validation Rule - <policy_name> page where you can create a rule.
Up, Down	Moves a selected rule. Submits the sort order to the database.
Rename	Opens the Posture Validation Policy page where you can rename the policy.
Clone	Creates a policy identical to a selected policy. Edit the cloned policy to create a new policy.
Delete	Deletes a policy.
Done	Opens the Posture Validation Policies page.

Posture Validation Rule - <policy_name> Page

Use this page to view and edit rules.

To display the Posture Validation Rules for <policy_name> page when adding a rule, choose **Posture Validation > Internal Posture Validation Setup > <policy_name> > <condition>**.

Table 13-9 *Posture Validation Rule - <policy_name> Page*

Option	Description
Condition Sets	<p>Lists the condition sets that are associated with a rule. A <condition_name> opens the Add/Edit Condition page.</p> <p>When adding or editing a rule, a compound Boolean expression determines the logical treatment of the conditions that are associated with a rule.</p> <ul style="list-style-type: none"> Match OR inside Condition and AND between Condition Sets—Provides a less strict treatment of conditions. Match AND inside Condition and OR between Condition Sets—Provides a more strict treatment of conditions.
Add Condition Set	Opens the Add/Edit Condition page.

Table 13-9 *Posture Validation Rule - <policy_name> Page (continued)*

Option	Description
Posture Token	Specifies the vendor and application, and a token (an APT). If the rule is true, the Token list determines the APT that is associated with the vendor and application that is selected in the corresponding Posture Assessment list. For more information about tokens, see Posture Tokens, page 13-3 .
Notification String	Specifies a text message that is sent to the application that the Result Credential Type list indicates. The vendor determines use of the text message. Some NAC-compliant applications do not implement the use of the Notification String box.

Add/Edit Condition Page

Use this page to add or edit conditions.

To display the Posture Validation Rules for <policy_name> page when adding a rule, choose **Posture Validation > Internal Posture Validation Setup > <policy_name> > <condition> > <condition_set>**.

Table 13-10 *Add/Edit Condition Page*

Option	Description
Condition Elements Table	Lists each condition. Specifies a vendor and application; the credential type. If the rule is true, the credential type determines the application to which the token in the corresponding Token list is associated. For example, the Cisco Trust Agent appears on the list as <code>Cisco:PA</code> . For more information about credential types, see About Posture Credentials and Attributes, page 13-5 .
Attribute	Lists the available attributes.
Entity	Lists the available entities for attributes that require entities.
Operator	Lists the appropriate operators for this attribute.
Value	Specifies an appropriate value for the attribute.

External Posture Validation Setup Pages

The following topics describe the External Posture Validation Setup pages:

- [External Posture Validation Servers Page, page 13-33](#)
- [Add/Edit External Posture Validation Server Page, page 13-34](#)

External Posture Validation Servers Page

Use this page to view existing external posture validation servers.

To display the External Posture Validation Servers page, choose **Posture Validation > External Posture Validation Setup**.

Table 13-11 *External Posture Validation Servers Page*

Option	Description
Name	Opens the Add/Edit External Posture Validation Server page for editing of an existing policy. Description, Forward Credential Type, and Server Details show the current configuration of the policy.
Add Server	Opens the Add/Edit External Posture Validation Server page for creation of a new policy.

Add/Edit External Posture Validation Server Page

Use this page to add or edit external posture validation servers.

To display the Add/Edit External Posture Validation Server page, choose **Posture Validation > External Posture Validation Setup**. Then click **Add Server** to add a server or click **<server_name>** to edit a server.

Table 13-12 *Add/Edit External Posture Validation Server Page*

Option	Description
Name	Specifies the name by which to identify the server. The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the left bracket ([), the right bracket (]), the comma (,), or the slash (/).
Description	Specifies a text description of the server, up to 255 characters. For each profile using the policy, the text you type in the Description box appears beside the policy. In the Description box you can add the details that you could not convey in the name of the policy. For example, you could describe its purpose or summarize its rules. Because you can apply the same policy to more than one profile, a useful description could also help prevent accidental configuration errors when someone modifies a policy without understanding which profiles use it.
Primary Server Configuration Secondary Server Configuration	Enables a primary NAC server (and an optional secondary NAC server). ACS relies on these servers to apply the policy and configure the set of credential types that ACS forwards. For each posture validation request to which an external policy is applied, ACS attempts to use the first enabled server configuration in the policy that is enabled. If the first enabled server is the primary server and ACS cannot reach the primary server or the primary server fails to respond to the request, ACS will use the secondary server, if it is configured and enabled.

Table 13-12 Add/Edit External Posture Validation Server Page (continued)

Option	Description
URL	<p>Specifies the HTTP or HTTPS URL for the server. The format for URLs is:</p> <pre>[http[s] ://]host[:port]/resource</pre> <p>where <i>host</i> is the hostname or IP address of the NAC server, <i>port</i> is the port number used, and <i>resource</i> is the rest of the URL, as required by the NAC server itself. The URL varies depending on the server vendor and configuration. For the URL that your NAC server requires, refer to your NAC server documentation.</p> <p>The default protocol is HTTP. URLs beginning with the hostname are assumed to be using HTTP. To use HTTPS, you must specify the URL beginning with <code>https://</code> and import a self-generated CA certificate into ACS for this policy server. See ACS Certificate Setup, page 9-22.</p> <p>If the port is omitted, the default port is used. The default port for HTTP is port 80. The default port for HTTPS is port 443.</p> <p>If the NAC server hostname is <i>antivirus1</i>, which uses port 8080 to respond to HTTP requests for the service provided <i>policy.asp</i>, a script kept in a web directory called <i>cnac</i>, valid URLs would be:</p> <pre>http://antivirus1:8080/cnac/policy.asp antivirus1:8080/cnac/policy.asp</pre> <p>If the same server used the default HTTP port, valid URLs would be:</p> <pre>http://antivirus1/cnac/policy.asp http://antivirus1:80/cnac/policy.asp antivirus1/cnac/policy.asp antivirus1:80/cnac/policy.asp</pre> <p>If the same server used HTTPS on the default port, valid URLs would be:</p> <pre>https://antivirus1/cnac/policy.asp https://antivirus1:443/cnac/policy.asp</pre>
Username	Specifies the username required for access to the server. The server ignores the values in the Username and Password fields if the server is not password protected.
Password	Specifies the password required for access to the server. The server ignores the values in the Username and Password fields if the server is not password protected.
Timeout (Sec)	<p>The number of seconds that ACS waits for a result from the external server, including domain name resolution. The Timeout value must be greater than zero (0). The default is 10.</p> <p>ACS forwards requests to the secondary server (if configured) when the primary server times out. If no secondary server is configured or if a request to the secondary server also times out, ACS cannot apply the external policy and therefore rejects the posture validation request.</p> <p>For each posture validation request, ACS always tries the primary server first, regardless of whether previous requests timed out.</p>

Table 13-12 **Add/Edit External Posture Validation Server Page** (continued)

Option	Description
Trusted Root CA	<p>The certificate authority (CA) that issued the server certificate, which the server uses. If the protocol is HTTPS, ACS forwards credentials to a server only if the CA that is specified on this list issued the certificate that it presents. If ACS cannot forward the request to the primary or secondary NAC server because the trusted root CAs did not issue the server certificates, the external policy cannot be applied and, therefore, the posture validation request is rejected.</p> <p>The Trusted Root CA list does must contain the CA that issued a NAC server certificate. For information, see Adding a Certificate Authority Certificate, page 9-26.</p> <p>ACS does not check NAC server certificates against Certificate Revocation Lists (CRLs), even if a configured CRL issuer for the CA of the NAC server certificate is present.</p> <p>The certificate name and type must match. For example, if the server presents a VeriSign Class 1 Primary CA certificate and VeriSign Class 1 Public Primary CA is selected on the Trusted Root CA list, ACS does not forward the credentials to the server when HTTPS is in use.</p>
Forwarding Credential Types	<p>The Available Credentials list specifies the credential types that <i>are not</i> sent to the external server. The Selected Credentials list contains the credential types that <i>are</i> sent to the external server.</p> <p>See the following information to add credential types to the Available Credentials list.</p> <p>ACS for Windows: You use the CSUtil.exe command. For detailed instructions, see Importing External Audit Posture-Validation Servers, page C-34.</p> <p>ACS SE: You use the NAC Attributes Management page in the web interface. For detailed instructions, see NAC Attribute Management (ACS SE Only), page 8-44.</p>

External Posture Validation Audit Setup Pages

The following topics describe the External Posture Validation Audit Setup pages:

- [External Posture Validation Audit Server Page, page 13-36](#)
- [External Posture Validation Audit Server Setup Page, page 13-36](#)

External Posture Validation Audit Server Page

Use the External Posture Audit Server page view the name, description, server details, and current posture tokens for each configured server.

To display the Add/Edit External Posture Validation Server page, choose **Posture Validation > External Posture Validation Audit Setup**.

External Posture Validation Audit Server Setup Page

Use this page to add or edit external posture validation audit servers.

Add Server Page

To display this page, choose **Posture Validation > External Posture Validation Audit Setup > Add Server**.

Edit Server Page

To display this page, choose **Posture Validation > External Posture Validation Audit Setup**, then click the **<server_name>**. You can edit the Audit Server settings as needed, but:

- If the audit policy is associated with more than one NAP, changes to the policy affect posture validation for each associated NAP.
- If you change the name of a policy, you are creating a new policy when you click **Submit**. You cannot rename a policy and change the settings of an existing policy at the same time.

Table 13-13 External Posture Validation Audit Server Setup Options

Option	Description
Name	The name for the audit policy. The name can contain up to 32 characters. Leading and trailing spaces are not allowed. Names cannot contain the left bracket ([), the right bracket (]), the comma (,), or the slash (/).
Description	Describes the audit policy (up to 255 characters).
Which Groups and Hosts are Audited	
Audit all user groups Audit these user groups Do not audit these user groups	The user group options determine the auditing of the groups in the Selected Groups list.
Audit all hosts Audit these hosts Do not audit these hosts	Audit all hosts that do not contain a posture agent. Audit only certain hosts or exclude certain hosts as defined in the Host IP Addresses and Ranges (IP/MASK) (comma-separated values) field. For Host MAC Address (comma-separated values), ACS accepts two MAC address formats, <i>00-0D-60-FB-16-D3</i> or <i>000D.60FB.16D3</i> . MAC prefixes that serve as ranges are acceptable. For example, <i>00-0D-60-FB-16</i> or <i>000D.60</i> would match any MAC address that begins with these bytes. MAC prefixes must contain an even number of hexadecimal digits. MAC address matching is case sensitive.
Select a Posture Token for the hosts that will not be audited	A posture token that ACS will apply to hosts that are not audited.
Use These Audit Servers	
Audit Server Vendor	Vendors that have an audit Application Posture Token (APT) defined in the internal ACS dictionary appear in the drop-down list. If no audit servers appear in the drop-down list, see Posture-Validation Attributes, page C-29 (ACS for Windows) or NAC Attribute Management (ACS SE Only), page 8-44 , for information on setting up audit servers.
Primary Server Configuration, Secondary Server Configuration	Each option enables configuration of audit servers. ACS requires a primary server. The secondary server provides failover capability (not required). The options for a Secondary Server Configuration are identical to the options for a Primary Server Configuration.

Table 13-13 External Posture Validation Audit Server Setup Options (continued)

Option	Description
URL	<p>The URL of the audit server. Specify the HTTP or HTTPS protocol.</p> <p>URLs must conform to the following format:</p> <pre>[http[s] ://]host[:port]/resource</pre> <p>where host is the hostname or IP address of the external server, port is the port number used, and resource is the rest of the URL, as required by the external server. The URL varies depending on the server vendor and configuration.</p> <p>The audit server documentation contains specific format guidelines.</p>
Username	The username that the audit server requires.
Password	The password that the audit server requires.
Timeout (sec)	The number of seconds that ACS waits for a result from the audit server, including domain name resolution. The Timeout value must be greater than zero (0).
Trusted Root CA	A certification authority that is required if the URL of the audit server specifies the HTTPS protocol. This option should match the certification authority that issued the audit server certificate installed on the primary server.
Validate Certificate Common Name	When checked (enabled), this option shows the host name within the URL for purposes of comparison with the common name in the certificate. If the names do not match, ACS closes the SSL connection, posture validation fails, and user access is denied.
Audit Flow Settings	
Use this Posture Token while Audit Server does not yet have a posture validation result	Interim posture token sent from ACS to the NAD while waiting for a result. ACS uses the In Progress token before the Audit Server determines the actual posture of the nonresponsive host.
Polling Intervals and Session-Timeout	Either the timeout values that are sent by the audit server or that are set in the authorization policy. ACS requires a polling interval if the configuration uses the values that are set in the authorization policy. The authorization policy must include the necessary RACs in order to assign specific timeout values in the final resulting tokens. See Configuring an Authorization Rule, page 14-36 .
Maximum amount of times the Audit Server should be polled	The maximum number of times that ACS will query the audit server for a result (posture token). Range of 1–10 times.
Policy string to be sent to the Audit Server	The name of the policy, if the audit server supports named policy invocation.
GAME Group Feedback	
Request Device Type from Audit Server	<p>Enables the audit policy configuration options. When enabled, the Audit feature can request a device type from the audit server and then check the device type against the device type that MAC authentication returns.</p> <p>If this check box is not available, define an audit device type attribute for the vendor in the internal ACS dictionary.</p> <p>ACS for Windows: Use the CSUtil.exe command. See Posture-Validation Attributes, page C-29 for information.</p> <p>ACS SE: Use the NAC Attributes Management page in the web interface. See NAC Attribute Management (ACS SE Only), page 8-44 for more information.</p>

Table 13-13 *External Posture Validation Audit Server Setup Options (continued)*

Option	Description
Assign This Group if Audit Server Did not Return a Device Type	Enables assignment of a device to any administrator-defined group when the audit server does not return a device type.
User Group	Lists all user groups, including Any. The device type that MAC authentication returns is initially compared with this list of device types.
Device Type	<p>Defines the comparison criteria for the User Group, using an operator and device type.</p> <p>Valid values for the operator are:</p> <ul style="list-style-type: none"> match-all = != contains starts-with regular-expression <p>Valid values for the device type drop-down are not editable. They include:</p> <ul style="list-style-type: none"> Printer IP Phone Network Infrastructure Wireless Access Point Windows Unix Mac Integrated Device PDA Unknown <p>Type a device type in the text box if the device type drop-down does not contain a particular device.</p>
Assign User Group	A drop-down list of administrator-defined user groups. If the comparison of the initial User Group with the Device Type succeeds, ACS will assign this user group.
Add, Delete, Up, Down	Controls that affect the user groups.
Submit, Delete, Cancel	<p>Controls that affect the whole policy.</p> <p>An audit policy can be in use with more than one NAC Network Access Profile. Before deleting a policy, you must identify the NAC Network Access Profiles that the deletion will affect.</p>



CHAPTER 14

Network Access Profiles

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, supports Network Access Profiles (NAP).

This chapter describes NAPs and contains:

- [Overview of NAPs, page 14-1](#)
- [Managing NAPs, page 14-4](#)
- [Using Profile Templates, page 14-7](#)
- [Configuring Policies for Profiles, page 14-22](#)
- [Policy Replication and Backup, page 14-38](#)
- [Network Access Profiles Pages Reference, page 14-39](#)

Overview of NAPs

Typical organizations have various kinds of users who access the network in different ways and for different purposes. Correspondingly, you must apply different security policies to the different use cases. For example, you might have to apply a tighter and more limiting security policy to the wireless access points of your building's lobby area, versus the physically secured production plant. Or, you might have to treat remote-access users who use a virtual private network (VPN) differently from users who log in from behind a firewall. Users who connect through certain subnetworks might be authenticated differently from other users. Wireless access is often treated more strictly than wired access, as is any form of remote access (for example, dial, VPN, home wireless).

A NAP, also known as a *profile*, is essentially a classification of network-access requests for applying a common policy. You can use NAPs to aggregate all policies that should be activated for a certain location in the network. Alternatively, you can aggregate all policies that handle the same device type, for example, VPNs or Access Points (APs).



Note

The Terminal Access Controller Access Control System (TACACS+) protocol for NAPs is not supported in ACS.

The following topics describe NAPs and their associated policies:

- [Classification of Access Requests, page 14-2](#)
- [Profile-based Policies, page 14-3](#)
- [Workflow for Configuring NAPs and Profile-based Policies, page 14-3](#)

- [Processing Unmatched User Requests, page 14-3](#)

Classification of Access Requests

You can classify access requests according to the AAA clients' IP addresses, membership in a network device group (NDG), protocol types, or other specific RADIUS attribute values sent by the network device through which the user connects.

You can use one or all of the following classification methods to classify access requests:

- [NAFs, page 14-2](#)
- [Protocol Types, page 14-2](#)
- [Advanced Filtering, page 14-2](#)

The profile is selected when all the selected conditions match. For each condition, the value **Any** always matches the condition. For example, if you create a network access filter (NAF) for wireless and then select the Aironet Protocol type, only devices with the protocol types in the wireless NAF will be selected for filtering.

NAFs

NAFs are groupings of AAA client configurations (which might represent multiple network devices), NDGs, or IP addresses of specific AAA client devices. You can use a NAF to group (and name) a disparate set of devices; for example: *these devices comprise the abc network service*.

You can also use NAFs to differentiate user requests on the same type of device. For example, while you undertake an IOS upgrade of Aironet wireless APs is undertaken (perhaps to enable some new encryption protocol) you might require a separate NAP for upgraded and nonupgraded APs.



Note

If you want to aggregate NDGs and use them as a filter to assign users to a profile, you must configure NAFs before you set up a profile.

Protocol Types

You use Protocol Types to classify a user request based on the type of protocol that is used to request access to the network.

Advanced Filtering

You can create rules based on specific RADIUS attributes and values (including Cisco AV pairs). Each rule contains one or more rule elements, and each rule element must be true for the whole rule to be true. In other words, all rule elements of a rule are joined with a Boolean AND. For more information about advanced filtering options, see [Profile Setup Page, page 14-40](#).

Profile-based Policies

After you set up a profile, you associate a set of rules or policies with it to reflect your organization's security policies. These *profile-based policies* include rules for authentication, authorization, and posture validation.

By defining profile-based policies, you can redirect authentication to different directories. For example, wireless users need to authenticate to AD while the same users who access the network through VPN might need to authenticate to an RSA One-Time Password (OTP) directory.

When a packet is received, ACS evaluates the profile filters to classify the packet. When a profile matches, ACS applies the configuration and policies that are associated with the profile during packet processing. ACS uses a first-match strategy on the first access request of the transaction. If no matching profile is found, ACS reverts to the global configuration settings.

Workflow for Configuring NAPs and Profile-based Policies

You can create a profile from scratch, or you can use one of the supplied templates to populate some default values. The templates that are provided are particularly useful for NAC-enabled networks. See [Using Profile Templates, page 14-7](#), for more information.

The following is the order of work for creating NAPs and their associated policies:

1. Identify the network services that you want to control with ACS (for example, VPN, Dial, WLAN, ip_admission).
2. Set up a profile for each network service. Setting up a profile defines how ACS will recognize or identify requests for example, device IP, NDG, NAF, advanced filtering). For more information, see [Adding a Profile, page 14-4](#).
3. Define the password protocols and EAP configuration for the service. For more information, see [Protocol Configuration for NAPs, page 14-23](#).
4. Define the authentication methods that are required for the service. For more information, see [Authentication Policy Configuration for NAPs, page 14-27](#).
5. Define the posture-validation policies or rules (optional, if network admission control (NAC) is part of the deployment). See [Posture-Validation Policy Configuration for NAPs, page 14-29](#) for more information.
6. Define SoH rules. See [Setting a Posture-Validation Policy to Process Statements of Health, page 14-32](#) for more information.
7. Define the authorization mappings from group to RADIUS authorization components (RAC) and downloadable access control lists (DACL). Also include the system posture token (SPT) if NAC is in use. For more information, see [Configuring an Authorization Rule, page 14-36](#).

If access is granted (`access-accept`) ACS merges between user, user-group RAC and ACLs, and provisions a result to the AAA client. For more information, see [Merging Attributes, page 14-35](#).

Processing Unmatched User Requests

In ACS you can configure global configuration settings as well as NAP-specific settings. The global configuration settings serve two purposes:

- Defining the fallback behavior for a request that does not match a profile.

- Defining the baseline for NAPs (if you want to enable a protocol in the NAP authentication page, you must first enable it in the Global Authentication Setup page).

Although legacy global settings and NAPs are supported and are interoperable, we do not recommend both of them, except for the case that is described in this section.

We recommend that you deny access when no profile matches and the access request cannot be classified.

The only case where ACS fallback behavior and NAPs should be used is with TACACS+. NAPs does not currently support TACACS+. Granting access using the global configuration is the only way to use TACACS+ and NAP configuration with RADIUS.

When you use both, you must ensure that the fallback behavior using global configuration will not create a security flaw in the network.

Managing NAPs

These topics describe how to set up and manage NAPs:

- [Adding a Profile, page 14-4](#)
- [Ordering Profiles, page 14-5](#)
- [Editing a Profile, page 14-5](#)
- [Cloning a Profile, page 14-6](#)
- [Deleting a Profile, page 14-6](#)
- [Using Profile Templates, page 14-7](#)

Adding a Profile

This topic describes how to set up a profile from scratch. For information about creating a profile from a profile template, see [Using Profile Templates, page 14-7](#).

To add a profile:

-
- | | |
|---------------|---|
| Step 1 | In the navigation bar, click Network Access Profiles .
The Network Access Profiles Page appears. |
| Step 2 | Click Add Profile .
The Profile Setup page appears. |
| Step 3 | In the Name box, type the name of the new profile. |
| Step 4 | In the Description box, type a description of the new profile. |
| Step 5 | To enable the profile, check the Active check box. |
| Step 6 | Configure the access request classification settings for the profile. See Profile Setup Page, page 14-40 for more information about profile configuration options. |
| Step 7 | Click Submit .
The Network Access Profile page reappears. The Network Access Profile's first match is implemented to authenticate or authorize a client request, or both. |

- Step 8** Click the **Up** or **Down** buttons to move the profile to the correct position and submit the information to ACS.
- Step 9** Configure how ACS should handle unmatched access requests. See [Processing Unmatched User Requests, page 14-3](#) for information.
- Step 10** Click **Apply and Restart** for your changes to take effect.
-

Ordering Profiles

Since ACS applies a first-match principle when trying to match an access request with a profile, the order of the profiles in the list is significant.

To set the order of the profile:

- Step 1** In the [Network Access Profiles Page, page 14-39](#), click the radio buttons to select a profile.
- Step 2** Click the **Up** or **Down** to move the profile to the position you want.
- Step 3** Click **Apply and Restart** for your changes to take effect.
-

Editing a Profile

To edit the profile configuration:

- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page appears.
- Step 2** To modify the filtering methods for a profile:
- In the Network Access Profiles page, click the profile name.
The Profile Setup page appears.
 - Modify filtering methods, as required. For information about filtering options, see [Profile Setup Page, page 14-40](#).
- Step 3** To modify configuration policies for a profile:
- Select the relevant configuration policy for the profile.
The relevant policy configuration page appears.
 - Edit the policy. For more information, see [Configuring Policies for Profiles, page 14-22](#).
- Step 4** To save your profile configuration settings, return to the Network Access Profiles page and click **Apply and Restart**.
-

Cloning a Profile

Cloning replicates all the following relevant components for a NAP:

- **Protocol references**—Password protocols.
- **Authentication references**—External databases.
- **Posture references**—Internal or external posture validation, and external audit server. For more information about posture references, see [Setting Up Posture Validation Policies, page 13-16](#).
- **Authorization references**—RACs and DACLS.

Cloning a NAP does not copy the shared-profile components, or the internal and external posture-validation policies, that the profile references. The newly cloned profile *references* the same shared-profile components as the original profile. For example, components that are referenced by name (RACs, DACLS, NAFs) remain the same.

When you clone a NAP, it is initially inactive by default. This inactive state avoids ambiguity when ACS tries to match an access request to a profile. After you modify the cloned profile, you can change the status to the active state.

The Profile description, Active Flag, Protocol Selection, Advanced Filter, Authentication, and Authorization policies are all cloned (copied). Posture-validation policies (Internal/External/Audit Servers) are not copied, but are referenced by the newly created Profile.

The naming pattern for cloning is **Copy-of-**. For multiple cloning (cloning the cloned element) the prefix **Copy-(2)-of-** is given.

If the new name length exceeds 32 characters, it is truncated to 32 characters.

To clone a profile:

-
- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page appears.
 - Step 2** Click the name of the profile you want to clone.
The Profile Setup page appears.
 - Step 3** Click **Clone**.
A copy of the cloned profile appears in the Network Access Profiles page.
 - Step 4** (Optional) Modify the cloned profile. For information about editing profiles, see [Editing a Profile, page 14-5](#).
 - Step 5** Click **Apply and Restart** for your changes to take effect.
-

Deleting a Profile

To delete a profile:

-
- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page appears.
 - Step 2** Click the **Name**.

- The Profile Setup page appears.
- Step 3** Click **Delete**.
- A warning message appears.
- Step 4** Click **OK** to delete the profile configuration.
- Step 5** Click **Apply and Restart** for your changes to take effect.
-

Using Profile Templates

You use a *profile template* to construct a new profile. Instead of setting up a new profile from scratch, you can select a profile from a predefined set of profile templates. For a list of templates, see [Profile Templates, page 14-8](#). The templates include a preconfigured set of NAC samples that you can use as the basis for building NAC policies. After you have set up a new profile based on a template, you can customize the profile settings to the specific needs of your security policy.



Note

Each template references a set of shared-profile components. Before creating a template, ACS verifies that the appropriate shared-profile components exist. If the shared-profile components were not configured, ACS uses a set of shared-profile components that were created especially for the selected template.

When you select a predefined template, ACS creates a full-scale NAP, including profile authentication, posture validation, and authorization policies.

The following topics describe profile templates and how to use them:

- [Prerequisites for Using Profile Templates, page 14-7](#)
- [Creating a Profile with a Profile Template, page 14-8](#)
- [Profile Templates, page 14-8](#)

Prerequisites for Using Profile Templates

Before you can use a profile template, you must configure:

- At least one AAA client by using the RADIUS Internet Engineering Task Force (IETF) protocol.
- Certificate setup.
- Administrator accounts (if needed).
- Logging settings.
- Global Authentication Setup for templates, depending on the template.
- User-Level or Group-Level Downloadable ACLs in the Interface Configuration > Advanced Options, depending on the template.

ACS rules are constructed from attributes that reside in the ACS dictionaries. During installation, the ACS posture dictionary is initialized to include attributes that belong to the `cisco:pa`. (It is mandatory that this default set of attributes be supported by every Cisco Trust Agent implementation.)

The internal posture-validation policies that the templates create are based on these sets of attributes.

In ACS, each template that is created references a set of reusable objects. Before creating the template, ACS verifies that the relevant reusable objects already exist. If they do not, ACS automatically creates the required objects for the template. Creation of profiles from templates will not fail if these objects do not exist beforehand. If the reusable objects exist for the selected template, ACS uses the relevant reusable objects.

**Note**

You cannot delete an attribute if it is being used in a posture-validation policy.

Creating a Profile with a Profile Template

To select a profile template:

-
- Step 1** In the navigation bar, click **Network Access Profiles**.
The Network Access Profiles page appears.
 - Step 2** Click **Add Template Profile**.
The [Create Profile from Template Page, page 14-43](#), appears.
 - Step 3** Enter a **Name** and **Description** for the Profile.
 - Step 4** Select a template from the drop-down list.
 - Step 5** Check the **Active** check box to activate the profile.
 - Step 6** Click **Submit**.
A window appears showing the new objects that have been created for the profile.
 - Step 7** Click **Close**.
The Network Access Profiles page reappears showing the new profile.
 - Step 8** To save your profile configuration settings, click **Apply and Restart**.
-

Profile Templates

These topics describe the profile templates that ACS provides:

- [NAC L3 IP, page 14-9](#)
- [NAC L2 IP, page 14-11](#)
- [NAC Layer 2 802.1x, page 14-14](#)
- [Microsoft IEEE 802.1x, page 14-16](#)
- [Wireless \(NAC L2 802.1x\), page 14-17](#)
- [Agentless Host for L2 \(802.1x Fallback\), page 14-17](#) (802.1x fallback)
- [Agentless Host for L3, page 14-18](#) (EAP over User Datagram Protocol (UDP) fallback)
- [Agentless Host for L2 and L3, page 14-20](#)

NAC L3 IP

This template is used for access requests from a LAN Port IP by using Layer 3 posture validation.

Before you use this template, ensure that you have checked the following options in the Global Authentication Setup page:

- Allow Posture Validation.
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) authenticated in-band PAC provisioning.
- EAP-FAST MS-CHAPv2.
- EAP-FAST Generic Token Card (GTC).

Downloadable ACLs

Downloadable per-user ACL support is available for Layer 3 network devices that support downloadable ACLs. These include Cisco PIX security appliances, Cisco VPN solutions, and Cisco IOS routers. You can define sets of ACLs that you can apply per user or per group. This feature complements NAC support by enabling the enforcement of the correct ACL policy. When you use this feature in conjunction with NAFs, you can apply downloadable ACLs can differently per device, allowing you to tailor ACLs uniquely per user or per access device.

Table 14-1 describes the Profile Sample in the NAC Layer 3 IP Sample Profile Template.

Table 14-1 **NAC Layer 3 IP Profile Sample**

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	([[26/9/1]Cisco av-pair]aaa:service = ip_admission) AND ([006]Service-Type != 10)
Authentication	Protected Extensible Authentication Protocol (PEAP)	Allow Posture Only is checked
	Credential Validation Database	N/A

Table 14-1 NAC Layer 3 IP Profile Sample (continued)

Section	Property		Value		
Posture Validation	Posture Validation Rule	Name	NAC-EXAMPLE-POSTURE-EXAMPLE		
		Required credential types	Cisco:PA		
		Selected internal posture policies	NAC-SAMPLE-CTA-POLICY		
		Selected external posture policies	N/A		
		System Posture Token configuration	System Posture Token	PA message	URL Redirect
			Healthy	Healthy	N/A
			Checkup	Checkup	N/A
			Transition	Transition	N/A
			Quarantine	Quarantine	N/A
			Infected	Infected	N/A
			Unknown	Unknown	N/A

Table 14-2 Authorization Rules for NAC Layer 3 IP Profile Template

Authorization Rules	User Group	System Posture Token	Shared RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC-SAMPLE-HEALTHY-ACL
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC-SAMPLE-QUARANTINE-ACL
Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Table 14-3 describes the posture-validation policies in the NAC Layer 3 IP Sample Profile Template.

Table 14-3 Posture Validation for NAC Layer 3 IP Sample

Section	Object	Value
Internal posture policy	NAC-SAMPLE-CTA-POLICY	Condition
	Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0
	Default	N/A
		System Posture Token
		Cisco:PA:Healthy
		Notification String
		N/A
		Cisco:PA:Quarantine
		N/A

Table 14-4 describes the Shared Profile Components in the NAC Layer 3 IP Sample Profile Template.

Table 14-4 Shared Profile Components for NAC Layer 3 IP Sample

Type	Object	Value
RADIUS Authorization Components	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [26/9/1]cisc-av-pair status-query-timeout=300 [029] Termination-Action RADIUS-Request (1)
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [26/9/1]cisc-av-pair status-query-timeout=30 [029] Termination-Action RADIUS-Request (1)
Downloadable IP ACLs	NAC-SAMPLE-HEALTHY-ACL	ACL Content Name
	NAC-SAMPLE-QUARANTINE-ACL	L3-EXAMPLE
		Content
		permit ip any any
		NAF
		(All-AAA-Clients)

NAC L2 IP

Before you use this template, ensure that you have checked the Enable EAP Configuration > Allow Posture Validation option in the Global Authentication Setup page.

You can use NAC Layer 2 IP on an access port on an edge switch to which an endpoint system or client is connected. The device (host or client) can be a PC, a workstation, or a server that is connected to the switch access port through a direct connection, an IP phone, a hub, or a wireless access point.

When NAC Layer 2 IP is enabled, UDP only works with IPv4 traffic. The switch checks the antivirus condition of the endpoint devices or clients and enforces access-control policies.

This template sets Advanced Filtering and Authentication properties with NAC-L2-IP Configuration automatically.

ACS and AV Pairs

When you enable NAC Layer 2 IP validation, ACS provides NAC AAA services by using RADIUS. ACS gets information about the antivirus credentials of the endpoint system and validates the antivirus condition of the endpoint.

You can set these Attribute-Value (AV) pairs on ACS by using the RADIUS cisco-av-pair vendor-specific attributes (VSAs).

- **Cisco Secure-Defined-ACL**—Specifies the names of the downloadable ACLs on the ACS. The switch gets the ACL name through the Cisco Secure-Defined-ACL AV pair in this format:

#ACL#-IP-name-number

where *name* is the ACL name and *number* is the version number, such as 3f783768.

The Auth-Proxy posture code checks if the access-control entries (ACEs) of the specified downloadable ACL were previously downloaded. If it was not, the Auth-Proxy posture code sends an AAA request with the downloadable ACL name as the username so that the ACEs are downloaded. The downloadable ACL is then created as a named ACL on the switch. This ACL has ACEs with a source address of **Any** and does not have an implicit **Deny** statement at the end. When the downloadable ACL is applied to an interface after posture validation is complete, the source address is changed from any to the host source IP address. The ACEs are prepended to the downloadable ACL that is applied to the switch interface to which the endpoint device is connected.

If traffic matches the Cisco Secure-Defined-ACL ACEs, the appropriate NAC actions are taken.

- **url redirect and url-redirect-acl**—Specifies the local URL policy on the switch. The switches use these cisco-av-pair VSAs:

— *url-redirect* = *<HTTP or HTTPS URL>*

— *url-redirect-acl* = *switch ACL name*

These AV pairs enable the switch to intercept an HyperText Transfer Protocol (HTTP) or Secure HyperText Transfer Protocol (HTTPS) request from the endpoint device and forward the client web browser to the specified redirect address from which the latest antivirus files can be downloaded. The url-redirect AV pair on the ACS contains the URL to which the web browser will be redirected. The url-redirect-acl AV pair contains the name of an ACL which specifies the HTTP or HTTPS traffic to be redirected. The ACL must be defined on the switch. Traffic which matches a permit entry in the redirect ACL will be redirected.

These AV pairs might be sent if the host's posture is not healthy.

For more information about AV pairs that Cisco IOS software supports, see the documentation about the software releases that run on the AAA clients.

Default ACLs

If you configure NAC Layer 2 IP validation on a switch port, you must also configure a default port ACL on a switch port. You should also apply the default ACL to IP traffic for hosts that have not completed posture validation.

If you configure the default ACL on the switch and the ACS sends a host access policy to the switch, the switch applies the policy to traffic from the host that is connected to a switch port. If the policy applies to the traffic, the switch forwards the traffic. If the policy does not apply, the switch applies the default ACL. However, if the switch gets a host access policy from the ACS, but the default ACL is not configured, the NAC Layer 2 IP configuration does not take effect.

When ACS sends the switch a downloadable ACL that specifies a redirect URL as a policy-map action, this ACL takes precedence over the default ACL that is already configured on the switch port. The default ACL also takes precedence over the policy that is already configured on the host. If the default port ACL is not configured on the switch, the switch can still apply the downloadable ACL from ACS.

You use this template for access requests from Layer 2 devices that do not have the 802.1x client installed. The Authentication Bypass (802.1x fallback) template is used for access requests to bypass the nonclient authentication process. Users are mapped to a User Group based on their identity.

**Note**

Do not use the Populate from Global button; otherwise, this authentication field will be inherited from the settings in the Global Authentication Setup in System Configuration.

Table 14-5 describes the content of the Profile in the NAC Layer 2 IP Sample Profile Template.

Table 14-5 NAC Layer 2 IP Profile Sample

Section	Property		Value		
NAP	Name		User configurable		
	Description		User configurable		
Profile	NAF		N/A		
	Protocol		N/A		
	Advance filter		([[26/9/1]Cisco av-pair]aaa:service = ip_admission) AND ([006]Service-Type != 10)		
Authentication	PEAP		Allow Posture Only is checked		
	Credential Validation Database		N/A		
Posture Validation	Posture Validation Rule	Name	NAC-EXAMPLE-POSTURE-EXAMPLE		
		Required credential types	Cisco:PA		
		Selected internal posture policies	NAC-SAMPLE-CTA-POLICY		
		Selected external posture policies	N/A		
		System Posture Token configuration	System Posture Token	PA message	URL Redirect
			Healthy	Healthy	N/A
			Checkup	Checkup	N/A
			Transition	Transition	N/A
			Quarantine	Quarantine	N/A
			Infected	Infected	N/A
			Unknown	Unknown	N/A

Table 14-6 describes the content of the Authorization Rules in the NAC Layer 2 IP Sample Profile Template.

Table 14-6 Authorization Rules for NAC Layer 2 IP Profile Template

Authorization Rules	User-Group	System Posture Token	RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC-SAMPLE-HEALTHY-ACL
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC-SAMPLE-QUARANTINE-ACL

Table 14-6 Authorization Rules for NAC Layer 2 IP Profile Template (continued)

Authorization Rules	User-Group	System Posture Token	RAC	DACL
Default			NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

[Table 14-7](#) describes the content of the posture-validation policies in the NAC Layer 2 IP Sample Profile Template.

Table 14-7 Posture Validation for NAC Layer 2 IP Sample

Section	Object		Value		
Internal posture policy	NAC-SAMPLE-POSTURE-RULE		Condition	System Posture Token	Notification String
		Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0	Cisco:PA:Healthy	N/A
		Default	N/A	Cisco:PA:Quarantine	N/A

NAC Layer 2 802.1x

Before you use this template, ensure that you have checked the following options in the Global Authentication Setup page:

- EAP-FAST
- EAP-FAST Authenticated in-band PAC Provisioning
- EAP-FAST MS-CHAPv2
- EAP-FAST GTC

[Table 14-8](#) describes the content of the NAC L2 802.1x Sample Profile Template.

Table 14-8 NAC L2 802.1x Profile Sample

Section	Property	Value
NAP	Name	User configured
	Description	User configured
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	([006]Service-Type != 10) and (not exist [26/9/1]cisco-av-pair aaa:service)

Table 14-8 NAC L2 802.1x Profile Sample (continued)

Section	Property	Value		
Authentication	EAP-FAST	Allow EAP-FAST is checked. Allow authenticated in-band PAC provisioning is checked. Allow inner methods EAP-GTC is checked. Allow inner methods EAP-MS-CHAPv2 is checked. Allow Stateless Session Resume is checked. Accept client on authenticated provisioning is checked. Posture Validation required is checked.		
	Credential Validation Database	ACS Internal user database		
Posture Validation				
Posture validation Rule	Name	NAC-SAMPLE-POSTURE-RULE		
	Required credential types	Cisco:PA		
	Selected internal posture policies	NAC-SAMPLE-CTA-POLICY		
	Selected external posture policies	N/A		
	System Posture Token configuration	System Posture Token	PA message	URL
		Healthy	Healthy	N/A
		Checkup	Checkup	N/A
		Transition	Transition	N/A
		Quarantine	Quarantine	N/A
		Infected	Infected	N/A
	Unknown	Unknown	N/A	

[Table 14-9](#) describes the content of the Authorization Rules in the NAC Layer 802.1x Sample Profile Template.

Table 14-9 Authorization Rules for NAC Layer 2 801.x Profile Sample

Authorization Rules	User group	System Posture Token	RAC	DACL
Rule 1	N/A	Healthy	NAC-SAMPLE-HEALTHY-L2-RAC	N/A
Rule 2	N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L2-RAC	N/A
Default			NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL

Table 14-9 Authorization Rules for NAC Layer 2 801.x Profile Sample (continued)

Authorization Rules	User group	System Posture Token	RAC	DACL
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

[Table 14-10](#) describes the content of the posture-validation policies in the NAC Layer 802.1x Sample Profile Template.

Table 14-10 Posture Validation for NAC Layer 2 802.1x Profile Sample

Section	Object	Value			
Internal posture policy	NAC-SAMPLE-CTA-POLICY		Condition	System Posture Token	Notification String
		Rule 1	Cisco:PA:PA-Name contains CTA and Cisco:PA:PA-Version >=1.0	Cisco:PA:Healthy	N/A
		Default	N/A	Cisco:PA:Quarantine	N/A

[Table 14-11](#) describes the content of the Shared Profile Components in the NAC Layer 802.1x Sample Profile Template.

Table 14-11 Shared Profile Components for NAC Layer 2 802.1x Profile Template

Type	Object	Value
RADIUS Authorization Components	NAC-SAMPLE-HEALTHY-L2-RAC	<pre>[027] Session-Timeout = 36,000 [26/9/1] cisco-av-pair sec:pg=healthy_hosts [029] Termination-Action RADIUS-Request (1) [064] Tunnel-Type [T1] VLAN (13) [065] Tunnel-Medium-Type [T1] 802 (6) [081] Tunnel-Private-Group-ID = healthy</pre>
	NAC-SAMPLE-QUARANTINE-L2-RAC	<pre>[027] Session-Timeout = 3,600 [26/9/1] cisco-av-pair sec:pg=quarantine_hosts [029] Termination-Action RADIUS-Request (1) [064] Tunnel-Type [T1] VLAN (13) [065] Tunnel-Medium-Type [T1] 802 (6) [081] Tunnel-Private-Group-ID = quarantine</pre>

Microsoft IEEE 802.1x

Before you use this template, ensure that you have checked the Allow EAP-MS-CHAPv2 option in the Global Authentication Setup page.

[Table 14-12](#) describes the Profile Sample in the Microsoft IEEE 802.1x Sample Profile Template.

Table 14-12 *Microsoft IEEE 802.1x Profile Sample*

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	(([006]Service-Type != 10) and (not exist [26/9/1]cisco-av-pair aaa:service))
Authentication	PEAP	Allow EAP MS-CHAPv2 is checked
	Credential Validation Database	ACS Internal Users Database
Posture Validation	N/A	

[Table 14-13](#) describes the Authorization Rules in the Microsoft IEEE 802.1x Sample Profile Template.

Table 14-13 *Authorization Rules for Microsoft IEEE 802.1x Profile Sample*

Authorization Rules	User Group	System Posture Token	RAC	DACL
Default	Deny = unchecked			
Include RADIUS attributes from user's group	Checked			
Include RADIUS attributes from user record	Checked			

Wireless (NAC L2 802.1x)

The templates for wireless (NAC L2 802.1x) are the same as the NAC L2 802.1x templates. See [NAC Layer 2 802.1x, page 14-14](#) for more information.

Agentless Host for L2 (802.1x Fallback)

You can use the Agentless Host for L2 (802.1x Fallback) profile template to create a profile that matches a RADIUS request that will come from a switch. Once the profile is created an analysis of the RADIUS packet that comes from the Catalyst 6500 must be done to create an accurate match for the profile. The RADIUS request from the switch has a Service Type value of 10, just like NAC-L2-IP; but does not have a Cisco Attribute Value Pair (AVP) that contains the keywords service. Therefore, two entries are created in the Advanced Filtering box.

[Table 14-14](#) describes the content of the Profile Sample in the Agentless Host for L2 (802.1x Fallback) Sample Profile Template.

Table 14-14 Agentless Host for L2 (802.1x Fallback) Sample Profile

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable
Profile	NAF	N/A
	Protocol	N/A
	Advance filter	(not exist [26/9/1]cisco-av-pair aaa:service) AND ([006]Service-Type = 10)
	Credential Validation Database	N/A
Authentication	Protocols	Allow Agentless Request Processing will be checked Default user-group will be set to default group
Posture Validation	N/A	

[Table 14-15](#) describes the content of the Authorization Rules in the Authentication Bypass Sample Profile Template.

Table 14-15 Authorization Rules for Agentless Host for L2 (802.1x Fallback) Sample Profile

Authorization Rules	User Group	System Posture Token	RAC	DACL
Rule 1	Default-group	N/A	NAC-SAMPLE-QUARANTINE-L2-RAC	N/A
Default	Deny = checked			
Include RADIUS attributes from user's group	Unchecked			
Include RADIUS attributes from user record	Unchecked			

Agentless Host for L3

This template is used for access requests for NAC Agentless Hosts (NAH), also known as agentless hosts. These requests use EAP over UDP (EoU).

[Table 14-16](#) describes the Profile Sample in the Agentless Host for L3 Sample Profile Template.

Table 14-16 Agentless Host for L3 Sample Profile Template

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable

Table 14-16 Agentless Host for L3 Sample Profile Template (continued)

Section	Property	Value			
Profile	NAF	N/A			
	Protocol	N/A			
	Advance filter	([[26/9/1]Cisco av-pair]aaa:service = ip_admission) AND ([006]Service-Type = 10)			
	Credential Validation Database	N/A			
Posture Validation	N/A				
Authorization	Rules	User-group	System Posture Token	RAC	DACL
		N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC_SAMPLE_HEALTHY_ACL
		N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
		N/A	Transition	NAC-SAMPLE-TRANSITION-L3-RAC	NAC_SAMPLE_TRANSITION_ACL
	Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
	Include RADIUS attributes from user's group	Unchecked			
	Include RADIUS attributes from user record	Unchecked			

[Table 14-17](#) describes the Shared Profile Components in the Agentless Host for L3 Sample Profile Template.

Table 14-17 Shared Profile Components for Agentless Host for L3 Sample

Type	Object	Value		
RADIUS Authorization Components	NAC-SAMPLE-TRANSITION-L3-RAC	[027] Session-Timeout = 60 [029] Termination-Action RADIUS-Request (1) A Session-Timeout can be overwritten if hinted by an audit server		
	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [029] Termination-Action RADIUS-Request (1)		
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [029] Termination-Action RADIUS-Request (1)		
Downloadable IP ACLs		ACL Content Name	Content	NAF
	NAC-_SAMPLE-_TRANSITION-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_HEALTHY-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_QUARANTINE-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)

Agentless Host for L2 and L3

This template is used for access requests from agentless hosts connected to an L2 Network Access Device (NAD). ACS first admits the device to a quarantine network where it can receive an IP address. Audit begins when the device has received an IP address. At this point, the audit is the same as an audit for an L3 host. The NAD must be configured to learn the host's IP address ahead of time. ACS responds to an initial Access-Request with a notification to the device to issue another request when it learns the IP address. If the NAD does not learn the host's IP address, ACS invokes a failure condition and policy flow falls over to Audit Fail-Open policy. The administrator can then choose to reject the user, or assign a posture token and an optional user group.

[Table 14-18](#) describes the Profile Sample in the Agentless Host for L2 and L3 Sample Profile Template.

Table 14-18 Agentless Host for L2 and L3 Sample Profile Template

Section	Property	Value
NAP	Name	User configurable
	Description	User configurable

Table 14-18 Agentless Host for L2 and L3 Sample Profile Template (continued)

Section	Property	Value			
Profile	NAF	N/A			
	Protocol	N/A			
	Advance filter	([006]Service-Type = 10) AND (not exist [26/9/1]cisco-av-pair aaa:service) AND (audit-session-id=^)			
	Credential Validation Database	N/A			
Posture Validation	N/A				
Authorization	Rules	User-group	System Posture Token	RAC	DACL
		N/A	Healthy	NAC-SAMPLE-HEALTHY-L3-RAC	NAC_SAMPLE_HEALTHY_ACL
		N/A	Quarantine	NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
		N/A	Transition	NAC-SAMPLE-TRANSITION-L3-RAC	NAC_SAMPLE_TRANSITION_ACL
	Default	Deny = unchecked		NAC-SAMPLE-QUARANTINE-L3-RAC	NAC_SAMPLE_QUARANTINE_ACL
	Include RADIUS attributes from user's group	Unchecked			
	Include RADIUS attributes from user record	Unchecked			

Table 14-19 describes the Shared Profile Components in the Agentless Host for L2 and L3 Sample Profile Template.

Table 14-19 Shared Profile Components for Agentless Host for L3 and L3 Sample

Type	Object	Value		
RADIUS Authorization Components	NAC-SAMPLE-TRANSITION-L3-RAC	[027] Session-Timeout = 60 [029] Termination-Action RADIUS-Request (1) A Session-Timeout can be overwritten if hinted by an audit server		
	NAC-SAMPLE-HEALTHY-L3-RAC	[027]Session-Timeout = 36,000 [029] Termination-Action RADIUS-Request (1)		
	NAC-SAMPLE-QUARANTINE-L3-RAC	[027]Session-Timeout = 3,600 [029] Termination-Action RADIUS-Request (1)		
Downloadable IP ACLs		ACL Content Name	Content	NAF
	NAC-_SAMPLE-_TRANSITION-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_HEALTHY-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)
	NAC-_SAMPLE-_QUARANTINE-_ACL	L3-EXAMPLE	permit ip any any	(All-AAA-Clients)

Configuring Policies for Profiles

After you set up a profile, you associate a set of rules or policies with it, to reflect your organization's security policies. You can configure policies for:

- **Protocols** — Define the password protocols and EAP configuration.
- **Authentication**—A set of configuration policies that are related to authentication mechanisms.
- **Posture validation**—Define the manner in which posture validation will be performed (only if you plan to deploy NAC in your network).
- **Authorization**—Configure a set of authorization rules (optional).

ACS associates attributes according to the profile that was requested. The attributes that are returned in an `Access-Accept` message are a consolidation of attributes that are associated with a profile (such as `Tunnel-Type` for a VPN profile request) and session-specific attributes that are bound to the end-user (such as `Idle-Timeout` for example). The profile mapping is independent of the user identity; therefore, each user can use multiple profiles, and has only one entry in the validating database.

These topics describe how to configure and manage policies for NAPs:

- [Protocol Configuration for NAPs, page 14-23](#)
- [Authentication Policy Configuration for NAPs, page 14-27](#)
- [Posture-Validation Policy Configuration for NAPs, page 14-29](#)
- [Authorization Policy Configuration for NAPs, page 14-34](#)

Protocol Configuration for NAPs

These topics describe how to configure authentication protocols for NAPs:

- [Authentication Protocols, page 14-23](#)
- [Agentless Request Processing, page 14-24](#)
- [EAP Configuration for NAPs, page 14-25](#)
- [EAP-FAST with Posture Validation, page 14-25](#)
- [EAP Authentication with RADIUS Key Wrap, page 14-25](#)
- [Configuring Protocols, page 14-26](#)

Authentication Protocols

You can configure all relevant parameters for authentication protocols for your NAPs. These parameters are applied during access request processing.

Populating Protocol Setting with ACS Global Settings

You can populate the protocol settings with the ACS global settings, and then customize them. This method facilitates configuring the protocol settings each time you set up a new profile.

Global Authentication Setup serves as a central location for all of the EAP configuration settings in the active or inactive profiles. You cannot enable EAP types in an ACS profile, which are disabled in the Global Authentication Page. Every EAP type that is unchecked in the Global Authentication Page will automatically be unchecked in all ACS (active and inactive) profiles. Options that are not available in the Global Authentication Setup page, are unchecked in the Protocol Settings page after populating from the Global Authentication Setup page.

To apply global settings: Click **Populate from Global** to apply authentication settings that were set in the **System Configuration > Global Authentication Setup** window. For more information, see [Configuring Authentication Options, page 9-21](#).

We recommend that you check all authentication protocols in the Global Authentication Setup for NAC.

The following authentication protocols, listed from weakest to most secure, can be configured:

- RADIUS Authentication protocols allow or disallow authentication by using:
 - Password Authentication Protocol (PAP) protocol.
 - CHAP password protocol.
 - MS-CHAPv1 password protocol.
 - MS-CHAPv2 password protocol.
 - Agentless Request Processing. For more information, see [Agentless Request Processing, page 14-24](#).
 - An option to allow or disallow a set of EAP types (outer and inner) to be used for EAP authentication, including the relevant setting for each EAP-type. See [EAP Configuration for NAPs, page 14-25](#), for more information.
- You can configure the following EAP protocols:
 - PEAP
 - EAP-FAST

- EAP-Transport Layer Security (TLS) with or without RADIUS Key Wrap. See [EAP Authentication with RADIUS Key Wrap, page 14-25](#), for more information.
- EAP-Message Digest 5 (MD5)

The protocols that you select determine the flexibility of negotiation. The final result is to determine which protocol to use to authenticate. For more information about protocols, see [About Certification and EAP Protocols, page 9-1](#).

**Note**

LEAP (EAP-Cisco Wireless) is not supported when working with Network Access Profiles.

Agentless Request Processing

Agentless Request Processing, is an identity-based network security feature that is configured on a port basis. A switch makes a RADIUS request to ACS with the MAC (Media Access Control) address of the endhost connecting to the switch. Agentless authentication happens on the switch or device as a fallback that results from a 802.1x failure or an EAPoUDP failure, and hence bypasses these mechanisms. This feature is useful for allowing network access for hosts without 802.1x or EAPoUDP support. For example, devices such as printers or terminals that do not have an 802.1x client can use this feature to access to the network.

You can use this feature to map MAC addresses to user groups. You can use a configured LDAP server or the internal ACS Database to authenticate MAC address user requests. ACS uses the LDAP server to look up MAC addresses and to retrieve LDAP group attributes for MAC addresses. If the MAC addresses exist in the LDAP Server, ACS maps the LDAP Group to the ACS Groups configured in the configured ACS External LDAP Database. ACS accepts any of the MAC address standard formats. If the list of defined addresses does not contain a MAC address, you can associate a fallback user group with the access request. Groups can be included in the profile's authorization policy and then be evaluated for network admission based on authorization rules.

For information about configuring the LDAP external database for agentless requests see *Configuration Guide for Cisco Secure ACS Release 4.2*.

The MAC address is sent in the Calling-Station-ID RADIUS attribute. ACS identifies an Agentless Request in this manner:

Service-Type = 10 (Call Check)

If the **Allow Agentless Request Processing** option is not enabled, MAC address authentication is not applied and the access request is rejected.

ACS supports the following three standard formats for representing MAC-48 addresses in human-readable form:

- Six groups of two hexadecimal digits, separated by hyphens (-) in transmission order, for example, *01-23-45-67-89-ab*.
- Six groups of two separated by colons (:), for example, *01:23:45:67:89:ab*.
- Three groups of four hexadecimal digits separated by dots (.), for example, *0123.4567.89ab*.

An Error alert appears for invalid MAC addresses. MAC addresses are presented in one format regardless of the format in which they were entered into ACS.

To process agentless requests, **Allow Agentless Request Processing** must be enabled in the [Protocols Settings for profile_name Page, page 14-43](#). You must also define settings in the [Authentication for profile_name Page, page 14-46](#). You choose which configured database to use to authenticate a MAC address user request, and define the default mapping for MAC addresses that do not match.

EAP Configuration for NAPs

EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x, or RADIUS and supports multiple authentication types:

- PEAP (Protected EAP)
- EAP-FAST
- EAP-TLS (based on X.509 certificates)
- EAP-MD5: Plain Password Hash (CHAP over EAP)
- EAP-GTC: OTP Tokens



Note

You can enable RADIUS Key Wrap attributes for PEAP, EAP-FAST and EAP-TLS authentication.

The following extended EAP methods are available for NAC:

- EAP-TLV: Carry posture credentials, adding posture AVPs, posture notifications.
- Status Query: You can use this new EAP method for securely querying the status of a peer without a full credential validation.
- EAPoUDP: use of EAP over UDP for Layer 3 transport.

EAP-FAST with Posture Validation

Several organizations might be in the process of supplying their hosts with the Cisco Trust Agent and some hosts might or might not have the Cisco Trust Agent installed. Cases might arise where you might want to enforce posture validation on machines with the Cisco Trust Agent; however, you do not want to fail authentication on those machines that are temporarily without the Cisco Trust Agent. When EAP-FAST is enabled with Required Posture Validation, you can select the Optional selection and supply a resulting SPT. You can use the SPT that is set here for setting Authorization settings. For a description of the tokens that are used in ACS, see [Posture Tokens, page 13-3](#).



Note

If posture-validation rules are not defined, the posture token returned is **Unknown**.

EAP Authentication with RADIUS Key Wrap

You can configure ACS to use PEAP, EAP-FAST and EAP-TLS authentication with RADIUS Key Wrap. ACS can then authenticate RADIUS messages and distribute the session key to the network access server (NAS). The EAP session key is encrypted by using Advanced Encryption Standard (AES), and the RADIUS message is authenticated by using HMAC-SHA-1.

Because RADIUS is used to transport EAP messages (in the EAP-Message attribute), securely authenticating RADIUS messages ensures securely authenticated EAP message exchanges. You can use RADIUS Key Wrap when PEAP, EAP-FAST and EAP-TLS authentication is enabled as an external authentication method. Key Wrap is not supported for EAP-TLS as an inner method (for example, for EAP-FAST or PEAP).

RADIUS Key Wrap support in ACS uses three new AVPs for the cisco-av-pair RADIUS Vendor-Specific-Attribute (VSA); the TLV value of Cisco VSA is [26/9/1]:

- **Random-Nonce**—Generated by the NAS, it adds randomness to the key data encryption and authentication, and links requests and response packets to prevent replay attacks.
- **Key**—Used for session key distribution.
- **Message-Authenticator-Code**—Ensures the authenticity of the RADIUS message, including the EAP-Message and Key attributes.

When using RADIUS Key Wrap, ACS enforces the use of these three RADIUS Key Wrap AVPs for message exchanges and key delivery. ACS will reject all RADIUS (EAP) requests that contain RADIUS Key Wrap AVPs and the standard RADIUS Message-Authenticator attribute.

To use RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications, you must enable the EAP authentication with RADIUS Key Wrap in the Protocol Settings page for the NAP. You must also define two shared secret keys for each AAA Client, or for an NDG. Each key must be unique, and must also be distinct from the RADIUS shared key. RADIUS Key Wrap does not support proxy functionality, and should not be used with a proxy configuration.

Configuring Protocols

To configure protocols for NAPs:

Step 1 Choose **Network Access Profiles**.

The Network Access Profiles page appears.

Step 2 Click **Protocol** for the relevant NAP.

The Protocols and EAP Configuration page appears.

Step 3 To populate the page with ACS global protocol settings, select **Populate from Global**. For more information about global protocol settings, see [Configuring Authentication Options, page 9-21](#).



Note If LEAP was configured in the Global Authentication Setup page, it will not be supported with NAPs.

Step 4 To process agentless requests, choose one of the available options in **Allow Agent Request Processing** to authenticate MAC address user requests.

Step 5 Change other settings as required. For information about options, see [Protocols Settings for profile_name Page, page 14-43](#).

Step 6 Click **Submit**.

The Network Access Profiles page reappears.

Step 7 Click **Apply and Restart** for your changes to take effect.

Authentication Policy Configuration for NAPs

Authentication settings define which databases are used to validate the credentials of the user for authentication. Before you configure authentication policies configure the External User Databases that you mapped to ACS user groups by the mapping rules that are defined in Database Group Mapping.

**Note**

The ACS internal database is the default selected database.

You can also configure Agentless Request Processing for MAC addresses as part of your authentication policy. For more information, see [Agentless Request Processing, page 14-24](#).

These topics describe how to configure authentication settings:

- [Credential Validation Databases, page 14-27](#)
- [Group Filtering at NAP Level, page 14-27](#)
- [Object Identifier Check for EAP-TLS Authentication, page 14-28](#)
- [Configuring Authentication Policies, page 14-28](#)

Credential Validation Databases

The Credential Validation Databases are databases that you use to validate users. The Available Databases are the configured External User Databases that are mapped to ACS user groups by the mapping rules defined in Databases Group Mapping. The ACS internal database appears, by default, as a selected database.

**Note**

If you specify multiple databases for authentication, ACS will query each directory server in the order specified until it receives an authoritative response. You should put the most likely directory servers higher in the list to improve response times and user experience.

Group Filtering at NAP Level

You can use ACS to perform group filtering at the NAP level. Depending on the user's external database group membership, ACS can reject or accept access to the network based on the group filtering settings.

Group filtering indicates the expected group membership in an external LDAP database. For example, if the group filter for the NAP is configured as *LDAP_GRP1*, *LDAP_GRP2*, the user must belong to any one of these groups in LDAP to authenticate successfully.

Group filtering is checked while performing group mapping during external database authentication.

**Note**

Group filtering occurs at the NAP level and cannot be used as a NAP selection criteria, since a user's external database membership is still unknown during the NAP selection processing.

**Note**

This feature is based at the NAP level only for RADIUS authentications, since NAPs are applicable only for RADIUS packet processing.

Object Identifier Check for EAP-TLS Authentication

ACS can compare the OID against the Enhanced Key Usage (EKU) field in the user's certificate. ACS denies access if the OID and EKU do not match. For more information about options, see [Authentication for profile_name Page, page 14-46](#).

When OID comparison is enabled and a valid OID string is entered, all the certificates that the users present for EAP-TLS authentication are checked against the OIDs entered. Authentication will be successful only if the OIDs match. If OID comparison is enabled but the user certificate presented does not contain any OID in the EKU field, authentication will fail.

To enable OID comparison you must:

- Enable EAP-TLS from the NAP page.
- Enter only contain numbers, dots, commas and spaces in the OID strings, for example: 1.3.6.1.5.5.7.3.2 is a valid OID string.
- Enter multiple OIDs as comma-separated values. For example: 1.3.6.1.5.5.7.3.1, 1.3.6.1.5.5.7.3.2 is a valid string.

Configuring Authentication Policies

To configure authentication policies for NAPs:

-
- Step 1 Choose **Network Access Profiles**.
 - Step 2 Click **Authentication** for the relevant policy.
The Authentication Settings page appears.
 - Step 3 Select **Populate from Global** to populate authentication settings from the ACS Global Authentication Setup page. For more information, see [Global Authentication Setup Page, page 9-41](#).
 - Step 4 Select the **Credential Validation Databases**. For information about options, see [Authentication for profile_name Page, page 14-46](#).
 - Step 5 Configure **Group Filtering**. For more information about options, see [Authentication for profile_name Page, page 14-46](#).
 - Step 6 To configure MAC authentication settings:
 - a. Choose which configured database to use to authenticate MAC address user request. You can use a configured LDAP server or the internal ACS Database to authenticate MAC address user requests.
 - b. Define the default mapping for MAC addresses that do not match by selecting a group from the drop-down list.For information about options, see [Authentication for profile_name Page, page 14-46](#).
 - Step 7 Compare the OID (optional). For information about options, see [Authentication for profile_name Page, page 14-46](#).
 - Step 8 Click **Submit**.
The Network Access Profiles page reappears.
 - Step 9 Click **Apply and Restart** for your changes to take effect.
-

Posture-Validation Policy Configuration for NAPs

These topics contain information about configuring posture-validation policies:

- [About Posture Validation Rules, page 14-29](#)
- [Setting a Posture-Validation Policy, page 14-30](#)
- [Deleting a Posture Validation Rule, page 14-31](#)
- [Configuring Posture Validation for Agentless Hosts, page 14-33](#)

About Posture Validation Rules

Posture validation rules are used to select the posture validation components. A posture validation rule is comprised of a condition and actions. The condition is a set of required credential types. The actions are to determine which internal policies or external servers should be used for posture validation. Posture validation rules return a posture token and action for a posture request. See [Chapter 13, “Posture Validation in Network Access Control,”](#) for more information.

ACS interprets a posture-validation rule as:

If posture credentials contain data that was sent from the following plug-ins <required credential types>, then perform posture validation by using the following internal, external, or both internal and external posture validation methods <list of internal policies and external servers>.

ACS applies all the policies that associated with the selected posture-validation rule to derive application posture tokens (APT), which represent the state of the client (also known as the endpoint). ACS compares all derived APTs and uses the worst case posture token as the SPT, which symbolizes the overall posture of the client.

You can also set up policies and associated rules to process SoH from external AAA servers used in these networks.

Audit servers are Cisco and third-party servers that determine posture information about a client without relying on the presence of a NAC-compliant Posture Agent (PA). These types of clients are referred to as NAC Agentless Hosts (NAH). Audit servers are used to assess posture validation with an organization's security policy. For more information, see [Setting a Posture-Validation Policy, page 14-30](#).

The Cisco PA is also known as the Cisco Trust Agent.

Each rule contains:

- Name (posture-validation policy) for identification.
- Required credential types that define the credential types that activate this rule.
- Internal policies and external servers that execute to calculate the posture token. You should configure these policies before creating Posture Validation rules. See [Configuring Policies, page 13-15](#).
- Posture Agent (PA) messages that return to the client for each SPT.
- URL redirect that is sent to the AAA client for each SPT.



Note

ACS supports up to 100 rules per policy.

The posture rules are evaluated in a first-match strategy. A posture-validation policy can have zero or more ordered posture-validation rules and is selected by using the first rule that matches.

Audit Server Functionality

The audit server scans the host and returns the token to ACS. The audit server may use asynchronous port scans, HTTP redirection, a proprietary client, and table lookups to provide posture-validation information. ACS polls for the audit result, so the audit server must hold its results until the next poll.

For more information about setting up audit servers, see [Setting Up an External Audit Posture Validation Server, page 13-25](#).

System Posture Token Configuration

A system posture token is associated with the state of the computer and a posture token is associated with the state of a NAC-compliant application.

Actions are the result of applying a policy to the credentials received in a posture-validation request. ACS determines the posture token of each request by comparing the actions from all policies applied to the request. The worst posture token becomes the system posture token.

URL Redirect Policy

The URL Redirect policy provides a mechanism to redirect all HTTP or HTTPS traffic to a remediation server that allows a noncompliant host to perform the necessary upgrade actions to become compliant. The policy comprises:

- A URL that points to the remediation server.
- An ACL on the switch that causes all HTTP or HTTPS packets from the host other than those destined to the remediation server address to be captured and redirected to the switch software for the necessary HTTP redirection.

The ACL name for the host policy, the redirect URL, and the URL redirect ACL are conveyed by using RADIUS Attribute-Value objects.

Fail Open for Errors

You can configure fail open for errors that can prevent the retrieval of posture token from an upstream NAC server. If fail open is not configured, the user request is rejected.

When fail open is configured, and an error occurs when communicating with an upstream posture-validation server, the policy results will be as if posture validation was successful. The SPT for the given policy will be a static, preconfigured value.

You can select whether to enable fail open for profiles that are associated with an:

- External Posture Validation Server— If more than one server is configured for a profile, each server that fails contributes an APT to the final SPT. The worst case token is used as the SPT, which symbolizes the overall posture of the NAC-client computer. See [Setting a Posture-Validation Policy, page 14-30](#).
- Audit Server— Configuring fail open results in the SPT being set to the statically configured posture token. See [Configuring Posture Validation for Agentless Hosts, page 14-33](#).

Setting a Posture-Validation Policy

A posture-validation policy can have one or more posture-validation rules. When ACS uses a posture-validation policy to evaluate a posture-validation request, the first match is implemented. The selected rules determine which internal and external policies will be activated for the request.

You can configure posture-validation policies that might be associated with a rule in Internal or External Posture Validation Setup, as applicable.

Before you begin:

- Ensure that you have checked the Allow Posture Validation option in Network Access Profiles > Authentication Settings page (see [Authentication for profile_name Page, page 14-46](#)).
- Ensure that you have set posture validation settings (see [Configuring NAC in ACS, page 13-13](#) for details).

To add an internal posture-validation policy, external posture-validation server, or both, to a profile:

-
- Step 1** Choose **Network Access Profiles**.
- Step 2** Choose **Posture Validation** for the selected profile.
The Posture Validation page appears.
- Step 3** Click **Add Rule**.
The Posture Validation Rule Page appears. For details of options on this page, see [Posture Validation Rule for profile_name Page, page 14-48](#).
- Step 4** Enter a Name for the rule.
- Step 5** Configure the **Required Credential Types**.
- Step 6** Choose the Internal Posture Validation Policies and External Posture Validation Servers to be activated.
- Step 7** To configure fail open for a selected external posture validation server do one:
- Check **Reject User** to deny access for fail open.
 - In the Failure Posture Assessment field, select:
 - **Credential Type**—The namespace for the APT which replaces the APT that should have been returned from the failed server.
 - **Posture Token**—The posture token to be used in the event of a failure.
- Step 8** (Optional) Use the **System Posture Token Configuration** Table to set PA Messages and URL Redirects for the System Posture Token.
- Step 9** Click **Submit**. The Posture Validation page reappears.
- Step 10** In the Posture Validation page, click **Done**.
The Network Access Profiles page reappears.
- Step 11** Select **Apply and Restart** for your changes to take effect.
- Step 12** Click **Cancel** to return to the posture-validation policy.
-

Deleting a Posture Validation Rule

To delete an internal posture-validation policy rule:

-
- Step 1** Choose **Network Access Profiles**.
- Step 2** Choose **Posture Validation** for the selected profile.
The Posture Validation page appears.
- Step 3** Click the rule name that you want to delete. The [Posture Validation Rule for profile_name Page](#) appears.
- Step 4** Click **Delete**.

A warning message appears.

Step 5 Click **OK**.

Setting a Posture-Validation Policy to Process Statements of Health

A posture-validation policy can have one or more posture-validation rules. When ACS uses a posture-validation policy to evaluate a posture-validation request, the first match is implemented. The chosen rules determine which internal and external policies will be activated for the request.

You can configure posture-validation policies that might be associated with a rule in Internal or External Posture Validation Setup, as applicable.

You can also set up a SoH posture validation rule.

Before you begin:

Ensure that you have:

- Checked the **Allow Posture Validation** option on the Authentication Settings page (see [Authentication for profile_name Page, page 14-46](#)).
- Set posture validation settings (see [Configuring NAC in ACS, page 13-13](#) for details).
- Checked the **Microsoft Network Access Protection Settings** check box on the Advanced Options page.

To add an SoH posture validation rule to a profile:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose **Posture Validation** for the selected profile.

The Posture Validation page appears.

Step 3 Click **Add Rule** under the Statement of Health Posture Validation Rules table.

The Statement of Health Posture Validation Rule page appears.

Step 4 Enter a Name for the rule.

Step 5 Configure the **Endpoint Location**.

Step 6 Choose which External Posture Validation Servers are to be activated.

Step 7 To configure ACS to reject a user if the Network Policy Server (NPS) is unable to finalize the Statement of Health for the client, check the **Reject User** check box.



Note The Reject User option works only if the NPS Server is unable to finalize the Statement of Health for the client.

Step 8 If you want to specify a token that will be used if the NPS Server is unable to finalize the Statement of Health for the client:

- Uncheck the **Reject User** check box.
- From the drop-down list in the Failure Posture Token field, choose a token type to assign.

**Note**

Even if the user is not rejected, the NPS Server validates the Statement of Health and returns an appropriate token to ACS.

ACS uses the token that you specify for the Statement of Health Posture rule *only* if the NPS Server is unable to finalize the Statement of Health for the client. Therefore, the token that you choose here is a “fail-safe” token that is used only when the NPS Server cannot process the Statement of Health, and it is not mandatory that you choose one.

- Step 9** In the URL Redirect table, for each of the System Posture Token types, enter a URL for a server to which to redirect users.
- Step 10** Click **Submit**.
The Posture Validation page reappears.
- Step 11** In the Posture Validation page, click **Done**.
The Network Access Profiles page reappears.
- Step 12** Click **Apply and Restart** for your changes to take effect.
- Step 13** Click **Cancel** to return to the posture-validation policy.

Deleting a Statement of Health Posture Validation Rule

To delete an SoH posture validation rule:

- Step 1** Choose **Network Access Profiles**.
- Step 2** Choose **Posture Validation** for the chosen profile.
The Posture Validation page appears.
- Step 3** Click the rule name that you want to delete. The Statement of Health Posture Validation Rule for profile_name page appears.
- Step 4** Click **Delete**.
A warning message appears.
- Step 5** Click **OK**.

Configuring Posture Validation for Agentless Hosts

Posture-validation rules define what the returned posture token for posture validation will be. The posture-validation table includes posture-validation rules and audit configuration settings.

Posture-validation rules contain:

- A required credential that defines the mandatory credential types that activate the rule.
- The local policies and external servers that will execute to calculate the posture token.
- PA (posture agent) Messages that will return to the client for each posture token.
- A URL redirect that will be sent to the AAA client for each posture token.

A posture-validation policy can have 0-*n* ordered posture rules.

The posture validation selected is the first that match of the mandatory credential types.

The posture token that will return is the worst assessment that returned from the selected local policies and external posture servers.

If the client is an agentless host, the selected Audit server will audit the client.

To configure a posture validation policy for a NAH:

-
- Step 1** Choose **Network Access Profiles**.
- Step 2** Choose **Posture Validation** for the selected profile.
The Posture Validation Page appears.
- Step 3** Choose **Select Audit**.
The [Select External Posture Validation Audit for profile_name Page](#) appears.
- Step 4** Choose the relevant audit server. Select **Do Not Use Audit Server** if you do not want to use an audit server for posture validation.
- Step 5** To enable fail open:
- Check the **Do Not reject when Audit failed** check box.
 - Choose the **posture token** to be used in the event of a failure.
 - Enter a value for **session-timeout** for the audit server.
 - To assign a user group, check the **Assign a User Group** check box and choose a group from the drop-down list.
- Step 6** Click **Submit**.
- Step 7** Click **Apply and Restart** for your changes to take effect.
-

Authorization Policy Configuration for NAPs

These topics provide information on configuring authorization rules:

- [About Authorization Rules, page 14-34](#)
- [Configuring an Authorization Rule, page 14-36](#)
- [Configuring a Default Authorization Rule, page 14-37](#)
- [Ordering the Authorization Rules, page 14-37](#)
- [Deleting an Authorization Rule, page 14-38](#)
- [Troubleshooting Profiles, page 14-38](#)

About Authorization Rules

Authorization policies comprise rules that are applied to a NAP. Authorization policies are used for authorizing an authenticated user. Authorization rules can be based on group membership, posture validation, or both. Authorization actions are built from RACs and ACLs.

For more information about configuring RACs, see [RADIUS Authorization Components, page 4-6](#). For more information about downloadable ACLs, see [Downloadable IP ACLs, page 4-13](#).

Credentials are used in identity and posture authorization. Each application's posture credentials are evaluated separately. Credentials are compared against the posture-validation policies.

When you configure authorization policies consider the result if:

- User authentication is assignment to a User Group.
- Posture validation is a System Posture Token.
- EAP-FAST authentication and posture validation in the same session results in assignment to a user group and a posture token.

Authorization policies are a conversion of an ACS user group and a posture token to a set of RADIUS attributes that will be sent to the device. You may deny access for a specific user group, or deny access based on a returned token.

An authorization rule can be defined as:

If the user-group = selected-user-group or the posture-assessment = selected-posture-assessment, then provision the profile with the selected-RAC or the selected DACL.

Authorization rules allow for variation of device provisioning within the NAP based on group membership and posture token. The set of possible mappings is theoretically quite high for each NAP, for each group, and for each posture. However, in practice most users will be caught by a default case; for example, normal healthy users. Exceptions might be groups that require specialized access rights (for example, administrators) or users with Infected or Quarantined postures. Therefore, when you design the authorization rules, it is useful to define the normal condition first; then the set of exception cases that require more specific mappings.

You can also use authorization rules to explicitly deny (send an access-reject) as an action.

After you have configured your authorization rules, check that the Network Access Restriction (NAR) policies for the selected user group do not override the NAP policies. Accept or reject will be applied, depending on the result of the NAR evaluation. For more information, see [Network Access Restrictions, page 4-18](#).

Shared RACs

You can use NAPs to provision the same RADIUS attribute to have different values for different users, groups and NAPs. The one-user-one-group-one-profile is now more flexible by using profile based policies. For each NAP, you can configure what policies will authenticate and authorize based on RADIUS attribute values.

For a particular group (for example, Admins) who require distinct authorization profiles for the Corporate LAN, VPN, and WLAN NAPs, you can assign them a specific set of RADIUS attributes to allow them special access. If your user is in a group named contractors, they may get the same set of attributes with different values that may specify more stringent security measures. For more information about configuring RACs for NAPs, see [Understanding RACs and NAPs, page 4-7](#)

Merging Attributes

You can use RADIUS attribute overrides for group or user attributes. When you choose these options, ACS merges RADIUS attributes, downloadable ACLs, and other attributes that are created dynamically. RADIUS attributes can be at a user record level, group level and shared RAC level.

Attribute merging is performed by a process of repeated overriding whatever is listed in priority order, highest first. The order is:

- User overrides

- Dynamic session (for example, posture token)
- Authentication protocol (for example, session timeout, wireless session keys)
- Downloadable ACL (assignment)
- Shared RACs
- Static group

When you merge between group, RAC, and user attributes, remember that attributes set at a group level are not guaranteed to make the final profile. Depending on your selections, RAC might override them.

The attributes in the assigned Shared RAC override those that are defined in a static ACS group. That attribute set is then overridden with attributes from downloadable ACL and so on. Be cautious when you use NAP authorization policies.

Configuring an Authorization Rule

Before You Begin

Define per-service provisioning components (Shared RACs and DACLS). If required for a given service, create custom RACs and DACLS for those groups of users that require specific settings.

To configure an authorization rule:

-
- Step 1** Choose **Network Access Profiles**.
 - Step 2** Choose the selected profile **Authorization** policy.
The Authorization Rule page appears.
 - Step 3** Click **Add Rule**.
A new rule row appears.
 - Step 4** Define the authorization rule conditions:
 - Choose a **User Group** from the drop-down list.
 - In a NAC network, choose the **System Posture Token**. (In a non-NAC network, leave the System Posture Token as **Any**.)

For more information about condition options, see [Authorization Rules for profile_name, page 14-50](#).
 - Step 5** Define the authorization rule actions:
You can deny access or you can choose one or both authorization actions to implement when the authorization rules match:
 - **Deny Access**—Check this option to deny access for users that have matching conditions. When you choose this option the other action options are grayed out.
 - **Shared RAC**—Choose a Shared RAC from the drop-down list.
 - **Downloadable ACL**—Choose a downloadable ACL from the drop-down list.

For more information about action options, see [Authorization Rules for profile_name, page 14-50](#).
 - Step 6** Set RADIUS attribute overrides.
The following options are enabled by default. Uncheck them if you do not want to use RADIUS attributes per user record or per user's group:
 - Include RADIUS attributes from user's group
 - Include RADIUS attributes from user record

Step 7 Click **Submit**.

Related Topics

- [RADIUS Authorization Components, page 4-6](#)
- [Downloadable IP ACLs, page 4-13](#)

Configuring a Default Authorization Rule

You can set a default authorization rule if a condition is not defined or no matched condition is found. You can deny or grant access based on Shared RACs and DACLs selections.

To configure a default authorization rule:

Step 1 Choose **Network Access Profiles**.

Step 2 Choose the selected profile **Authorization** policy.

The [Authorization Rules for profile_name](#) appears.

Step 3 Click **Add Rule**.

Step 4 Select Authentication Action for the line that contains the text **If a condition is not defined or there is no matched condition**.

Step 5 Choose Authentication Actions.

You may choose an authorization action to implement for the default rule:

- **Deny Access**—Choose this option to deny access for users that have matching conditions. You do not have to select any shared RACs or DACLs for this option.
- **Shared RAC**—Choose a Shared RAC from the drop-down list. For more information, see [Troubleshooting Profiles, page 14-38](#).
- **Downloadable ACL**—Choose a downloadable ACL from the drop-down list. See [Downloadable IP ACLs, page 4-13](#) for more information.

Step 6 Set RADIUS attribute overrides.

The following options are enabled by default. Uncheck them if you do not want to use RADIUS attributes per user record or per user's group:

- Include RADIUS attributes from user's group
- Include RADIUS attributes from user record

Step 7 Click **Submit**.

Ordering the Authorization Rules

The authorization policy first match is implemented to authorize a client request.



Note

You must place your highest priority authorization policies at the top of the list. If you select Any Group for the User Group or Any Assessment for the posture token first match, the underlying policies will not be effective because authorization accepts the first match.

When you specify the order of conditions in a policy, determine the likelihood of each condition to be true and then order the policies so that the condition most likely to be true is first and the least likely to be true is last.

To order authorization rules:

-
- Step 1** In the Authorization Rules page, click the radio button to select the authorization rule that you want to reorder.
- Step 2** Click **Up** or **Down** to set the order.
-

Deleting an Authorization Rule

To delete an authorization rule:

-
- Step 1** In the Authorization Rules page, click the radio button to select the authorization rule that you want to delete.
- Step 2** Click **Delete** to remove the selected rule.

By default, RADIUS attribute rules from user or group records are enabled.

Troubleshooting Profiles

If the profile that is sent to the device is not what you expected, the authorization policy has probably been changed to disable group or user attributes. These attributes are being merged with the RAC that the policy assigns. Other possibilities are that ACS automatically adds certain attributes as part of the authentication protocol or an external audit server might sometimes dictate a specific Session-Timeout.

Ensure that attribute merging is not selected.



Note

The Session-Timeout values for NAC deployments can have a significant impact on ACS performance. You should adjust it for the scale of your network and ACS transaction capacity.

Policy Replication and Backup

All NAP policies are entirely replicated when you select NAPs for replication. Profiles contain a collaboration of configuration settings. The profile replication components include:

- Network Access Profiles
- Posture-validation settings
- AAA clients and hosts
- External database configuration
- Global authentication configuration
- NDGs
- Dictionaries

- Shared-profile components (RAC, NAF, and downloadable ACLs)
- Additional logging attributes.

EAP-FAST uses a different mechanism for replication and, therefore, should also be checked.

**Note**

Replication of profiles contradicts with replication of Network Configuration Device tables, therefore do not check both of these components at the same time. Replication in ACS only works between the same versions of ACS. Replication does not include external databases and all other global ACS configuration parameters.

For more information about replication, see [ACS Internal Database Replication, page 8-1](#).

Network Access Profiles Pages Reference

These topics describe the pages in the Network Access Profile section of the ACS web interface:

- [Network Access Profiles Page, page 14-39](#)
- [Profile Setup Page, page 14-40](#)
- [Create Profile from Template Page, page 14-43](#)
- [Protocols Settings for profile_name Page, page 14-43](#)
- [Authentication for profile_name Page, page 14-46](#)
- [Posture Validation Page, page 14-48](#)
- [Posture Validation Rule for profile_name Page, page 14-48](#)
- [Authorization Rules for profile_name, page 14-50](#)
- [Select External Posture Validation Audit for profile_name Page, page 14-49](#)

Network Access Profiles Page

The Network Access Profiles page is the starting point for configuring profile-based policies.

To open this page, click **Network Access Profiles on the navigation bar**.

Table 14-20 Network Access Profiles Page

Option	Description
Name	Activates the configuration for the profile. Opens the Profile Setup Page .
Policies	Contains links to protocols, authentication, posture validation, and authorization policies. <ul style="list-style-type: none"> • Protocols—Configures the password protocols and EAP configuration. Opens the Protocols Settings for profile_name Page page. • Authentication—Controls the profile's authentication policy. Opens the Authentication for profile_name Page where you can select the database that is used to validate user credentials. • Posture Validation—Configures posture-validation policies. Opens the Deleting a Posture Validation Rule. • Authorization—Maps between a user-group and system posture token result, to a radius-profile tag and Access Control List (ACL) name. Opens the Configuring a Default Authorization Rule.
Add Profile	Opens the Profile Setup Page to configure NAPs.
Add Template Profile	Creates a profile from a selection of templates including NAC L3 IP, NAC L2 IP, and Agentless Host. Use the templates to facilitate the construction of a profile. Opens the Create Profile from Template Page .
Up and Down buttons	Changes the order of the profiles. Click the Up or Down buttons to change the sort order.
Deny access when no profile matches	When enabled, and the access request does not match any profile, authentication fails and ACS denies the access request. This is the recommended option for handling unmatched access requests.
Grant access using global configuration, when no profile matches	When enabled, and the access request does not match any profile, authentication fails and ACS grants the access request based on the default configuration. The Unknown User policy then determines packet processing. Use this option for TACACS+ with NAPs.
Apply and Restart	Restarts ACS and applies the modifications.

Related Topics

- [Managing NAPs, page 14-4](#)
- [Using Profile Templates, page 14-7](#)

Profile Setup Page

Use this page to add, edit, clone, or delete a Network Access Profile.

To open this page, choose **Network Access Profiles > Add Profile** or **highlight the profile Name**.

Table 14-21 *Profile Setup Page*

Option	Description
Name	The profile name.
Description	The profile description.
Active	Activates or deactivates the profile.
Network Access Filter	The list of available NAFs for use with this profile (Default = Any).
Protocol Types	<p>The list of client vendor types from which ACS allows access requests.</p> <ul style="list-style-type: none"> • Allow Any Protocol Type—Allows any protocol type in the Protocol type list. • Allow Selected Protocol Types—Use only the protocol type(s) in the Selected list. The arrows to move the Protocol Types between lists.
Advanced Filtering	
Attribute	<p>A list of all RADIUS attributes. A number uniquely identifies each RADIUS attribute; for example, 001 is the number for <code>User-Name</code>, except for vendor-specific attributes. Vendor Specific Attributes (VSAs) use the number 026 as an identifier. The format is:</p> <p><i>Cisco AV-pair 026 / <vendor type> / <vendor attribute></i></p> <p>For example, 026/009/001 is a Cisco AV-pair attribute.</p> <p>Note ACS supports Cisco IOS RADIUS AV pairs. Before you select an AV pair, confirm that your AAA client supports it. The condition always fails for an AV pair that the AAA client does not support.</p>

Table 14-21 Profile Setup Page (continued)

Option	Description
Operator	<p>The list of operators appropriate to each attribute. Defines the comparison method by which ACS evaluates whether the rule element is true.</p> <ul style="list-style-type: none"> • = (equal to)—The rule element is true if the value in the attribute is exactly equal to the value that you specify. • != (not equal to)—The rule element is true if the value in the attribute does not equal the value that you specify. • > (greater than)—The rule element is true if the value in the attribute is greater than the value that you specify. • < (less than)—The rule element is true if the value in the attribute is less than the value that you specify. • <= (less than or equal to)—The rule element is true if the value in the attribute is less than or equal to the value that you specify. • >= (greater than or equal to)—The rule element is true if the value in the attribute is greater than or equal to the value that you specify. • contains—The rule element is true if the attribute contains a string and if any part of that string matches the string that you specify. • starts with—The rule element is true if the attribute contains a string and if the beginning of that string matches the string that you specify. • regular expression—The rule element is true if the attribute contains a string that matches the regular expression that you specify. ACS supports the following regular expression operators: <ul style="list-style-type: none"> – ^ (caret)—The ^ operator matches the start of a string. – \$ (dollar)—The \$ operator matches the end of a string. <p>Note Operators contains, start with, and regular expression only apply to string-type attribute values.</p>
Value	A value appropriate to the attribute.
cisco-av-pair	For the {026/009/001} cisco-av-pair attribute, the operator and values for the av-pair-key and av-pair-value.
Submit	Submits modifications. Returns to the Profile Setup Page .
Clone	Creates a copy of the NAP.
Delete	Deletes a profile, after warning.
Cancel	Returns to the Profile Setup Page without implementing changes.

Related Topics

- [Network Access Filters, page 4-2.](#)
- [Managing NAPs, page 14-4](#)
- [Cloning a Profile, page 14-6](#)

Create Profile from Template Page

Use this page to create a new profile from a template.

To open this page, choose **Network Access Profiles > Add Profile from Template**.

Table 14-22 Create Profile from Template Page

Option	Description
Name	A name for the profile.
Description	A description for the profile.
Template	The list of available templates. Note The NAC L3 IP template requires the Allow Posture Validation setting on the Protocols Settings for profile_name Page .
Active	Activates or deactivates the profile.
Submit	Submits modifications. Returns to the Profile Setup Page .
Cancel	Returns to the Profile Setup Page without implementing changes.

Related Topics

[Using Profile Templates, page 14-7](#)

Protocols Settings for *profile_name* Page

Use this page to set password protocols and EAP configuration.

To open this page, choose **Network Access Profiles > Protocols** (appears for each profile).

Table 14-23 Protocols and EAP Configuration Page

Option	Description
Populate from Global	Populates the Protocol Settings with the ACS Global Authentication settings. This method facilitates configuration of the authentication settings for new profiles.
Authentication Protocols	
Allow PAP	Enables PAP. PAP uses clear-text passwords (that is, unencrypted passwords) and is the least secure authentication protocol.
Allow CHAP	Enables CHAP. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with the Windows user database.
Allow MS-CHAPv1	Enables MS-CHAPv1.
Allow MS-CHAPv2	Enables MS-CHAPv2.
Allow Agentless Request Processing	Enable to configure the authentication process for a profile that receives a MAC address request.
EAP Configuration	
Allow RADIUS Key Wrap	Enables RADIUS Key Wrap attributes in PEAP, EAP-FAST and EAP-TLS authentication.

Table 14-23 Protocols and EAP Configuration Page

Option	Description
PEAP	<p>The PEAP types. Check at least one box to enable authentication with PEAP. In most cases, check all boxes.</p> <p>Note PEAP is a certificate-based authentication protocol. Authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.</p> <ul style="list-style-type: none"> • Allow EAP-MSCHAPv2—Enables EAP-MS-CHAPv2 within PEAP authentication. Use for AD authentication. • Allow EAP-GTC—Enables EAP-GTC within PEAP authentication. Use for RSA Secure ID authentication. • Allow Posture validation—Enables the collection of posture data when using PEAP. This option uses EAP over UDP. Allow Posture Validation must be checked to use the NAC L3 IP Profile Template on the Create Profile from Template Page. • Allow EAP TLS—Enables EAP-TLS within PEAP authentication.
EAP FAST	
Allow EAP-FAST	Enables EAP-FAST authentication, All other EAP-FAST-related options are irrelevant if unchecked. Some of the following settings must have corresponding settings on the PC based authentication agent (the EAP-FAST client).
Use PACS	Check if you want ACS to provision authorization PACs for EAP-FAST clients. All the relevant PAC options are disabled if this option is not checked.
Allow anonymous in-band PAC provisioning	If this check box is checked, ACS establishes a secure anonymous TLS handshake with the client to provision it with a so-called PAC by using phase zero of EAP-FAST, and using EAP-MS-CHAP as the inner method.
Allow full TLS renegotiation in case of Invalid PAC	Check if you want ACS to allow a full TLS renegotiation when the client is attempting to authenticate by using an invalid PAC.
Allow anonymous in-band PAC provisioning	Check if you want ACS to establish a secure anonymous TLS handshake with the client, to provision it with a so-called PAC, by using phase zero of EAP-FAST, and by using EAP-MSCHAP as the inner method.
Enable anonymous TLS renegotiation	This option allows an anonymous TLS handshake between the end-user client and ACS. EAP-MS-CHAP will be used as the only inner method in phase zero.
Allow authenticated in-band PAC provisioning	<p>ACS uses secure sockets 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 are installed on ACS.</p> <ul style="list-style-type: none"> • Accept client on authenticated provisioning—Enable to slightly shorten the protocol. • Require client certificate for provisioning—Enable if the clients are configured with public key infrastructure (PKI) certificates.

Table 14-23 Protocols and EAP Configuration Page

Option	Description
Allow Stateless session resume	<p>When enabled, ACS provisions authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled).</p> <ul style="list-style-type: none"> • Authorization PAC TTL <number> <timeframe>—Determines the expiration time of the user authorization PAC. When ACS receives an expired authorization PAC, it performs phase two EAP-FAST authentication.
When receiving client certificate, select one of the following lookup methods	<p>Certificate SAN Lookup—Choose to lookup the certificate based on the Subject Alternative Name field in the client certificate.</p> <p>Certificate CN Lookup—Choose to look up the certificate base on the Common Name field in the client certificate.</p>
Do not use PACs	<p>When enabled, determines whether ACS runs EAP-FAST but does not issue or accept any tunnel or machine PACs. All requests for PACs are ignored and ACS responds with a Success-TLV without a PAC. All the relevant PAC options are disabled if this option is not checked.</p> <ul style="list-style-type: none"> • Requires Client Certificate—Select to support EAP-FAST tunnel establishment with a client certificate. • Disable Client Certificate Lookup and Comparisons —Select to disable the client certificate lookup and whether the clients are configured with public key infrastructure (PKI) certificates. When this option is enabled, EAP-FAST PKI Authorization Bypass is invoked. Authorization is generally performed by retrieving the user's group data and certificate from an external database. ACS then compares at least one of the certificate, CN, or SAN to the values received from the client supplied certificate. If the comparison succeeds the group is mapped to an ACS user-group, otherwise the authentication fails. When PKI Authorization Bypass is enabled this stage is passed over and the session is mapped to a pre-configured user-group. See PAC Free EAP-FAST, page 9-16 for more information. • Assign Group — Select a group to map these requests to an ACS user-group.
Allowed inner methods	<p>When enabled, determines which inner EAP methods run inside the EAP-FAST tunnel. For anonymous in-band provisioning, EAP-GTC and EAP-MS-CHAPv2 must be enabled for backward compatibility. In most cases, all the inner methods should be checked.</p> <p>Note ACS always starts the authentication process by using the first enabled EAP method. For example, if you select EAP-GTC and EAP-MS-CHAPv2, then the first enabled EAP method is EAP-GTC.</p> <ul style="list-style-type: none"> • EAP-GTC—Uses a two-factor authentication; for example, OTP. • EAP-MSCHAPv2—Used for AD authentication. • EAP-TLS—Uses certificates for authentication.

Table 14-23 Protocols and EAP Configuration Page

Option	Description
Posture Validation	<p>Determines the EAP-FAST posture-validation mode. Select one of the following posture-validation modes:</p> <ul style="list-style-type: none"> • None—Authentication is performed; however, no posture-validation data is requested from the client and no SPT is returned. • Required—Authentication and posture validation are performed in the same authentication session. As a result, an SPT is returned. If this option is selected and posture credentials that are requested from the client are not received, authentication fails. If you are implementing NAC, this option should be enabled. • Optional—Client may not supply posture data. Sets a default SPT when a client cannot supply posture data to ACS. • Use Token—Select an SPT from the drop-down list to use as the default posture token. • Posture Only—Perform posture validation without running authentication inner methods within the authentication session. This option returns an SPT for posture validation.
EAP-TLS	<p>Enables EAP-TLS authentication.</p> <p>EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.</p> <ul style="list-style-type: none"> • Allow EAP-TLS—Check to enable EAP-TLS authentication.
EAP-MD5	Enables EAP-based Message Digest 5 hashed authentication.

Related Topics

[Protocol Configuration for NAPs, page 14-23](#)

Authentication for *profile_name* Page

Use this page to specify the databases that the profile uses for authentication rules, and to set up the Agentless Request Processing for MAC addresses configuration.

To display this page, choose **Network Access Profiles > Authentication** (appears for each profile).

Table 14-24 Authentication Settings Page

Option	Description
Credential Validation Databases	<p>The lists of Available Databases and Selected Databases that can validate users. The lists of databases include the ACS Internal Database and all databases configured in External User Databases > Unknown User Policy. If the Unknown User Policy configures a database to fail, the database cannot become a validation database and fails with an error message.</p>
Populate from Global	<p>Populates the Authentication Settings from the System Configuration > Global Authentication Setup page. Facilitates configuration of the authentication settings.</p>

Table 14-24 Authentication Settings Page

Option	Description
Group Filtering	Use this option to configure group filtering based on groups defined in the LDAP external database.
Available Groups/Selected Groups	The list of Available Groups and Selected Groups that can validate users. The lists of groups include the groups configured in LDAP External User Databases configuration. Use the arrows to move the Available Groups into the Selected Groups list.
Authenticate MAC With	<p>ACS can authenticate MAC addresses with an LDAP server or the ACS Internal Database.</p> <p>ACS supports the following three standard formats for representing MAC-48 addresses in human-readable form:</p> <ul style="list-style-type: none"> • Six groups of two hexadecimal digits, separated by hyphens (-) in transmission order, for example, <i>01-23-45-67-89-ab</i>. • Six groups of two separated by colons (:), for example, <i>01:23:45:67:89:ab</i>. • Three groups of four hexadecimal digits separated by dots (.), for example, <i>0123.4567.89ab</i>.
LDAP Server	<p>If chosen, configures an LDAP server from the available servers on the External User Databases > External User Database Configuration page.</p> <p>ACS uses the LDAP server to look up MAC addresses and to retrieve LDAP group attributes for MAC addresses. If the MAC addresses exist in the LDAP Server, ACS maps the LDAP Group to the ACS Groups configured in the configured ACS External LDAP Database.</p>
Internal ACS Database	<p>If chosen, provides fields for MAC Addresses, each with an associated User Group.</p> <p>Each NAP can hold up to 10,000 MAC addresses in the Authentication page. Each NAP can hold up to 100 mappings (a map between list of one or more MAC addresses to a group), meaning you can have up to 100 lines of mappings from lists of MACs to user-groups. You can map up to 10,000 MAC Addresses to the same user-group in one NAP.</p>
Default Action (If Agentless request was not assigned to a user group)	If the MAC addresses were not found in the LDAP Server or the ACS Internal Database, or if the LDAP Server is not reachable, provides a group to which to assign the MAC addresses.
OID Comparison	Compare Object ID with the Enhanced Key Usage (EKU) field in the user's certificate.
Enter OIDs separated by comma	OID strings can only contain numbers, dots (.), commas(,) and spaces. Multiple OIDs can be entered as comma-separated values.
Submit	Submits changes to the ACS internal database.
Cancel	Returns to the Network Access Profiles Page without submitting new changes.

Related Topics

- [Authentication Policy Configuration for NAPs, page 14-27](#)

Posture Validation Page

Use this page to order and associate Posture Validation rules.

To display this page, click **Posture Validation** in the [Network Access Profiles Page, page 14-39](#).

Table 14-25 *Posture Validation Page for profile_name Page*

Field	Description
Posture Validation Rules	
Rule Name	The name of the posture-validation rule.
Required Credential Types	The Available Credentials list displays the credential types that ACS does not require. The Selected Credentials list displays the credential types that ACS requires in a posture-validation request in order to use this posture-validation rule to evaluate the posture-validation request.
Associate With	The policies that are associated with a rule.
Up/Down	Sets the order of evaluation.
Add Rule	Opens the Posture Validation Rule for profile_name Page on which you create a new posture-validation rule.
Select Audit	Opens the Select External Posture Validation Audit for profile_name Page to configure an audit server for NAC. NAC-compliant AAA clients can handle NAC for computers that do not respond to attempts to start a posture-validation session with the Cisco Trust Agent by querying an audit server. If the Cisco Trust Agent is not installed on the computer or is unreachable for other reasons, NAC-compliant AAA clients will attempt to perform posture validation on an audit server. The result that an audit server returns is a posture token.

Related Topics

- [Chapter 13, “Posture Validation”](#)
- [Setting a Posture-Validation Policy, page 14-30](#)

Posture Validation Rule for profile_name Page

Use this page to define a Posture Validation rule.

To display this page, click **Add Rule** in the [Posture Validation Page, page 14-48](#).

Table 14-26 *Posture Validation Rule for profile_name Page*

Field	Description
Rule Name	Displays the rule name for identification.
Add Rule	Click to add a posture-validation rule. The Posture Validation Rule configuration page appears.
Edit Rule	Highlight the Rule Name. The Posture Validation Rule configuration page for the specific profile appears for editing.
Action	
Select Internal Posture Validation Policies	Select the internal posture validation policies that ACS will apply to the attributes received in the request for this rule.

Table 14-26 *Posture Validation Rule for profile_name Page*

Field	Description
Select External Posture Validation Server	Select the external posture validation server policies that ACS will apply to the attributes received in the request for this rule.
Failure Action	Check to configure the Fail Open feature.
Failure Posture Token	Select the credential type (AV pair) that is returned to the supplicant. Select the Posture Token for the credential type.
System Posture Token Configuration	Use this table to configure the SPT to return to the AAA client. There are six predefined, nonconfigurable SPTs. The SPT results are listed in order from best to worst: <ul style="list-style-type: none"> • System Posture Token—A Posture Agent Message and URL Redirect for each posture token. • System Posture Token—A message that will appear for each posture agent. • URL Redirect—The URL redirect that will be sent to the AAA client for each posture token.

Related Topics

- [Setting Up Posture Validation Policies, page 13-16](#)
- [Setting Up an External Policy Server, page 13-22](#)
- [Setting a Posture-Validation Policy, page 14-30](#)

Select External Posture Validation Audit for *profile_name* Page

Use this page to select an external posture validation audit server for posture validation.

To display this page, click **Select Audit** in the [Posture Validation Page, page 14-48](#).

Field	Description
Select	Select the external posture-validation audit server or select Do Not Use Audit Server .
Fail Open Configuration	Determines treatment of errors that might occur, thereby preventing the retrieval of a posture token from an upstream NAC server. If fail open is not configured, ACS rejects the user request.
Do not reject when Audit failed	Enables or disables fail open (default = enabled). <ul style="list-style-type: none"> • Use this token when unable to retrieve posture data—An appropriate token. • Timeout—The timeout value for the session. • Assign a User Group—The destination user group.

Related Topics

- [Setting Up an External Audit Posture Validation Server, page 13-25](#)
- [Configuring Posture Validation for Agentless Hosts, page 14-33](#)

Authorization Rules for *profile_name*

Use this page to list the set of authorization rules for a Network Access Profile.

To display this page, click **Authorization** in the [Network Access Profiles Page, page 14-39](#).

Table 14-27 *Authorization Rules for profile_name*

Field	Description
Condition	
User Group	The ACS group to which the user was mapped. This field defines the group of users for this rule. If you are not basing authorization rules on authentication, select Any .
System Posture Token	The posture token that was returned as a result of posture validation. ACS checks the token status before proceeding to follow the configured actions. You can use posture tokens to validate user groups. If you are not using posture validation, select Any .
Action	
Deny Access	Denies access for requests that do not match any configured policy.
Shared RAC	The list of RACs defined in the Shared Profile Components > RADIUS Authorization Components option. Note If you configure an external posture validation audit server to use session-timeout settings in the Authorization policy, you must select a shared RAC. See Configuring Policies, page 13-15 and External Posture Validation Audit Setup Pages, page 13-36 .
Downloadable ACL	The list of downloadable ACLs defined in Shared Profile Components > Downloadable IP ACLs.
If a condition is not defined or there is no matched condition:	A default action when a matched condition is not found.
Include RADIUS attributes from user's group	Enable to use RADIUS attributes per user's group.
Include RADIUS attributes from user record	Enable to use RADIUS attributes per user record.

Related Topics

- [Configuring an Authorization Rule, page 14-36](#)
- [Configuring a Default Authorization Rule, page 14-37](#)



CHAPTER 15

Unknown User Policy

This chapter addresses the Unknown User Policy feature, found in the External User Databases section of the ACS web interface. You can also configure the Unknown User Policy for Network Access Profiles (NAPs). In the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, the internal database against which an unknown user authenticates, must be explicitly selected from the Credential Validation Databases in the NAP configuration settings for Authentication.

After you have configured at least one database in the External User Databases section of the ACS web interface, you can decide how to implement other ACS features that are related to authentication. These features are the Unknown User Policy and user group mapping.

For information about user group mapping, see [Chapter 16, “User Group Mapping and Specification.”](#)

For information about databases supported by ACS and how to configure databases in the web interface, see [Chapter 12, “User Databases.”](#)

This chapter contains:

- [Known, Unknown, and Discovered Users, page 15-2](#)
- [Authentication and Unknown Users, page 15-3](#)
 - [About Unknown User Authentication, page 15-3](#)
 - [General Authentication of Unknown Users, page 15-3](#)
 - [Windows Authentication of Unknown Users, page 15-4](#)
 - [Performance of Unknown User Authentication, page 15-6](#)
- [Authorization of Unknown Users, page 15-6](#)
- [Unknown User Policy Options, page 15-6](#)
- [Database Search Order, page 15-7](#)
- [Configuring the Unknown User Policy, page 15-8](#)
- [Disabling Unknown User Authentication, page 15-9](#)

Known, Unknown, and Discovered Users

The Unknown User Policy feature provides different means of handling authentication requests, depending upon the type of user requesting AAA services. There are three types of users. Their significance varies depending on whether the service requested is authentication:

- **Known Users**—Users explicitly added, manually or automatically, to the ACS internal database. These are users added by an administrator using the web interface, by the RDBMS Synchronization feature or by the Database Replication feature. You can also use the **CSUtil.exe** utility (ACS for Windows). For more information about **CSUtil.exe** see [Appendix C, “CSUtil Database Utility.”](#) ACS handles authentication requests for known users with authentication:

ACS attempts to authenticate a known user with the single user database with which the user is associated with. If the user database is the ACS internal database and the user does not represent a Voice-over-IP (VoIP) user account, a password is required for the user. If the user database is an external user database or if the user represents a VoIP user account, ACS does not have to store a user password in the user database.

ACS does not support failover authentication. If authentication fails with the database that the user is associated with, ACS uses no other means to authenticate the user and ACS informs the AAA client of the authentication failure.

- **Unknown Users**—Users who do not have a user account in the ACS internal database. This means that the user has not received authentication from ACS or that the user account was deleted. Your configuration of the Unknown User Policy specifies how ACS handles authentication requests for unknown users.

For details about unknown user authentication, see [General Authentication of Unknown Users, page 15-3](#).

- **Discovered Users**—Users whose accounts ACS created in the ACS internal database after successful authentication by using the Unknown User Policy. All discovered users were unknown users. When ACS creates a discovered user, the user account contains only the username, a Password Authentication list setting that reflects the database that provided authentication for the user, and a Group to which the user is assigned list setting of Mapped By External Authenticator, which enables group mapping. Using the ACS web interface or RDBMS Synchronization, you can further configure the user account as needed. For example, after a discovered user is created in ACS, you can assign user-specific network access restrictions to the discovered user.



Note ACS does not import credentials (such as passwords, certificates) for a discovered user.

The authentication process for discovered users is identical to the authentication process for known users who are authenticated with external user databases and whose ACS group membership is determined by group mapping.



Note

We recommend removing a username from a database when the privileges that are associated with that username are no longer required. For more information about deleting a user account, see [Deleting a User Account, page 6-39](#).

The unique identifiers for a user are the username and profile name. A user is no longer identified by its username only; but by combination of username and profile name. Discovered users that are dynamically created through use of different profiles have distinguished records in the database. So, settings for user **john** with profile name **routers** will not affect settings for user *john* and profile name *switches*.

For more information on NAPs, see [Chapter 14, “Network Access Profiles.”](#)

Authentication and Unknown Users

This section provides information about using the Unknown User Policy with authentication. The information in this section is also relevant for NAP authentication policies, unless stated otherwise.

This section contains:

- [About Unknown User Authentication, page 15-3](#)
- [General Authentication of Unknown Users, page 15-3](#)
- [Windows Authentication of Unknown Users, page 15-4](#)
- [Performance of Unknown User Authentication, page 15-6](#)

About Unknown User Authentication

The Unknown User Policy is a form of authentication forwarding. In essence, this feature is an extra step in the authentication process. If a username does not exist in the ACS internal database, ACS forwards the authentication request of an incoming username and password to external databases with which it is configured to communicate. The external database must support the authentication protocol used in the authentication request.

The Unknown User Policy enables ACS to use a variety of external databases to attempt authentication of unknown users. This feature provides the foundation for a basic single sign-on capability through ACS. Because external user databases handle the incoming authentication requests, you do not have to maintain the credentials of users within ACS, such as passwords. This eliminates the necessity of entering every user multiple times and prevents data-entry errors inherent to manual procedures.



Note

When you configure NAP, the internal database might not be selected in the web interface. You can select the internal database for authentication in the same way that you select external databases.

General Authentication of Unknown Users

If you have configured the Unknown User Policy in ACS, ACS attempts to authenticate unknown users:

1. ACS checks its internal user database. If the user exists in the ACS internal database (that is, it is a known or discovered user), ACS tries to authenticate the user with the authentication protocol of the request and the database that is specified in the user account. Authentication passes or fails.
2. If the user does not exist in the ACS internal database (that is, it is an unknown user), ACS tries each external user database that supports the authentication protocol of the request, in the order that the Selected Databases list specifies. If authentication with an external user databases passes, ACS automatically adds the user to the ACS internal database, with a pointer to use the external user database that succeeded on this authentication attempt. ACS does not continue to search subsequent databases after authentication passes. Users who are added by unknown user authentication are flagged as such within the ACS internal database and are called discovered users.

The next time the discovered user tries to authenticate, ACS authenticates the user against the database that was successful the first time. Discovered users are treated the same as known users.

3. If the unknown user fails authentication with all configured external databases, the user is not added to the ACS internal database and the authentication fails.

The previous scenario is handled differently if user accounts with identical usernames exist in separate Windows domains. For more information, see [Windows Authentication of Unknown Users, page 15-4](#).



Note

Because usernames in the ACS internal database must be unique, ACS supports a single instance of any given username across all databases that it is configured to use. For example, assume every external user database contains a user account with the username John. Each account is for a different user, but they each, coincidentally, have the same username. After the first John attempts to access the network and has authenticated through the unknown user process, ACS retains a discovered user account for that John and only that John. Now, ACS tries to authenticate subsequent attempts by any user named John using the same external user database that originally authenticated John. Assuming their passwords are different than the password for the John who authenticated first, the other Johns are unable to access the network.

Windows Authentication of Unknown Users

Because the same username can recur across the trusted Windows domains against which ACS authenticates users, ACS treats authentication with a Windows user database as a special case.

To perform authentication, ACS communicates with the Windows operating system of the computer that is running ACS. Windows uses its built-in facilities to forward the authentication requests to the appropriate domain controller.

This section contains:

- [Domain-Qualified Unknown Windows Users, page 15-4](#)
- [Windows Authentication with Domain Qualification, page 15-5](#)
- [Multiple User Account Creation, page 15-5](#)

Domain-Qualified Unknown Windows Users

When a domain name is supplied as part of a authentication request, ACS detects that a domain name was supplied and tries the authentication credentials against the specified domain. The dial-up networking clients that are provided with various Windows versions differ in the method by which users can specify their domains. For more information, see [Windows Dial-Up Networking Clients, page 12-6](#).

Using a domain-qualified username allows ACS to differentiate a user from multiple instances of the same username in different domains. For unknown users who provide domain-qualified usernames and who are authenticated by a Windows user database, ACS creates their user accounts in the ACS internal database in the form *DOMAIN\username*. The combination of username and domain makes the user unique in the ACS database.

For more information about domain-qualified usernames and Windows authentication, see [Usernames and Windows Authentication, page 12-7](#).

Windows Authentication with Domain Qualification

If the username is nondomain qualified or is in UPN format, the Windows operating system of the computer that is running ACS follows a more complex authentication order, which ACS cannot control. Though the order of resources used can differ, when searching for a nondomain qualified username or UPN username, Windows usually follows this order:

1. The local domain controller.
2. The domain controllers in any trusted domains, in an order determined by Windows.
3. If ACS runs on a member server, the local accounts database.

Windows attempts to authenticate the user with the first account that it finds whose username matches the one that ACS passes to Windows. Whether authentication fails or succeeds, Windows does not search for other accounts with the same username; therefore, Windows can fail to authenticate a user who supplies valid credentials because Windows may check the supplied credentials against the wrong account that coincidentally has an identical username.

You can circumvent this difficulty by using the Domain List in the ACS configuration for the Windows user database. If you have configured the Domain List with a list of trusted domains, ACS submits the username and password to each domain in the list, using a domain-qualified format, until ACS successfully authenticates the user, or has tried each domain in the Domain List and fails the authentication.



Note

If your network has multiple occurrences of a username across domains (for example, every domain has a user called Administrator) or if users do not provide their domains as part of their authentication credentials, you must configure the Domain List for the Windows user database in the External User Databases section. If not, only the user whose account Windows happens to check first authenticates successfully. The Domain List is the only way that ACS controls the order in which Windows checks domains. The most reliable method of supporting multiple instances of a username across domains is to require users to supply their domain memberships as part of the authentication request. For more information about the effects of using the Domain List, see [Nondomain-Qualified Usernames](#), page 12-8.

Multiple User Account Creation

Unknown user authentication can create more than one user account for the same user. For example, if a user provides a domain-qualified username and successfully authenticates, ACS creates an account in the format *FFF*. If the same user successfully authenticates without prefixing the domain name to the username, ACS creates an account in the format *username*. If the same user also authenticates with a UPN version of the username, such as *username@example.com*, ACS creates a third account.

If, to assign authorizations, you rely on groups rather than individual user settings, all accounts that authenticate by using the same Windows user account should receive the same privileges. Regardless of whether the user prefixes the domain name, group mapping will assign the user to the same ACS user group, because both ACS user accounts correspond to a single Windows user account.

Performance of Unknown User Authentication

Processing authentication requests for unknown users requires slightly more time than processing authentication requests for known users. This small delay may require additional timeout configuration on the AAA clients through which unknown users may attempt to access your network.

Added Authentication Latency

Adding external user databases against which to authenticate unknown users can significantly increase the time needed for each individual authentication. At best, the time needed for each authentication is the time taken by the external user database to authenticate, plus some time for ACS processing. In some circumstances (for example, when using a Windows user database), the extra latency introduced by an external user database can be as much as tens of seconds. If you have configured the Unknown User Policy to include multiple databases in unknown user authentication, the latency for which your AAA client timeout values must account is the sum of the time taken for each external user database to respond to an authentication request of an unknown user, plus the time taken for ACS processing.

You can reduce the effect of this added latency by setting the order of databases. If you are using an authentication protocol that is particularly time sensitive, such as PEAP, we recommend configuring unknown user authentication to attempt authentication first with the database most likely to contain unknown users who use the time-sensitive protocol. For more information, see [Database Search Order, page 15-7](#).

Authentication Timeout Value on AAA clients

You must increase the AAA client timeout to accommodate the longer authentication time that is required for ACS to pass the authentication request to the external user databases that an unknown user authentication uses. If the AAA client timeout value is not set high enough to account for the delay that an unknown user authentication requires, the AAA client times out the request and every unknown user authentication fails.

In Cisco IOS, the default AAA client timeout value is five seconds. If you have ACS configured to search through several databases or your databases are slow to respond to authentication requests, consider increasing the timeout values on AAA clients. For more information about authentication timeout values in IOS, refer to your Cisco IOS documentation.

Authorization of Unknown Users

Although the Unknown User Policy allows authentication requests to be processed by databases that are configured in the External User Database section, ACS is responsible for all authorizations that are sent to AAA clients and end-user clients. Unknown user authentication works with the ACS user group mapping features to assign unknown users to user groups that you have already configured and, therefore, to assign authorization to all unknown users who pass authentication. For more information, see [Chapter 16, “User Group Mapping and Specification,”](#) and [Chapter 13, “Posture Validation.”](#)

Unknown User Policy Options

On the Configure Unknown User Policy page, you can specify what ACS does for unknown user authentication. The options for configuring the Unknown User Policy are:

- **Fail the attempt**—Disables unknown user authentication; therefore, ACS rejects authentication requests for users whom the ACS internal database does not contain. Selecting this option excludes the use of the Check the following external user databases option.
- **Check the following external user databases**—Enables unknown user authentication; therefore, ACS uses the databases in the Selected Databases list to provide unknown user authentication.



Note For authentication requests, ACS applies the Unknown User Policy to unknown users only. ACS does not support fallback to unknown user authentication when known or discovered users fail authentication.

Selecting this option excludes the use of the Fail the attempt option.

- **External Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that ACS does *not* use during unknown user authentication.
- **Selected Databases**—Of the databases that you have configured in the External User Databases section, lists the databases that ACS *does* use during unknown user authentication. ACS attempts the requested service—authentication—by using the selected databases one at a time in the order that you specified. For more information about the significance of the order of selected databases, see [Database Search Order, page 15-7](#).
- **Configure Enable Password Behavior**—Determines the initial TACACS+ Enable Password setting in the **Advanced TACACS+ Settings** section of newly created dynamic users. For more information, see [Setting TACACS+ Enable Password Options for a User, page 6-23](#).

If you check the **Internal database**, you set the TACACS+ Enable Password setting in the configuration of a dynamic user to **Use Separate Password**. Edit the TACACS+ Enable Password for the user to perform TACACS+ enable authentications.

If **The database in which the user profile is held** is selected, the TACACS+ Enable Password setting in the configuration of a new dynamic user will be set to Use External Database Password, and the database by which the user was correctly authenticated will be selected in the selection box on the user record. This configuration affects the initial setting of the new dynamic user. Once ACS has cached the user, you can override the TACACS+ Enable Password setting, and use the Configure Enable Password Behavior.

- **Configure Caching Unknown Users**—Disables the creation of dynamic users while using an external database for authentication.

For detailed steps for configuring the Unknown User Policy, see [Configuring the Unknown User Policy, page 15-8](#).

Database Search Order

You can configure the order in which ACS checks the selected databases when ACS attempts unknown authentication. The Unknown User Policy supports unknown user authentication. It will:

1. Find the next user database in the Selected Databases list that supports the authentication protocol of the request. If the list contains no user databases that support the authentication protocol of the request, stop unknown user authentication and deny network access to the user.
2. Send the authentication request to the database in Step 1.
3. If the database responds with an `Authentication succeeded` message, create the discovered user account, perform group mapping, and grant the user access to the network.

4. If the database responds with an `Authentication failed` message or does not respond and other databases are listed below the current database, return to Step 1.
5. If no additional databases appear below the current database, deny network access to the user.

When you specify the order of databases in the Selected Databases list, we recommend placing as near to the top of the list as possible databases that:

- Process the most requests.
- Process requests that are associated with particularly time-sensitive AAA clients or authentication protocols.
- Require the most restrictive mandatory credential types (applies to policy only).

As a user authentication example, if wireless LAN users access your network with PEAP, arrange the databases in the Selected Databases list so that unknown user authentication takes less than the timeout value that is specified on the Cisco Aironet Access Point.

Configuring the Unknown User Policy

Use this procedure to configure your Unknown User Policy.

For NAP policies, see [Adding a Profile, page 14-4](#).

Before You Begin

For information about the Configure the Unknown User Policy page, see [Unknown User Policy Options, page 15-6](#).

To specify how ACS processes unknown users:

-
- Step 1** In the navigation bar, click **External User Databases**, and then click **Unknown User Policy**.
 - Step 2** To deny unknown user authentication requests, select the **Fail the attempt** option.
 - Step 3** To allow unknown user authentication, enable the Unknown User Policy:
 - a. Select the **Check the following external user databases** option.
 - b. For each database that you want ACS to use for unknown user authentication, select the database in the External Databases list and click --> (right arrow button) to move it to the Selected Databases list. To remove a database from the Selected Databases list, select the database, and then click <-- (left arrow button) to move it back to the External Databases list.
 - c. To assign the database search order, select a database from the Selected Databases list, and click **Up** or **Down** to move it into the position that you want.



Note For more information about the significance of database order, see [Database Search Order, page 15-7](#).

- Step 4** To configure the enable password behavior, select **The internal database** option for each authentication or select **The database in which the user profile is held** option to allow newly created dynamic users, using the TACACS+ protocol, to have their enable password settings initialized. Clicking **The database in which the user profile is held** option permits subsequent authentications to work with the external database that cached the user.
- Step 5** Click **Submit**.

ACS saves and implements the Unknown User Policy configuration that you created. ACS processes unknown user authentication requests by using the databases in the order in the Selected Databases list.

Disabling Unknown User Authentication

You can configure ACS so that it does not provide authentication service to users who are not in the ACS internal database.

To turn off unknown user authentication:

-
- Step 1** In the navigation bar, click **External User Databases**, and then click **Unknown User Policy**.
 - Step 2** Select the **Fail the attempt** option.
 - Step 3** Click **Submit**.

Unknown user authentication is halted. ACS does not allow unknown users to authenticate with external user databases.



CHAPTER 16

User Group Mapping and Specification

This chapter provides information about group mapping and specification. The the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, uses these features to assign users who are authenticated by an external user database to a single ACS group.

This chapter contains:

- [About User Group Mapping and Specification, page 16-1](#)
- [Group Mapping by External User Database, page 16-1](#)
- [Group Mapping by Group Set Membership, page 16-3](#)
- [RADIUS-Based Group Specification, page 16-8](#)

About User Group Mapping and Specification

You can use the Database Group Mapping feature in the External User Databases section to associate unknown users with an ACS group for the purpose of assigning authorization profiles. For external user databases from which ACS can derive group information, you can associate the group memberships, which are defined for the users in the external user database, to specific ACS groups. For Windows user databases, group mapping is further specified by domain; because each domain maintains its own user database.

In addition to the Database Group Mapping feature, for some database types, ACS supports Remote Access Dial-In User Service (RADIUS)-based group specification.

Group Mapping by External User Database

You can map an external database to a ACS group. Unknown users who authenticate by using the specified database automatically belong to, and inherit the authorizations of, the group. For example, you could configure ACS so that all unknown users who authenticate with a certain token server database belong to a group called Telecommuters. You could then assign a group setup that is appropriate for users who are working away from home, such as `MaxSessions=1`. Or, you could configure restricted hours for other groups; but give unrestricted access to Telecommuters group members.

While you can configure ACS to map all unknown users in any external user database type to a single ACS group, the following external user database types are the external user database types whose users you can only map to a single ACS group:

- Open Database Connectivity (ODBC) (ACS for Windows only)

- Lightweight and Efficient Application Protocol (LEAP) Proxy RADIUS server
- Remote Access Dial-In User Service (RADIUS) token server
- RSA SecurID token server

For a subset of the external user database types that were previously listed, group mapping by external database type is overridden on a user-by-user basis when the external user database specifies an ACS group with its authentication response. ACS supports specification of group membership for the following external user database types:

- LEAP Proxy RADIUS server.
- RADIUS token server.

For more information about specifying group membership for users who are authenticated with one of these database types, see [RADIUS-Based Group Specification, page 16-8](#).

ACS for Windows

Additionally, users who are authenticated by an ODBC external user database can also be assigned to a specified ACS group. Group specification by ODBC database authentication overrides group mapping. For more information about specifying group membership for users who are authenticated with an ODBC database, see [ODBC Database \(ACS for Windows Only\), page 12-35](#).

Creating an ACS Group Mapping for a Token Server, ODBC Database, or LEAP Proxy RADIUS Server Database

To set or change a token server, ODBC database (ACS for Windows only), or LEAP Proxy RADIUS Server database group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Group Mappings**.
 - Step 3** Click the name of the token server, ODBC database configuration (ACS for Windows only), or LEAP Proxy RADIUS Server, for which you want to configure a group mapping.
The Define Group Mapping table appears.
 - Step 4** From the Select a default group for *database* list, click the group to which users who were authenticated with this database should be assigned.



Tip The Select a default group for *database* list displays the number of users who are assigned to each group.

- Step 5** Click **Submit**.
ACS assigns unknown and discovered users who are authenticated by the external database type that you selected in Step 3 to the ACS group that is selected in Step 4. For users who are authenticated by a RADIUS token server, ODBC database (ACS for Windows only), or LEAP Proxy RADIUS Server database, the mapping is only applied as a default if those databases did not specify an ACS group for the user.

**Note**

For more information about group specification for RADIUS token servers, see [RADIUS-Based Group Specification, page 16-8](#). For more information about group specification for ODBC databases (ACS for Windows), see [ACS Authentication Process with an ODBC External User Database, page 12-36](#).

Group Mapping by Group Set Membership

You can create group mappings for some external user databases based on the combination of external user database groups to which users belong. The following database types are the external user database types for which you can create group mappings based on group set membership:

- Windows domains—ACS provides two options for group mappings. You can select groups from a list of groups, or you can enter the groups manually. Use the second option when you have too many groups to enumerate (for example, 500 groups).

**Note**

ACS can only perform group mapping by using the local and global groups to which a user belongs in the domain that authenticated the user. You cannot use group membership in domains that the authenticated domain trusts that is for ACS group mapping. You cannot remove this restriction by adding a remote group to a group that is local to the domain providing the authentication.

- Generic Lightweight Directory Access Protocol (LDAP).

When you configure an ACS group mapping based on group set membership, you can add one or many external user database groups to the set. For ACS to map a user to the specified ACS group, the user must match *all* external user database groups in the set.

As an example, you could configure a group mapping for users who belong to the Engineering and Tokyo groups and a separate one for users who belong to Engineering and London. You could then configure separate group mappings for the combinations of Engineering-Tokyo and Engineering-London, and configure different access times for the ACS groups to which they map. You could also configure a group mapping that only included the Engineering group that would map other members of the Engineering group who were not members of Tokyo or London.

Group Mapping Order

ACS always maps users to a single ACS group; yet a user can belong to more than one group set mapping. For example, a user named *John* could be a member of the group combination Engineering and California, and at the same time be a member of the group combination Engineering and Managers. If ACS group set mappings exist for both these combinations, ACS has to determine to which group *John* should be assigned.

ACS prevents conflicting group set mappings by assigning a mapping order to the group set mappings. When a user who is authenticated by an external user database is assigned to an ACS group, ACS starts at the top of the list of group mappings for that database. ACS sequentially checks the user group

memberships in the external user database against each group mapping in the list. When finding the first group set mapping that matches the external user database group memberships of the user, ACS assigns the user to the ACS group of that group mapping and terminates the mapping process.



Tip

The order of group mappings is important because it affects the network access and services that are allowed to users. When defining mappings for users who belong to multiple groups, ensure that they are in the correct order; so that users are granted the correct group settings.

For example, a user named *Mary* is assigned to the three-group combination of Engineering, Marketing, and Managers. *Mary* should be granted the privileges of a manager rather than an engineer. Mapping A assigns to ACS Group 2 users who belong to all three groups of which *Mary* is a member. Mapping B assigns to ACS Group 1 users who belong to the Engineering and Marketing groups. If Mapping B is listed first, ACS authenticates *Mary* as a user of Group 1 and she is assigned to Group 1, rather than Group 2 as managers should be.

No Access Group for Group Set Mappings

To prevent remote access for users who are assigned a group by a particular group set mapping, assign the group to the ACS No Access group. For example, you could assign all members of an external user database group *Contractors* to the No Access group so they could not dial in to the network remotely.

Default Group Mapping for Windows

For Windows user databases, ACS includes the ability to define a default group mapping. If no other group mapping matches an unknown user who is authenticated by a Windows user database, ACS assigns the user to a group based on the default group mapping.

Configuring the default group mapping for Windows user databases is the same as editing an existing group mapping, with one exception. When editing the default group mapping for Windows, instead of selecting a valid domain name on the Domain Configurations page, select **\DEFAULT**.

For more information about editing an existing group mapping, see [Editing a Windows or Generic LDAP Group Set Mapping, page 16-6](#).

Creating an ACS Group Mapping for Windows or Generic LDAP Groups

Before You Begin

To map a Windows or generic LDAP group to an ACS group:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Group Mappings**.
 - Step 3** Click the external user database name for which you want to configure a group mapping.
If you are mapping a Windows group set, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.
 - Step 4** If you are mapping a Windows group set for a new domain:
 - a. Click **New configuration**.

The Define New Domain Configuration page appears.

- b. If the Windows domain for which you want to create a group set mapping configuration appears in the Detected domains list, select the name of the domain.



Tip To clear your domain selection, click **Clear Selection**.

- c. If the Windows domain for which you want to create a group set mapping *does not appear* in the Detected domains list, type the name of a trusted Windows domain in the **Domain** box.
- d. Click **Submit**.

The new Windows domain appears in the list of domains in the Domain Configurations page.

- Step 5** If you are mapping a Windows group set, click the domain name for which you want to configure a group set mapping.

The Group Mappings for Domain: *domainname* table appears.

- Step 6** To add groups by selecting from a list:

- a. Click **Add Mapping**.

The Create new group mapping for *database* page opens, where *database* is the name of the external user database for which you want to add a mapping. The group list displays group names that are derived from the external user database.

- b. For each group to be added to the group set mapping, select the name of the applicable external user database group in the group list, and then click **Add to selected**. The Selected list shows all the groups to which a user must belong to be mapped to an ACS group.



Note A user must match *all* the groups in the Selected list so that ACS can use this group set mapping to map the user to an ACS group; however, a user can also belong to other groups (in addition to the groups listed) and still be mapped to an ACS group.



Tip To remove a group from the mapping, select the name of the group in the Selected list, and then click **Remove from selected**.

- c. In the ACS group list, select the name of the ACS group to which you want to map users who belong to all the external user database groups in the Selected list.



Note You can also select **No Access**. For more information about the **No Access** group, see [No Access Group for Group Set Mappings, page 16-4](#).

- Step 7** To add groups manually (use this option when you have too many groups to enumerate, for example, 500 groups):

- a. Click **Add Manual Mapping**. The Manual Mapping page opens.
- b. Enter the list of Windows groups separated by a comma (,).
- c. In the ACS group list, select the name of the ACS group to which you want to map users who belong to all the external user database groups in the Selected list.

**Note**

You can also select **No Access**. For more information about the **No Access** group, see [No Access Group for Group Set Mappings, page 16-4](#).

Step 8 Click **Submit**.

The group set you mapped to the ACS list appears at the bottom of the *database* groups column.

**Note**

The asterisk (*) at the end of each set of groups indicates that users who are authenticated with the external user database can belong to other groups besides those in the set.

Editing a Windows or Generic LDAP Group Set Mapping

You can change the ACS group to which a group set mapping is mapped.

**Note**

You cannot edit the external user database groups of an existing group set mapping. If you want to add or remove external user database groups from the group set mapping, delete the group set mapping and create one with the revised set of groups.

To edit a Windows or generic LDAP group mapping:

Step 1 In the navigation bar, click **External User Databases**.

Step 2 Click **Database Group Mappings**.

Step 3 Click the external user database name for which you want to edit a group set mapping.

If you are editing a Windows group set mapping, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.

Step 4 If you are editing a Windows group set mapping, click the domain name for which you want to edit a group set mapping.

The Group Mappings for Domain: *domainname* table appears.

Step 5 Click the group set mapping to be edited.

The Edit mapping for *database* page opens. The external user database group or groups that are included in the group set mapping appear above the ACS group list.

Step 6 From the ACS group list, select the name of the group to which to map the set of external database groups, and then click **Submit**.

**Note**

You can also select **No Access**. For more information about the **No Access** group, see [No Access Group for Group Set Mappings, page 16-4](#).

Step 7 Click **Submit**.

The Group Mappings for *database* page opens again and includes the changed group set mapping.

Deleting a Windows or Generic LDAP Group Set Mapping

You can delete individual group set mappings.

To delete a Windows or generic LDAP group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Group Mappings**.
 - Step 3** Click the external user database configuration whose group set mapping you want to delete.
If you are deleting a Windows group set mapping, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.
 - Step 4** If you are deleting a Windows group set mapping, click the domain name whose group set mapping you want to delete.
The Group Mappings for Domain: *domainname* table appears.
 - Step 5** Click the group set mapping that you want to delete.
 - Step 6** Click **Delete**.
ACS displays a confirmation dialog box.
 - Step 7** Click **OK** in the confirmation dialog box.
ACS deletes the selected external user database group set mapping.
-

Deleting a Windows Domain Group Mapping Configuration

You can delete an entire group mapping configuration for a Windows domain. When you delete a Windows domain group mapping configuration, you delete all group set mappings in the configuration.

To delete a Windows group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
 - Step 2** Click **Database Group Mappings**.
 - Step 3** Click the name of the Windows external user database.
 - Step 4** Click the domain name whose group set mapping you want to delete.
 - Step 5** Click **Delete Configuration**.
ACS displays a confirmation dialog box.
 - Step 6** Click **OK** in the confirmation dialog box.
ACS deletes the selected external user database group mapping configuration.
-

Changing Group Set Mapping Order

You can change the order in which ACS checks group set mappings for users who are authenticated by Windows and generic LDAP databases. To order group mappings, you must have already mapped them. For more information about creating group mappings, see [Creating an ACS Group Mapping for Windows or Generic LDAP Groups, page 16-4](#).

To change the order of group mappings for a Windows or generic LDAP group mapping:

-
- Step 1** In the navigation bar, click **External User Databases**.
- Step 2** Click **Database Group Mappings**.
- Step 3** Click the external user database name for which you want to configure group set mapping order.
- If you are ordering Windows group set mappings, the Domain Configurations table appears. The Group Mappings for *database* Users table appears.
- Step 4** If you are configuring a Windows group mapping order, click the domain name for which you want to configure group set mapping order.
- The Group Mappings for Domain: *domainname* table appears.
- Step 5** Click **Order mappings**.



Note The Order mappings button appears only if more than one group set mapping exists for the current database and does not apply to default group mapping.

The Order mappings for *database* page appears. The group mappings for the current database appear in the Order list.

- Step 6** Select the name of a group set mapping that you want to move, and then click **Up** or **Down** until it is in the position that you want.
- Step 7** Repeat Step 7 until the group mappings are in the correct order.
- Step 8** Click **Submit**.
- The Group Mappings for *database* page displays the group set mappings in the order that you defined.
- Step 9** Click **Submit**.
- ACS saves the SPT-to-user-group mapping.
-

RADIUS-Based Group Specification

For some types of external user databases, ACS supports the assignment of users to specific ACS groups based on the RADIUS authentication response from the external user database. ACS provides this assignment in addition to the unknown user group mapping described in [Group Mapping by External User Database, page 16-1](#). RADIUS-based group specification overrides group mapping. The database types that support RADIUS-based group specification are:

- LEAP Proxy RADIUS server
- RADIUS token server

ACS supports per-user group mapping for users who are authenticated with a LEAP Proxy RADIUS Server database. This group mapping support is provided in addition to the default group mapping described in [Group Mapping by External User Database, page 16-1](#).

To enable per user group mapping, configure the external user database to return authentication responses that contain the Cisco IOS/PIX RADIUS attribute 1, [009\001] `cisco-av-pair` with the following value:

```
ACS:CiscoSecure-Group-Id = N
```

where *N* is the ACS group number (0 through 499) to which ACS should assign the user. For example, if the LEAP Proxy RADIUS Server authenticated a user and included the following value for the Cisco IOS/PIX RADIUS attribute 1, [009\001] `cisco-av-pair`:

```
ACS:CiscoSecure-Group-Id = 37
```

ACS assigns the user to group 37 and applies authorization that is associated with group 37.



APPENDIX A

TACACS+ Attribute-Value Pairs

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, supports Terminal Access Controller Access Control System (TACACS+) attribute-value (AV) pairs. You can enable different AV pairs for any supported attribute value.

Cisco IOS AV Pair Dictionary

To use the full range of the Cisco IOS AV-pair dictionary for TACACS+, the AAA client should use IOS version 11.3 or later. Cisco IOS 11.1 and 11.2 have only partial support for TACACS+ AV-pairs.



Note

If you specify a given AV pair in ACS, you must also enable the corresponding AV pair in the Cisco IOS software that is running on the AAA client. Therefore, you must consider which AV pairs your Cisco IOS release supports. If ACS sends an AV pair to the AAA client that the Cisco IOS software does not support, that attribute is not implemented.

For more information on TACACS+ AV pairs, refer to Cisco IOS documentation for the release of Cisco IOS that is running on your AAA clients.



Note

All TACACS+ values are strings. The concept of value *type* does not exist in TACACS+ as it does in Remote Access Dial-In User Service (RADIUS).

TACACS+ AV Pairs



Note

Beginning with ACS 2.3, some TACACS+ attributes no longer appear on the Group Setup page; because IP pools and callback supersede:

```
addr
addr-pool
callback-dialstring
```

Additionally, these attributes cannot be set via database synchronization, and *ip:addr=n.n.n.n* is not allowed as a Cisco vendor-specific attribute (VSA).

ACS supports many TACACS+ AV pairs. For descriptions of these attributes, refer to Cisco IOS documentation for the release of Cisco IOS that is running on your AAA clients. TACACS+ AV pairs supported in ACS are:

- acl=
- autocmd=
- callback-line
- callback-rotary
- cmd-arg=
- cmd=
- dns-servers=
- gw-password
- idletime=
- inacl#n
- inacl=
- interface-config=
- ip-addresses
- link-compression=
- load-threshold=n
- max-links=n
- nas-password
- nocalcallback-verify
- noescape=
- nohangup=
- old-prompts
- outacl#n
- outacl=
- pool-def#n
- pool-timeout=
- ppp-vj-slot-compression
- priv-lvl=
- protocol=
- route
- route#n
- routing=
- rte-ftr-in#n
- rte-ftr-out#n
- sap#n
- sap-fltr-in#n
- sap-fltr-out#n
- service=
- source-ip=
- timeout=
- tunnel-id
- wins-servers=
- zonelist=

TACACS+ Accounting AV Pairs

ACS supports many TACACS+ accounting AV pairs. For descriptions of these attributes, see Cisco IOS documentation for the release of Cisco IOS that is running on your AAA clients. TACACS+ accounting AV pairs that ACS supports are:

- bytes_in
- bytes_out
- cmd
- data-rate
- disc-cause
- disc-cause-ext
- elapsed_time
- event
- mlp-links-max
- mlp-sess-id
- nas-rx-speed
- nas-tx-speed
- paks_in
- paks_out
- port
- pre-bytes-in
- pre-bytes-out
- pre-paks-in
- pre-paks-out
- pre-session-time
- priv_level
- protocol
- reason
- service
- start_time
- stop_time
- task_id
- timezone
- xmit-rate



APPENDIX B

RADIUS Attributes

The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, supports many Remote Access Dial-In User Service (RADIUS) attributes. This appendix lists the standard attributes, vendor-proprietary attributes, and vendor-specific attributes that ACS supports.

This appendix contains:

- [Before Using RADIUS Attributes, page B-1](#)
- [Cisco IOS Dictionary of RADIUS IETF, page B-2](#)
- [Cisco IOS/PIX 6.0 Dictionary of RADIUS VSAs, page B-4](#)
- [About the cisco-av-pair RADIUS Attribute, page B-5](#)
- [Cisco VPN 3000 Concentrator/ASA/PIX 7.x+ Dictionary of RADIUS VSAs, page B-6](#)
- [Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs, page B-10](#)
- [Cisco Building Broadband Service Manager Dictionary of RADIUS VSA, page B-10](#)
- [Cisco Airespace Dictionary of RADIUS VSA, page B-10](#)
- [IETF Dictionary of RADIUS IETF \(AV Pairs\), page B-11](#)
- [Microsoft MPPE Dictionary of RADIUS VSAs, page B-19](#)
- [Ascend Dictionary of RADIUS AV Pairs, page B-21](#)
- [Nortel Dictionary of RADIUS VSAs, page B-28](#)
- [Juniper Dictionary of RADIUS VSAs, page B-28](#)
- [3COMUSR Dictionary of RADIUS VSAs, page B-28](#)

Before Using RADIUS Attributes

You can enable different attribute-value (AV) pairs for Internet Engineering Task Force (IETF) RADIUS and any supported vendor. For outbound attributes, you can configure the attributes that are sent and their content by using the ACS web interface. The RADIUS attributes that are sent to authentication, authorization, and accounting (AAA) clients in access-accept messages are user specific.

To configure a specific attribute to be sent for a user, you must ensure that:

1. In the Network Configuration section, you must configure the AAA client entry corresponding to the access device that grants network access to the user to use a variety of RADIUS that supports the attribute that you want sent to the AAA client. For more information about the RADIUS attribute sets that RADIUS varieties support, see [Displaying TACACS+ Configuration Options, page 2-6](#).

2. In the Interface Configuration section, you must enable the attribute so that it appears on user or user group profile pages. You can enable attributes on the page corresponding to the RADIUS variety that supports the attribute. For example, IETF RADIUS Session-Timeout attribute (27) appears on the RADIUS (IETF) page.

**Note**

By default, per-user RADIUS attributes are not enabled (they do not appear in the Interface Configuration page). Before you can enable attributes on a per-user basis, you must enable the **Per-user TACACS+/RADIUS Attributes** option on the Advanced Options page in the Interface Configuration section. After enabling per-user attributes, a user column will appear as disabled in the Interface Configuration page for that attribute.

3. In the profile that you use to control authorizations for the user—in the user or group edit pages or Shared RADIUS Authorization Component page—you must enable the attribute. Enabling this attribute causes ACS to send the attribute to the AAA client in the access-accept message. In the options that are associated with the attribute, you can determine the value of the attribute that is sent to the AAA client.

**Note**

Settings in a user profile override settings in a group profile. For example, if you configure Session-Timeout in the user profile and also in the group to which the user is assigned, ACS sends the AAA client the Session-Timeout value that is specified in the user profile. If Network Access Profiles (NAPs) are being used, it is possible that attributes from Shared RADIUS Authorization Components may be included in the access-accept response. For a discussion about the interaction among group, user, and Shared Radius Authorization Components (SRAC) attributes, see [Merging Attributes, page 14-35](#).

Cisco IOS Dictionary of RADIUS IETF

ACS supports Cisco RADIUS IETF (IOS RADIUS AV pairs). Before selecting AV pairs for ACS, you must confirm that your AAA client is a compatible release of Cisco IOS or compatible AAA client software. For more information, see the *Installation Guide for Cisco Secure ACS for Windows Release 4.2* or the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2* for information about network and port requirements.

**Note**

If you specify a given AV pair on ACS, the corresponding AV pair must be implemented in the Cisco IOS software that is running on the network device. Always consider which AV pairs your Cisco IOS release supports. If ACS sends an AV pair that the Cisco IOS software does not support, the attribute is not implemented.

**Note**

Because IP pools and callback supersede them, the following RADIUS attributes do not appear on the Group Setup page:

Number	Name
8	Framed-IP-Address
19	Callback-Number
218	Ascend-Assign-IP-Pool

None of these attributes can be set via Relational Database Management System (RDBMS) Synchronization.

Table B-1 lists the supported Cisco IOS RADIUS AV pairs.

Table B-1 Cisco IOS Software RADIUS AV Pairs

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
1	User-Name	String	Inbound	No
2	User-Password	String	Outbound	No
3	CHAP-Password	String	Outbound	No
4	NAS-IP Address	Ipaddr	Inbound	No
5	NAS-Port	Integer	Inbound	No
6	Service-Type	Integer	Both	No
7	Framed-Protocol	Integer	Both	No
9	Framed-IP-Netmask	Ipaddr (maximum length 15 characters)	Outbound	No
10	Framed-Routing	Integer	Outbound	No
11	Filter-Id	String	Outbound	Yes
12	Framed-MTU	Integer (maximum length 10 characters)	Outbound	No
13	Framed-Compression	Integer	Outbound	Yes
14	Login-IP-Host	Ipaddr (maximum length 15 characters)	Both	Yes
15	Login-Service	Integer	Both	No
16	Login-TCP-Port	Integer (maximum length 10 characters)	Outbound	No
18	Reply-Message	String	Outbound	Yes
21	Expiration	Date	—	—
22	Framed-Route	String	Outbound	Yes
24	State	String (maximum length 253 characters)	Outbound	No
25	Class	String	Outbound	Yes
26	Vendor specific	String	Outbound	Yes
27	Session-Timeout	Integer (maximum length 10 characters)	Outbound	No
28	Idle-Timeout	Integer (maximum length 10 characters)	Outbound	No
30	Called-Station-ID	String	Inbound	No

Table B-1 Cisco IOS Software RADIUS AV Pairs (continued)

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
31	Calling-Station-ID	String	Inbound	No
33	Login-LAT-Service	String (maximum length 253 characters)	Inbound	No
40	Acct-Status-Type	Integer	Inbound	No
41	Acct-Delay-Time	Integer	Inbound	No
42	Acct-Input-Octets	Integer	Inbound	No
43	Acct-Output-Octets	Integer	Inbound	No
44	Acct-Session-ID	String	Inbound	No
45	Acct-Authentic	Integer	Inbound	No
46	Acct-Session-Time	Integer	Inbound	No
47	Acct-Input-Packets	Integer	Inbound	No
48	Acct-Output-Packets	Integer	Inbound	No
49	Acct-Terminate-Cause	Integer	Inbound	No
61	NAS-Port-Type	Integer	Inbound	No
62	NAS-Port-Limit	Integer (maximum length 10 characters)	Both	No

Cisco IOS/PIX 6.0 Dictionary of RADIUS VSAs

ACS supports Cisco IOS/PIX 6.0 vendor-specific attributes (VSAs). The vendor ID for this Cisco RADIUS Implementation is 9.

[Table B-2](#) lists the supported Cisco IOS/PIX 6.0 RADIUS VSAs.



Note

For a discussion of the Cisco IOS/PIX 6.0 RADIUS `cisco-av-pair` attribute, see [About the cisco-av-pair RADIUS Attribute, page B-5](#).



Note

For details about the Cisco IOS H.323 VSAs, refer to Cisco IOS Voice-over-IP (VoIP) documentation.



Note

For details about the Cisco IOS Node Route Processor-Service Selection Gateway VSAs (VSAs 250, 251, and 252), refer to Cisco IOS documentation.

Table B-2 Cisco IOS/PIX 6.0 RADIUS VSAs

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
1	cisco-av-pair	String	Both	Yes
2	cisco-nas-port	String	Inbound	No
23	cisco-h323-remote-address	String	Inbound	No
24	cisco-h323-conf-id	String	Inbound	No

Table B-2 Cisco IOS/PIX 6.0 RADIUS VSAs (continued)

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
25	cisco-h323-setup-time	String	Inbound	No
26	cisco-h323-call-origin	String	Inbound	No
27	cisco-h323-call-type	String	Inbound	No
28	cisco-h323-connect-time	String	Inbound	No
29	cisco-h323-disconnect-time	String	Inbound	No
30	cisco-h323-disconnect-cause	String	Inbound	No
31	cisco-h323-voice-quality	String	Inbound	No
33	cisco-h323-gw-id	String	Inbound	No
35	cisco-h323-incoming-conn-id	String	Inbound	No
101	cisco-h323-credit-amount	String (maximum length 247 characters)	Outbound	No
102	cisco-h323-credit-time	String (maximum length 247 characters)	Outbound	No
103	cisco-h323-return-code	String (maximum length 247 characters)	Outbound	No
104	cisco-h323-prompt-id	String (maximum length 247 characters)	Outbound	No
105	cisco-h323-day-and-time	String (maximum length 247 characters)	Outbound	No
106	cisco-h323-redirect-number	String (maximum length 247 characters)	Outbound	No
107	cisco-h323-preferred-lang	String (maximum length 247 characters)	Outbound	No
108	cisco-h323-redirect-ip-addr	String (maximum length 247 characters)	Outbound	No
109	cisco-h323-billing-model	String (maximum length 247 characters)	Outbound	No
110	cisco-h323-currency	String (maximum length 247 characters)	Outbound	No
250	cisco-ssg-account-info	String (maximum length 247 characters)	Outbound	No
251	cisco-ssg-service-info	String (maximum length 247 characters)	Both	No
253	cisco-ssg-control-info	String (maximum length 247 characters)	Both	No

About the cisco-av-pair RADIUS Attribute

The first attribute in the Cisco IOS/PIX 6.0 RADIUS implementation, `cisco-av-pair`, supports the inclusion of many AV pairs by using the following format:

attribute sep value

where *attribute* and *value* are an AV pair supported by the releases of IOS implemented on your AAA clients, and *sep* is = for mandatory attributes and asterisk (*) for optional attributes. You can then use the full set of Terminal Access Controller Access Control System (TACACS+) authorization features for RADIUS.



Note

The attribute name in an AV pair is case sensitive. Typically, attribute names are all in lowercase letters.

The following is an example of two AV pairs included in a single Cisco IOS/PIX 6.0 RADIUS `cisco-av-pair` attribute:

```
ip:addr-pool=first
shell:priv-lvl=15
```

The first example activates the Cisco multiple named IP address pools feature during IP authorization (during PPP IPCP address assignment). The second example immediately grants access to a user of a device-hosted administrative session to **EXEC** commands.

In IOS, support for Network Admission Control (NAC) includes the use of the following AV pairs:

- **url-redirect**—Enables the AAA client to intercept an HTTP request and redirect it to a new URL. This pair is especially useful if the result of posture validation indicates that the NAC-client computer requires an update or patch that you have made available on a remediation web server. For example, a user can be redirected to a remediation web server to download and apply a new virus DAT file or an operating system patch. For example:

```
url-redirect=http://10.1.1.1
```

- **posture-token**—Enables ACS to send a text version of a system posture token (SPT) derived by posture validation. The SPT is always sent in numeric format and using the posture-token AV pair renders the result of a posture validation request more easily read on the AAA client. For example:

```
posture-token=Healthy
```



Caution

The posture-token AV pair is the only way that ACS notifies the AAA client of the SPT that posture validation returns. Because you manually configure the posture-token AV pair, errors in configuring the posture-token can cause the incorrect system posture token to be sent to the AAA client or; if the AV pair name is mistyped, the AAA client will not receive the system posture token at all.

For a list of valid SPTs, see [Posture Tokens, page 13-3](#).

- **status-query-timeout**—Overrides the status-query default value of the AAA client with the value that you specify, in seconds. For example:

```
status-query-timeout=150
```

For more information about AV pairs that IOS supports, refer to the documentation for the releases of IOS implemented on your AAA clients.

Cisco VPN 3000 Concentrator/ASA/PIX 7.x+ Dictionary of RADIUS VSAs

ACS supports Cisco VPN 3000/ASA/PIX 7.x+ RADIUS VSAs. The vendor ID for this Cisco RADIUS Implementation is 3076.



Note

Some of the RADIUS VSAs supported by Cisco virtual private network (VPN) 3000 Concentrators, Adaptive Security Appliance (ASA), and Project Information Exchange (PIX) 7.x+ appliances are interdependent. Before you implement them, we recommend that you refer to your respective device documentation.

For example, to control Microsoft Point-to-Point Encryption (MPPE) settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

Table B-3 lists the supported Cisco VPN 3000 Concentrator RADIUS VSAs.

Table B-3 Cisco VPN 3000 Concentrator /ASA/PIX 7.x+ RADIUS VSAs

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
1	CVPN3000-Access-Hours	String (maximum length 247 characters)	Outbound	No
2	CVPN3000-Simultaneous-Logins	Integer (maximum length 10 characters)	Outbound	No
5	CVPN3000-Primary-DNS	Ipaddr (maximum length 15 characters)	Outbound	No
6	CVPN3000-Secondary-DNS	Ipaddr (maximum length 15 characters)	Outbound	No
7	CVPN3000-Primary-WINS	Ipaddr (maximum length 15 characters)	Outbound	No
8	CVPN3000-Secondary-WINS	Ipaddr (maximum length 15 characters)	Outbound	No
9	CVPN3000-SEP-Card-Assignment	Integer	Outbound	No
11	CVPN3000-Tunneling-Protocols	Integer	Outbound	No
12	CVPN3000-IPSec-Sec-Association	String (maximum length 247 characters)	Outbound	No
13	CVPN3000-IPSec-Authentication	Integer	Outbound	No
15	CVPN3000-IPSec-Banner1	String (maximum length 247 characters)	Outbound	No
16	CVPN3000-IPSec-Allow-Passwd-Store	Integer	Outbound	No
17	CVPN3000-Use-Client-Address	Integer	Outbound	No
20	CVPN3000-PPTP-Encryption	Integer	Outbound	No
21	CVPN3000-L2TP-Encryption	Integer	Outbound	No
27	CVPN3000-IPSec-Split-Tunnel-List	String (maximum length 247 characters)	Outbound	No
28	CVPN3000-IPSec-Default-Domain	String (maximum length 247 characters)	Outbound	No
29	CVPN3000-IPSec-Split-DNS-Names	String (maximum length 247 characters)	Outbound	No
30	CVPN3000-IPSec-Tunnel-Type	Integer	Outbound	No
31	CVPN3000-IPSec-Mode-Config	Integer	Outbound	No
33	CVPN3000-IPSec-User-Group-Lock	Integer	Outbound	No
34	CVPN3000-IPSec-Over-UDP	Integer	Outbound	No
35	CVPN3000-IPSec-Over-UDP-Port	Integer (maximum length 10 characters)	Outbound	No
36	CVPN3000-IPSec-Banner2	String (maximum length 247 characters)	Outbound	No
37	CVPN3000-PPTP-MPPC-Compression	Integer	Outbound	No
38	CVPN3000-L2TP-MPPC-Compression	Integer	Outbound	No
39	CVPN3000-IPSec-IP-Compression	Integer	Outbound	No
40	CVPN3000-IPSec-IKE-Peer-ID-Check	Integer	Outbound	No
41	CVPN3000-IKE-Keep-Alives	Integer	Outbound	No

Table B-3 Cisco VPN 3000 Concentrator /ASA/PIX 7.x+ RADIUS VSAs (continued)

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
42	CVPN3000-IPSec-Auth-On-Rekey	Integer	Outbound	No
45	CVPN3000-Required-Client-Firewall-Vendor-Code	Integer (maximum length 10 characters)	Outbound	No
46	CVPN3000-Required-Client-Firewall-Product-Code	Integer (maximum length 10 characters)	Outbound	No
47	CVPN3000-Required-Client-Firewall-Description	String (maximum length 247 characters)	Outbound	No
48	CVPN3000-Require-HW-Client-Auth	Integer	Outbound	No
49	CVPN3000-Require-Individual-User-Auth	Integer	Outbound	No
50	CVPN3000-Authenticated-User-Idle-Timeout	Integer (maximum length 10 characters)	Outbound	No
51	CVPN3000-Cisco-IP-Phone-Bypass	Integer	Outbound	No
52	CVPN3000-User-Auth-Server-Name	String (maximum length 247 characters)	Outbound	No
53	CVPN3000-User-Auth-Server-Port	Integer (maximum length 10 characters)	Outbound	No
54	CVPN3000-User-Auth-Server-Secret	String (maximum length 247 characters)	Outbound	No
55	CVPN3000-IPSec-Split-Tunneling-Policy	Integer	Outbound	No
56	CVPN3000-IPSec-Required-Client-Firewall-Capability	Integer	Outbound	No
57	CVPN3000-IPSec-Client-Firewall-Filter-Name	String (maximum length 247 characters)	Outbound	No
58	CVPN3000-IPSec-Client-Firewall-Filter-Optional	Integer	Outbound	No
59	CVPN3000-IPSec-Backup-Servers	Integer	Outbound	No
60	CVPN3000-IPSec-Backup-Server-List	String (maximum length 247 characters)	Outbound	No
62	CVPN3000-MS-Client-Intercept-DHCP-Configure-Message	Integer	Outbound	No
63	CVPN3000-MS-Client-Subnet-Mask	Ipaddr (maximum length 15 characters)	Outbound	No
64	CVPN3000-Allow-Network-Extension-Mode	Integer	Outbound	No
65	Authorization-Type	Integer	Outbound	No
66	Authorization-Required	Integer	Outbound	No
67	Authorization-DN-Field	String	Outbound	No
68	IKE-Keepalive-Confidence-Interval	Integer	Outbound	No
69	WebVPN-Content-Filter-Parameters	Integer	Outbound	No
75	Cisco-LEAP-Bypass	Integer	Outbound	No
77	Client-Type-Version-Limiting	String	Outbound	No
79	WebVPN-Port-Forwarding-Name	String	Outbound	No

Table B-3 Cisco VPN 3000 Concentrator /ASA/PIX 7.x+ RADIUS VSAs (continued)

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
80	IE-Proxy-Server	String	Outbound	No
81	IE-Proxy-Server-Policy	Integer	Outbound	No
82	IE-Proxy-Exception-List	String	Outbound	No
83	IE-Proxy-Bypass-Local	Integer	Outbound	No
84	IKE-Keepalive-Retry-Interval	Integer	Outbound	No
85	Tunnel-Group-Lock	String	Outbound	No
86	Access-List-Inbound	String	Outbound	No
87	Access-List-Outbound	String	Outbound	No
88	Perfect-Forward-Secrecy-Enable	Integer	Outbound	No
89	NAC-Enable	Integer	Outbound	No
90	NAC-Status-Query-Timer	Integer	Outbound	No
91	NAC-Revalidation-Timer	Integer	Outbound	No
92	NAC-Default-ACL	Integer	Outbound	No
93	WebVPN-URL-Entry-Enable	Integer	Outbound	No
94	WebVPN-File-Access-Enable	Integer	Outbound	No
95	WebVPN-File-Server-Entry-Enable	Integer	Outbound	No
96	WebVPN-File-Server-Browsing-Enable	Integer	Outbound	No
97	WebVPN-Port-Forwarding-Enable	Integer	Outbound	No
98	WebVPN-Outlook-Exchange-Proxy-Enable	Integer	Outbound	No
98	WebVPN-Port-Forwarding-HTTP-Proxy	Integer	Outbound	No
99	WebVPN-Outlook-Exchange-Proxy-Enable	Integer	Outbound	No
100	WebVPN-Auto-Applet-Download-Enable	Integer	Outbound	No
101	WebVPN-Citrix-MetaFrame-Enable	Integer	Outbound	No
102	WebVPN-Apply-ACL	Integer	Outbound	No
103	WebVPN-SSL-VPN-Client-Enable	Integer	Outbound	No
104	WebVPN-SSL-VPN-Client-Required	Integer	Outbound	No
105	WebVPN-SSL-VPN-Client-Keep-Installation	Integer	Outbound	No
135	CVPN3000-Strip-Realm	Integer	Outbound	No

Cisco VPN 5000 Concentrator Dictionary of RADIUS VSAs

ACS supports the Cisco VPN 5000 RADIUS VSAs. The vendor ID for this Cisco RADIUS Implementation is 255. [Table B-4](#) lists the supported Cisco VPN 5000 Concentrator RADIUS VSAs.

Table B-4 Cisco VPN 5000 Concentrator RADIUS VSAs

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
001	CVPN5000-Tunnel-Throughput	Integer	Inbound	No
002	CVPN5000-Client-Assigned-IP	String	Inbound	No
003	CVPN5000-Client-Real-IP	String	Inbound	No
004	CVPN5000-VPN-GroupInfo	String (maximum length 247 characters)	Outbound	No
005	CVPN5000-VPN-Password	String (maximum length 247 characters)	Outbound	No
006	CVPN5000-Echo	Integer	Inbound	No
007	CVPN5000-Client-Assigned-IPX	Integer	Inbound	No

Cisco Building Broadband Service Manager Dictionary of RADIUS VSA

ACS supports a Cisco Building Broadband Service Manager (BBSM) RADIUS VSA. The vendor ID for this Cisco RADIUS Implementation is 5263.

[Table B-5](#) lists the supported Cisco BBSM RADIUS VSA.

Table B-5 Cisco BBSM RADIUS VSA

Number	Attribute	Type of Value	Inbound/Outbound	Multiple
001	CBBSM-Bandwidth	Integer	Both	No

Cisco Airespace Dictionary of RADIUS VSA

[Table B-6](#) lists the supported RADIUS (Cisco Airespace) attributes. In addition to these attributes, Cisco Airespace devices support some IETF attributes for 802.1x identity networking:

- Tunnel-Type (64)
- Tunnel-Medium-Type (65)
- Tunnel-Private-Group-Id (81)

ACS cannot offer partial support of IETF; hence, adding an Cisco Airespace device (into the Network Configuration) will automatically enable all IETF attributes.

Table B-6 Cisco Airespace RADIUS Attributes

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
1	Aire-WLAN-Id	Name of the user being authenticated.	Integer	Outbound	No
2	Aire-QoS-Level	Enumerations: 0: Bronze 1: Silver 2: Gold 3: Platinum 4: Uranium	Integer	Outbound	No
3	Aire-DSCP	—	Integer	Outbound	No
4	Aire-802.1P-Tag	—	Integer	Outbound	No
5	Aire-Interface-Name	—	String	Outbound	No
6	Aire-ACL-Name	—	String	Outbound	No

IETF Dictionary of RADIUS IETF (AV Pairs)

Table B-7 lists the supported RADIUS (IETF) attributes. If the attribute has a security server-specific format, the format is specified.

Table B-7 RADIUS (IETF) Attributes

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
1	User-Name	Name of the user being authenticated.	String	Inbound	No
2	User-Password	User password or input following an access challenge. Passwords longer than 16 characters are encrypted by using IETF Draft #2 or later specifications.	String	Outbound	No
3	CHAP-Password	PPP (Point-to-Point Protocol) Challenge Handshake Authentication Protocol (CHAP) response to an Access-Challenge.	String	Outbound	No
4	NAS-IP Address	IP address of the AAA client that is requesting authentication.	Ipaddr	Inbound	No

Table B-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
5	NAS-Port	<p>Physical port number of the AAA client that is authenticating the user. The AAA client port value (32 bits) comprises one or two 16-bit values, depending on the setting of the RADIUS server extended portnames command. Each 16-bit number is a 5-digit decimal integer interpreted as:</p> <ul style="list-style-type: none"> Asynchronous terminal lines, async network interfaces, and virtual async interfaces, the value is <code>00ttt</code>, where <i>ttt</i> is the line number or async interface unit number. Ordinary synchronous network interfaces, the value is <code>10xxx</code>. Channels on a primary-rate ISDN (Integrated Services Digital Network) interface, the value is <code>2ppcc</code>. Channels on a basic rate ISDN interface, the value is <code>3bb0c</code>. Other types of interfaces, the value is <code>6nnss</code>. 	Integer	Inbound	No
6	Service-Type	<p>Type of service requested or type of service to be provided:</p> <ul style="list-style-type: none"> In a request: <ul style="list-style-type: none"> Framed—For a known Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP) connection. Administrative User—For enable command. In a response: <ul style="list-style-type: none"> Login—Make a connection. Framed—Start SLIP or PPP. Administrative User—Start an EXEC or enable ok. Exec User—Start an EXEC session. 	Integer	Both	No
7	Framed-Protocol	Framing to be used for framed access.	Integer	Both	No
8	Framed-IP-Address	Address to be configured for the user.	—	—	—
9	Framed-IP-Netmask	IP netmask to be configured for the user when the user is a router to a network. This AV causes a static route to be added for Framed-IP-Address with the mask specified.	Ipaddr (maximum length 15 characters)	Outbound	No

Table B-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
10	Framed-Routing	Routing method for the user when the user is a router to a network. Only None and Send and Listen values are supported for this attribute.	Integer	Outbound	No
11	Filter-Id	Name of the filter list for the user, formatted: <i>%d</i> , <i>%d.in</i> , or <i>%d.out</i> . This attribute is associated with the most recent service-type command. For login and EXEC , use <i>%d</i> or <i>%d.out</i> as the line access list value from 0 to 199. For Framed service, use <i>%d</i> or <i>%d.out</i> as interface output access list and <i>%d.in</i> for input access list. The numbers are self-encoding to the protocol to which they refer.	String	Outbound	Yes
12	Framed-MTU	Indicates the maximum transmission unit (MTU) that you can configure for the user when the MTU is not negotiated by PPP or some other means.	Integer (maximum length 10 characters)	Outbound	No
13	Framed-Compression	Compression protocol used for the link. This attribute results in /compress being added to the PPP or SLIP autocommand generated during EXEC authorization. Not currently implemented for non-EXEC authorization.	Integer	Outbound	Yes
14	Login-IP-Host	Host to which the user will connect when the Login-Service attribute is included.	Ipaddr (maximum length 15 characters)	Both	Yes
15	Login-Service	Service that you should use to connect the user to the login host. Service is indicated by a numeric value: 0: Telnet 1: Rlogin 2: TCP-Clear 3: PortMaster 4: LAT	Integer	Both	No
16	Login-TCP-Port	Transmission Control Protocol (TCP) port with which to connect the user when the Login-Service attribute is also present.	Integer (maximum length 10 characters)	Outbound	No
18	Reply-Message	Text that the user will see.	String	Outbound	Yes
19	Callback-Number	—	String	Outbound	No
20	Callback-Id	—	String	Outbound	No

Table B-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
22	Framed-Route	Routing information to configure for the user on this AAA client. The RADIUS RFC (Request for Comments) format (net/bits [router [metric]]) and the old style dotted mask (net mask [router [metric]]) are supported. If the router field is omitted or zero (0), the peer IP address is used. Metrics are ignored.	String	Outbound	Yes
23	Framed-IPX-Network	—	Integer	Outbound	No
24	State	Allows State information to be maintained between the AAA client and the RADIUS server. This attribute is applicable only to CHAP challenges.	String (maximum length 253 characters)	Outbound	No
25	Class	Arbitrary value that the AAA client includes in all accounting packets for this user if supplied by the RADIUS server.	String	Both	Yes
26	Vendor-Specific	Carries subattributes known as vendor-specific attributes (VSAs), a feature of RADIUS that allows vendors to support their own extended attributes. Subattributes are identified by IANA-assigned vendor numbers in combination with the vendor-assigned subattribute number. For example, the vendor number for Cisco IOS/PIX 6.0 RADIUS is 9. The <code>cisco-av-pair</code> VSA is attribute 1 in the set of VSAs related to vendor number 9.	String	Outbound	Yes
27	Session-Timeout	Maximum number of seconds of service to provide to the user before the session terminates. This AV becomes the per-user absolute timeout. This attribute is not valid for PPP sessions.	Integer (maximum length 10 characters)	Outbound	No
28	Idle-Timeout	Maximum number of consecutive seconds of idle connection time that the user is allowed before the session terminates. This AV becomes the per-user session-timeout. This attribute is not valid for PPP sessions.	Integer (maximum length 10 characters)	Outbound	No
29	Termination-Action	Indicates what action the NAS should take when the specified service is completed. It is only used in Access-Accept packets. If the Value is set to RADIUS-Request (1), upon termination of the specified service, the NAS may send a new Access-Request to the RADIUS server, including the State attribute if any.	Integer	Both	No
30	Called-Station-Id	Allows the AAA client to send the telephone number or other information identifying the AAA client as part of the access-request packet by using automatic number identification or similar technology. Different devices provide different identifiers.	String	Inbound	No

Table B-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
31	Calling-Station-Id	Allows the AAA client to send the telephone number or other information identifying the end-user client as part of the access-request packet by using Dialed Number Identification Server (DNIS) or similar technology. For example, Cisco Aironet Access Points usually send the MAC address of the end-user client.	String	Inbound	No
32	NAS-Identifier	—	String	Inbound	No
33	Proxy-State	Included in proxied RADIUS requests per RADIUS standards. The operation of ACS does not depend on the contents of this attribute.	String (maximum length 253 characters)	Inbound	No
34	Login-LAT-Service	System with which the local area transport (LAT) protocol connects the user. This attribute is only available in the EXEC mode.	String (maximum length 253 characters)	Inbound	No
35	Login-LAT-Node	—	String	Inbound	No
36	Login-LAT-Group	—	String	Inbound	No
37	Framed-AppleTalk-Link	—	Integer	Outbound	No
38	Framed-AppleTalk-Network	—	Integer	Outbound	Yes
39	Framed-AppleTalk-Zone	—	String	Out	No
40	Acct-Status-Type	Specifies whether this accounting-request marks the beginning of the user service (start) or the end (stop).	Integer	Inbound	No
41	Acct-Delay-Time	Number of seconds the client has been trying to send a particular record.	Integer	Inbound	No
42	Acct-Input-Octets	Number of octets received from the port while this service is being provided.	Integer	Inbound	No
43	Acct-Output-Octets	Number of octets sent to the port while this service is being delivered.	Integer	Inbound	No
44	Acct-Session-Id	Unique accounting identifier that makes it easy to match start and stop records in a log file. The <code>Acct-Session-Id</code> restarts at 1 each time the router is power cycled or the software is reloaded. Contact Cisco support if this interval is unsuitable.	String	Inbound	No

Table B-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
44	Acct-Authentic	Way in which the user was authenticated—by RADIUS, the AAA client itself, or another remote authentication protocol. This attribute is set to radius for users who are authenticated by RADIUS; to remote for TACACS+ and Kerberos; or to local for local, enable, line, and if-needed methods. For all other methods, the attribute is omitted.	Integer	Inbound	No
46	Acct-Session-Time	Number of seconds the user has been receiving service.	Integer	Inbound	No
47	Acct-Input-Packets	Number of packets received from the port while this service is being provided to a framed user.	Integer	Inbound	No
48	Acct-Output-Packets	Number of packets sent to the port while this service is being delivered to a framed user.	Integer	Inbound	No
49	Acct-Terminate-Cause	Reports details on why the connection was terminated. Termination causes are indicated by a numeric value: 1: User request 2: Lost carrier 3: Lost service 4: Idle timeout 5: Session-timeout 6: Admin reset 7: Admin reboot 8: Port error 9: AAA client error 10: AAA client request 11: AAA client reboot 12: Port unneeded 13: Port pre-empted 14: Port suspended 15: Service unavailable 16: Callback 17: User error 18: Host request	Integer	Inbound	No
50	Acct-Multi-Session-Id	—	String	Inbound	No
51	Acct-Link-Count	—	Integer	Inbound	No
52	Acct-Input-Gigawords	—	Integer	Inbound	No

Table B-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
53	Acct-Output-Gigawords	—	Integer	Inbound	No
55	Event-Timestamp	—	Date	Inbound	No
60	CHAP-Challenge	—	String	Inbound	No
61	NAS-Port-Type	Indicates the type of physical port the AAA client is using to authenticate the user. Physical ports are indicated by a numeric value: 0: Asynchronous 1: Synchronous 2: ISDN-Synchronous 3: ISDN-Asynchronous (V.120) 4: ISDN- Asynchronous (V.110) 5: Virtual	Integer	Inbound	No
62	Port-Limit	Sets the maximum number of ports to be provided to the user by the network-access server.	Integer (maximum length 10 characters)	Both	No
63	Login-LAT-Port	—	String	Both	No
64	Tunnel-Type	—	Tagged integer	Both	Yes
65	Tunnel-Medium-Type	—	Tagged integer	Both	Yes
66	Tunnel-Client-Endpoint	—	Tagged string	Both	Yes
67	Tunnel-Server-Endpoint	—	Tagged string	Both	Yes
68	Acct-Tunnel-Connection	—	String	Inbound	No
69	Tunnel-Password	—	Tagged string	Both	Yes
70	ARAP-Password	—	String	Inbound	No
71	ARAP-Features	—	String	Outbound	No
72	ARAP-Zone-Access	—	Integer	Outbound	No

Table B-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
73	ARAP-Security	—	Integer	Inbound	No
74	ARAP-Security-Data	—	String	Inbound	No
75	Password-Retry	—	Integer	Internal use only	No
76	Prompt	—	Integer	Internal use only	No
77	Connect-Info	—	String	Inbound	No
78	Configuration-Token	—	String	Internal use only	No
79	EAP-Message	—	String	Internal use only	No
80	Message-Authenticator	—	String	Outbound	No
81	Tunnel-Private-Group-ID	—	Tagged string	Both	Yes
82	Tunnel-Assignment-ID	—	Tagged string	Both	Yes
83	Tunnel-Preference	—	Tagged integer	Both	No
85	Acct-Interim-Interval	—	Integer	Outbound	No
87	NAS-Port-Id	—	String	Inbound	No
88	Framed-Pool	—	String	Internal use only	No
90	Tunnel-Client-Auth-ID	—	Tagged string	Both	Yes
91	Tunnel-Server-Auth-ID	—	Tagged string	Both	Yes
135	Primary-DNS-Server	—	Ipaddr	Both	No
136	Secondary-DNS-Server	—	Ipaddr	Both	No
187	Multilink-ID	—	Integer	Inbound	No
188	Num-In-Multilink	—	Integer	Inbound	No
190	Pre-Input-Octets	—	Integer	Inbound	No

Table B-7 RADIUS (IETF) Attributes (continued)

Number	Name	Description	Type of Value	Inbound/Outbound	Multiple
191	Pre-Output-Octets	—	Integer	Inbound	No
192	Pre-Input-Packets	—	Integer	Inbound	No
193	Pre-Output-Packets	—	Integer	Inbound	No
194	Maximum-Time	—	Integer	Both	No
195	Disconnect-Cause	—	Integer	Inbound	No
197	Data-Rate	—	Integer	Inbound	No
198	PreSession-Time	—	Integer	Inbound	No
208	PW-Lifetime	—	Integer	Outbound	No
209	IP-Direct	—	Ipaddr	Outbound	No
210	PPP-VJ-Slot-Comp	—	Integer	Outbound	No
218	Assign-IP-pool	—	Integer	Outbound	No
228	Route-IP	—	Integer	Outbound	No
233	Link-Compression	—	Integer	Outbound	No
234	Target-Utils	—	Integer	Outbound	No
235	Maximum-Channels	—	Integer	Outbound	No
242	Data-Filter	—	Ascend filter	Outbound	Yes
243	Call-Filter	—	Ascend filter	Outbound	Yes
244	Idle-Limit	—	Integer	Outbound	No

Microsoft MPPE Dictionary of RADIUS VSAs

ACS supports the Microsoft RADIUS VSAs used for MPPE. The vendor ID for this Microsoft RADIUS Implementation is 311. MPPE is an encryption technology developed by Microsoft to encrypt PPP links. These PPP connections can be via a dial-up line, or over a VPN tunnel such as PPTP. MPPE is supported by several RADIUS network device vendors that ACS supports. The following ACS RADIUS protocols support the Microsoft RADIUS VSAs:

- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX 7.x+

- Ascend
- Cisco Airespace

To control Microsoft MPPE settings for users accessing the network through a Cisco VPN 3000-series concentrator, use the CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) attributes. Settings for CVPN3000-PPTP-Encryption (VSA 20) and CVPN3000-L2TP-Encryption (VSA 21) override Microsoft MPPE RADIUS settings. If either of these attributes is enabled, ACS determines the values to be sent in outbound RADIUS (Microsoft) attributes and sends them along with the RADIUS (Cisco VPN 3000/ASA/PIX 7.x+) attributes, regardless of whether RADIUS (Microsoft) attributes are enabled in the ACS web interface or how those attributes might be configured.

Table B-8 lists the supported MPPE RADIUS VSAs.

Table B-8 Microsoft MPPE RADIUS VSAs

Number	Attribute	Type of Value	Description	Inbound/Outbound	Multiple
1	MS-CHAP-Response	String	—	Inbound	No
2	MS-CHAP-Error	String	—	Outbound	No
3	MS-CHAP-CPW-1	String	—	Inbound	No
4	MS-CHAP-CPW-2	String	—	Inbound	No
5	MS-CHAP-LM-Enc-PW	String	—	Inbound	No
6	MS-CHAP-NT-Enc-PW	String	—	Inbound	No
7	MS-MPPE-Encryption-Policy	Integer	The MS-MPPE-Encryption-Policy attribute signifies whether the use of encryption is allowed or required. If the Policy field is equal to 1 (Encryption-Allowed), you can use any or none of the encryption types specified in the MS-MPPE-Encryption-Types attribute. If the Policy field is equal to 2 (Encryption-Required), you can use any of the encryption types specified in the MS-MPPE-Encryption-Types attribute; but at least one must be used.	Outbound	No
8	MS-MPPE-Encryption-Types	Integer	The MS-MPPE-Encryption-Types attribute signifies the types of encryption available for use with MPPE. It is a four-octet integer that is interpreted as a string of bits.	Outbound	No
10	MS-CHAP-Domain	String	—	Inbound	No
11	MS-CHAP-Challenge	String	—	Inbound	No

Table B-8 Microsoft MPPE RADIUS VSAs (continued)

Number	Attribute	Type of Value	Description	Inbound/Outbound	Multiple
12	MS-CHAP-MPPE-Keys	String	The MS-CHAP-MPPE-Keys attribute contains two session keys for use by the MPPE. This attribute is only included in Access-Accept packets. Note ACS auto generates the MS-CHAP-MPPE-Keys attribute value; there is no value to set in the web interface.	Outbound	No
16	MS-MPPE-Send-Key	String (maximum length 240 characters)	The MS-MPPE-Send-Key attribute contains a session key for use by MPPE. This key is for encrypting packets sent from the AAA client to the remote host. This attribute is only included in Access-Accept packets.	Outbound	No
17	MS-MPPE-Recv-Key	String (maximum length 240 characters)	The MS-MPPE-Recv-Key attribute contains a session key for use by MPPE. This key is for encrypting packets that the AAA client from the remote host receives. This attribute is only included in Access-Accept packets.	Outbound	No
18	MS-RAS-Version	String	—	Inbound	No
25	MS-CHAP-NT-Enc-PW	String	—	Inbound	No
26	MS-CHAP2-Response	String	—	Outbound	No
27	MS-CHAP2-CPW	String	—	Inbound	No

Ascend Dictionary of RADIUS AV Pairs

ACS supports the Ascend RADIUS AV pairs. [Table B-9](#) contains Ascend RADIUS dictionary translations for parsing requests and generating responses. All transactions comprise AV pairs. The value of each attribute is specified as:

- **string**—0-253 octets.
- **abinary**—0-254 octets.
- **ipaddr**—4 octets in network byte order.
- **integer**—32-bit value in big endian order (high byte first).
- **call filter**—Defines a call filter for the profile.



Note RADIUS filters are retrieved only when a call is placed by using a RADIUS outgoing profile or answered by using a RADIUS incoming profile. Filter entries are applied in the order in which they are entered. If you change a filter in an Ascend RADIUS profile, the changes do not take effect until a call uses that profile.

- **date**—32-bit value in big-endian order. For example, seconds since 00:00:00 universal time (UT), January 1, 1970.

- **enum**—Enumerated values are stored in the user file with dictionary value translations for easy administration.

Table B-9 Ascend RADIUS Attributes

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
Dictionary of Ascend Attributes				
1	User-Name	String	Inbound	No
2	User-Password	String	Outbound	No
3	CHAP-Password	String	Outbound	No
4	NAS-IP-Address	Ipaddr	Inbound	No
5	NAS-Port	Integer	Inbound	No
6	Service-Type	Integer	Both	No
7	Framed-Protocol	Integer	Both	No
8	Framed-IP-Address	Ipaddr	Both	No
9	Framed-IP-Netmask	Ipaddr	Outbound	No
10	Framed-Routing	Integer	Outbound	No
11	Framed-Filter	String	Outbound	Yes
12	Framed-MTU	Integer	Outbound	No
13	Framed-Compression	Integer	Outbound	Yes
14	Login-IP-Host	Ipaddr	Both	Yes
15	Login-Service	Integer	Both	No
16	Login-TCP-Port	Integer	Outbound	No
17	Change-Password	String	—	—
18	Reply-Message	String	Outbound	Yes
19	Callback-ID	String	Outbound	No
20	Callback-Name	String	Outbound	No
22	Framed-Route	String	Outbound	Yes
23	Framed-IPX-Network	Integer	Outbound	No
24	State	String	Outbound	No
25	Class	String	Outbound	Yes
26	Vendor-Specific	String	Outbound	Yes
30	Call-Station-ID	String	Inbound	No
31	Calling-Station-ID	String	Inbound	No
40	Acct-Status-Type	Integer	Inbound	No
41	Acct-Delay-Time	Integer	Inbound	No
42	Acct-Input-Octets	Integer	Inbound	No
43	Acct-Output-Octets	Integer	Inbound	No
44	Acct-Session-Id	Integer	Inbound	No

Table B-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
45	Acct-Authentic	Integer	Inbound	No
46	Acct-Session-Time	Integer	Inbound	No
47	Acct-Input-Packets	Integer	Inbound	No
48	Acct-Output-Packets	Integer	Inbound	No
64	Tunnel-Type	String	Both	Yes
65	Tunnel-Medium-Type	String	Both	Yes
66	Tunnel-Client-Endpoint	String (maximum length 250 characters)	Both	Yes
67	Tunnel-Server-Endpoint	String (maximum length 250 characters)	Both	Yes
68	Acct-Tunnel-Connection	Integer (maximum length 253 characters)	Inbound	No
104	Ascend-Private-Route	String (maximum length 253 characters)	Both	No
105	Ascend-Numbering-Plan-ID	Integer (maximum length 10 characters)	Both	No
106	Ascend-FR-Link-Status-Dlci	Integer (maximum length 10 characters)	Both	No
107	Ascend-Calling-Subaddress	String (maximum length 253 characters)	Both	No
108	Ascend-Callback-Delay	String (maximum length 10 characters)	Both	No
109	Ascend-Endpoint-Disc	String (maximum length 253 characters)	Both	No
110	Ascend-Remote-FW	String (maximum length 253 characters)	Both	No
111	Ascend-Multicast-GLeave-Delay	Integer (maximum length 10 characters)	Both	No
112	Ascend-CBCP-Enable	String	Both	No
113	Ascend-CBCP-Mode	String	Both	No
114	Ascend-CBCP-Delay	String (maximum length 10 characters)	Both	No
115	Ascend-CBCP-Trunk-Group	String (maximum length 10 characters)	Both	No
116	Ascend-AppleTalk-Route	String (maximum length 253 characters)	Both	No
117	Ascend-AppleTalk-Peer-Mode	String (maximum length 10 characters)	Both	No
118	Ascend-Route-AppleTalk	String (maximum length 10 characters)	Both	No
119	Ascend-FCP-Parameter	String (maximum length 253 characters)	Both	No
120	Ascend-Modem-PortNo	Integer (maximum length 10 characters)	Inbound	No
121	Ascend-Modem-SlotNo	Integer (maximum length 10 characters)	Inbound	No
122	Ascend-Modem-ShelfNo	Integer (maximum length 10 characters)	Inbound	No
123	Ascend-Call-Attempt-Limit	Integer (maximum length 10 characters)	Both	No
124	Ascend-Call-Block_Duration	Integer (maximum length 10 characters)	Both	No
125	Ascend-Maximum-Call-Duration	Integer (maximum length 10 characters)	Both	No
126	Ascend-Router-Preference	String (maximum length 10 characters)	Both	No
127	Ascend-Tunneling-Protocol	String (maximum length 10 characters)	Both	No
128	Ascend-Shared-Profile-Enable	Integer	Both	No
129	Ascend-Primary-Home-Agent	String (maximum length 253 characters)	Both	No

Table B-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
130	Ascend-Secondary-Home-Agent	String (maximum length 253 characters)	Both	No
131	Ascend-Dialout-Allowed	Integer	Both	No
133	Ascend-BACP-Enable	Integer	Both	No
134	Ascend-DHCP-Maximum-Leases	Integer (maximum length 10 characters)	Both	No
135	Ascend-Client-Primary-DNS	Address (maximum length 15 characters)	Both	No
136	Ascend-Client-Secondary-DNS	Address (maximum length 15 characters)	Both	No
137	Ascend-Client-Assign-DNS	Enum	Both	No
138	Ascend-User-Acct-Type	Enum	Both	No
139	Ascend-User-Acct-Host	Address (maximum length 15 characters)	Both	No
140	Ascend-User-Acct-Port	Integer (maximum length 10 characters)	Both	No
141	Ascend-User-Acct-Key	String (maximum length 253 characters)	Both	No
142	Ascend-User-Acct-Base	Enum (maximum length 10 characters)	Both	No
143	Ascend-User-Acct-Time	Integer (maximum length 10 characters)	Both	No
Support IP Address Allocation from Global Pools				
144	Ascend-Assign-IP-Client	Ipaddr (maximum length 15 characters)	Outbound	No
145	Ascend-Assign-IP-Server	Ipaddr (maximum length 15 characters)	Outbound	No
146	Ascend-Assign-IP-Global-Pool	String (maximum length 253 characters)	Outbound	No
DHCP Server Functions				
147	Ascend-DHCP-Reply	Integer	Outbound	No
148	Ascend-DHCP-Pool-Number	Integer (maximum length 10 characters)	Outbound	No
Connection Profile/Telco Option				
149	Ascend-Expect-Callback	Integer	Outbound	No
Event Type for an Ascend-Event Packet				
150	Ascend-Event-Type	Integer (maximum length 10 characters)	Inbound	No
RADIUS Server Session Key				
151	Ascend-Session-Svr-Key	String (maximum length 253 characters)	Outbound	No
Multicast Rate Limit Per Client				
152	Ascend-Multicast-Rate-Limit	Integer (maximum length 10 characters)	Outbound	No
Connection Profile Fields to Support Interface-Based Routing				
153	Ascend-IF-Netmask	Ipaddr (maximum length 15 characters)	Outbound	No
154	Ascend-Remote-Addr	Ipaddr (maximum length 15 characters)	Outbound	No
Multicast Support				
155	Ascend-Multicast-Client	Integer (maximum length 10 characters)	Outbound	No
Frame Datalink Profiles				
156	Ascend-FR-Circuit-Name	String (maximum length 253 characters)	Outbound	No

Table B-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
157	Ascend-FR-LinkUp	Integer (maximum length 10 characters)	Outbound	No
158	Ascend-FR-Nailed-Group	Integer (maximum length 10 characters)	Outbound	No
159	Ascend-FR-Type	Integer (maximum length 10 characters)	Outbound	No
160	Ascend-FR-Link-Mgt	Integer (maximum length 10 characters)	Outbound	No
161	Ascend-FR-N391	Integer (maximum length 10 characters)	Outbound	No
162	Ascend-FR-DCE-N392	Integer (maximum length 10 characters)	Outbound	No
163	Ascend-FR-DTE-N392	Integer (maximum length 10 characters)	Outbound	No
164	Ascend-FR-DCE-N393	Integer (maximum length 10 characters)	Outbound	No
165	Ascend-FR-DTE-N393	Integer (maximum length 10 characters)	Outbound	No
166	Ascend-FR-T391	Integer (maximum length 10 characters)	Outbound	No
167	Ascend-FR-T392	Integer (maximum length 10 characters)	Outbound	No
168	Ascend-Bridge-Address	String (maximum length 253 characters)	Outbound	No
169	Ascend-TS-Idle-Limit	Integer (maximum length 10 characters)	Outbound	No
170	Ascend-TS-Idle-Mode	Integer (maximum length 10 characters)	Outbound	No
171	Ascend-DBA-Monitor	Integer (maximum length 10 characters)	Outbound	No
172	Ascend-Base-Channel-Count	Integer (maximum length 10 characters)	Outbound	No
173	Ascend-Minimum-Channels	Integer (maximum length 10 characters)	Outbound	No
IPX Static Routes				
174	Ascend-IPX-Route	String (maximum length 253 characters)	Inbound	No
175	Ascend-FT1-Caller	Integer (maximum length 10 characters)	Inbound	No
176	Ascend-Backup	String (maximum length 253 characters)	Inbound	No
177	Ascend-Call-Type	Integer	Inbound	No
178	Ascend-Group	String (maximum length 253 characters)	Inbound	No
179	Ascend-FR-DLCI	Integer (maximum length 10 characters)	Inbound	No
180	Ascend-FR-Profile-Name	String (maximum length 253 characters)	Inbound	No
181	Ascend-Ara-PW	String (maximum length 253 characters)	Inbound	No
182	Ascend-IPX-Node-Addr	String (maximum length 253 characters)	Both	No
183	Ascend-Home-Agent-IP-Addr	Ipaddr (maximum length 15 characters)	Outbound	No
184	Ascend-Home-Agent-Password	String (maximum length 253 characters)	Outbound	No
185	Ascend-Home-Network-Name	String (maximum length 253 characters)	Outbound	No
186	Ascend-Home-Agent-UDP-Port	Integer (maximum length 10 characters)	Outbound	No
187	Ascend-Multilink-ID	Integer	Inbound	No
188	Ascend-Num-In-Multilink	Integer	Inbound	No
189	Ascend-First-Dest	Ipaddr	Inbound	No
190	Ascend-Pre-Input-Octets	Integer	Inbound	No

Table B-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
191	Ascend-Pre-Output-Octets	Integer	Inbound	No
192	Ascend-Pre-Input-Packets	Integer	Inbound	No
193	Ascend-Pre-Output-Packets	Integer	Inbound	No
194	Ascend-Maximum-Time	Integer (maximum length 10 characters)	Both	No
195	Ascend-Disconnect-Cause	Integer	Inbound	No
196	Ascend-Connect-Progress	Integer	Inbound	No
197	Ascend-Data-Rate	Integer	Inbound	No
198	Ascend-PreSession-Time	Integer	Inbound	No
199	Ascend-Token-Idle	Integer (maximum length 10 characters)	Outbound	No
200	Ascend-Token-Immediate	Integer	Outbound	No
201	Ascend-Require-Auth	Integer (maximum length 10 characters)	Outbound	No
202	Ascend-Number-Sessions	String (maximum length 253 characters)	Outbound	No
203	Ascend-Authen-Alias	String (maximum length 253 characters)	Outbound	No
204	Ascend-Token-Expiry	Integer (maximum length 10 characters)	Outbound	No
205	Ascend-Menu-Selector	String (maximum length 253 characters)	Outbound	No
206	Ascend-Menu-Item	String	Outbound	Yes

RADIUS Password Expiration Options

207	Ascend-PW-Warntime	Integer (maximum length 10 characters)	Outbound	No
208	Ascend-PW-Lifetime	Integer (maximum length 10 characters)	Outbound	No
209	Ascend-IP-Direct	Ipaddr (maximum length 15 characters)	Outbound	No
210	Ascend-PPP-VJ-Slot-Comp	Integer (maximum length 10 characters)	Outbound	No
211	Ascend-PPP-VJ-1172	Integer (maximum length 10 characters)	Outbound	No
212	Ascend-PPP-Async-Map	Integer (maximum length 10 characters)	Outbound	No
213	Ascend-Third-Prompt	String (maximum length 253 characters)	Outbound	No
214	Ascend-Send-Secret	String (maximum length 253 characters)	Outbound	No
215	Ascend-Receive-Secret	String (maximum length 253 characters)	Outbound	No
216	Ascend-IPX-Peer-Mode	Integer	Outbound	No
217	Ascend-IP-Pool-Definition	String (maximum length 253 characters)	Outbound	No
218	Ascend-Assign-IP-Pool	Integer	Outbound	No
219	Ascend-FR-Direct	Integer	Outbound	No
220	Ascend-FR-Direct-Profile	String (maximum length 253 characters)	Outbound	No
221	Ascend-FR-Direct-DLCI	Integer (maximum length 10 characters)	Outbound	No
222	Ascend-Handle-IPX	Integer	Outbound	No
223	Ascend-Netware-Timeout	Integer (maximum length 10 characters)	Outbound	No
224	Ascend-IPX-Alias	String (maximum length 253 characters)	Outbound	No

Table B-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
225	Ascend-Metric	Integer (maximum length 10 characters)	Outbound	No
226	Ascend-PRI-Number-Type	Integer	Outbound	No
227	Ascend-Dial-Number	String (maximum length 253 characters)	Outbound	No
Connection Profile/PPP Options				
228	Ascend-Route-IP	Integer	Outbound	No
229	Ascend-Route-IPX	Integer	Outbound	No
230	Ascend-Bridge	Integer	Outbound	No
231	Ascend-Send-Auth	Integer	Outbound	No
232	Ascend-Send-Passwd	String (maximum length 253 characters)	Outbound	No
233	Ascend-Link-Compression	Integer	Outbound	No
234	Ascend-Target-Util	Integer (maximum length 10 characters)	Outbound	No
235	Ascend-Max-Channels	Integer (maximum length 10 characters)	Outbound	No
236	Ascend-Inc-Channel-Count	Integer (maximum length 10 characters)	Outbound	No
237	Ascend-Dec-Channel-Count	Integer (maximum length 10 characters)	Outbound	No
238	Ascend-Seconds-Of-History	Integer (maximum length 10 characters)	Outbound	No
239	Ascend-History-Weigh-Type	Integer	Outbound	No
240	Ascend-Add-Seconds	Integer (maximum length 10 characters)	Outbound	No
241	Ascend-Remove-Seconds	Integer (maximum length 10 characters)	Outbound	No
Connection Profile/Session Options				
242	Ascend-Data-Filter	Call filter	Outbound	Yes
243	Ascend-Call-Filter	Call filter	Outbound	Yes
244	Ascend-Idle-Limit	Integer (maximum length 10 characters)	Outbound	No
245	Ascend-Preempt-Limit	Integer (maximum length 10 characters)	Outbound	No
Connection Profile/Telco Options				
246	Ascend-Callback	Integer	Outbound	No
247	Ascend-Data-Svc	Integer	Outbound	No
248	Ascend-Force-56	Integer	Outbound	No
249	Ascend-Billing-Number	String (maximum length 253 characters)	Outbound	No
250	Ascend-Call-By-Call	Integer (maximum length 10 characters)	Outbound	No
251	Ascend-Transit-Number	String (maximum length 253 characters)	Outbound	No
Terminal Server Attributes				
252	Ascend-Host-Info	String (maximum length 253 characters)	Outbound	No
PPP Local Address Attribute				
253	Ascend-PPP-Address	Ipaddr (maximum length 15 characters)	Outbound	No
MPP Percent Idle Attribute				

Table B-9 Ascend RADIUS Attributes (continued)

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
254	Ascend-MPP-Idle-Percent	Integer (maximum length 10 characters)	Outbound	No
255	Ascend-Xmit-Rate	Integer (maximum length 10 characters)	Outbound	No

Nortel Dictionary of RADIUS VSAs

[Table B-10](#) lists the Nortel RADIUS VSAs supported by ACS. The Nortel vendor ID number is 1584.

Table B-10 Nortel RADIUS VSAs

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
035	Bay-Local-IP-Address	Ipaddr (maximum length 15 characters)	Outbound	No
054	Bay-Primary-DNS-Server	Ipaddr (maximum length 15 characters)	Outbound	No
055	Bay-Secondary-DNS-Server	Ipaddr (maximum length 15 characters)	Outbound	No
056	Bay-Primary-NBNS-Server	Ipaddr (maximum length 15 characters)	Outbound	No
057	Bay-Secondary-NBNS-Server	Ipaddr (maximum length 15 characters)	Outbound	No
100	Bay-User-Level	Integer	Outbound	No
101	Bay-Audit-Level	Integer	Outbound	No

Juniper Dictionary of RADIUS VSAs

[Table B-11](#) lists the Juniper RADIUS VSAs supported by ACS. The Juniper vendor ID number is 2636.

Table B-11 Juniper RADIUS VSAs

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
001	Juniper-Local-User-Name	String (maximum length 247 characters)	Outbound	No
002	Juniper-Allow-Commands	String (maximum length 247 characters)	Outbound	No
003	Juniper-Deny-Commands	String (maximum length 247 characters)	Outbound	No

3COMUSR Dictionary of RADIUS VSAs

[Table B-12](#) lists the 3COMUSR RADIUS VSAs supported by ACS. The 3COMUSR vendor ID number is 429.

Table B-12 3COMUSR RADIUS VSAs

Number	Attribute	Type of Value	Inbound/ Outbound	Multiple
0x6C	Modulation-Type	Integer	IN OUT	No
0x99	Error-Control	Integer	IN OUT	No
0xC7	Compression	Integer	IN OUT	No
0x9015	Call-Tracking-ID	Integer	IN OUT	No
0x9014	MIC	Integer	IN OUT	No
0x9019	Chassis-Call-Slot	Integer	IN OUT	No
0x9023	Connect-Speed	Integer	IN OUT	No
0x901A	Chassis-Call-Span	Integer	IN OUT	No
0x901B	Chassis-Call-Channel	Integer	IN OUT	No
0x901D	Unauthenticated-Time	Integer	IN OUT	No
0x982F	MP-MRRU	Integer	IN OUT	No
0x9841	MP-EDO	Integer	IN OUT	No



APPENDIX C

CSUtil Database Utility



Note

The information in this appendix applies to ACS for Windows.

This appendix details the command-line utility, **CSUtil.exe**, for the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS. Among its several functions, you can use **CSUtil.exe** to add, change, and delete users from a colon-delimited text file. You can also use the utility to add and delete AAA client configurations.



Note

You can accomplish similar tasks by using the ACS System Backup, ACS System Restore, Database Replication, and RDBMS Synchronization features. For more information on these features, see [Chapter 8, “System Configuration: Advanced.”](#)

This chapter contains:

- [Location of CSUtil.exe and Related Files, page C-2](#)
- [CSUtil Command Syntax, page C-2](#)
- [Backing Up ACS with CSUtil.exe, page C-3](#)
- [Restoring ACS with CSUtil.exe, page C-4](#)
- [Initializing the ACS Internal Database, page C-5](#)
- [Creating an ACS Internal Database Dump File, page C-6](#)
- [Loading the ACS Internal Database from a Dump File, page C-7](#)
- [Cleaning up the ACS Internal Database, page C-8](#)
- [User and AAA Client Import Option, page C-9](#)
- [Exporting User List to a Text File, page C-15](#)
- [Exporting Group Information to a Text File, page C-16](#)
- [Decoding Error Numbers, page C-17](#)
- [User-Defined RADIUS Vendors and VSA Sets, page C-17](#)
- [PAC File Generation, page C-26](#)
- [Posture-Validation Attributes, page C-29](#)
- [Adding External Audit Device Type Attributes, page C-40](#)

Location of CSUtil.exe and Related Files

When you install ACS in the default location, **CSUtil.exe** is located in:

```
C:\Program Files\CiscoSecure ACS vX.X\bin
```

where *x.x* is the version of your ACS software. The **CSUtil.exe** tool is located in the *\bin* subdirectory of your ACS installation directory. Files generated by or accessed by **CSUtil.exe** are also located in the *\bin* directory. If you add other files, such as vendor definitions for the ACS dictionary, be sure to put them in the *\bin* directory.

CSUtil Command Syntax

The syntax for the **CSUtil** command is:

```
csutil [-q] [-b backup_filename] [-e number] [-g group_number] [-i file]
[-d [-p secret_key] dump_filename] [-l filename [-passwd secret_key]] [-n]
[-r all|users|config backup_file] [-u] [-listUDV] [-addUDV slot filename.ini]
[-delUDV slot] [-dumpUDV database_dump_filename]
[-t] [-filepath full_filepath] [-passwd password] [-machine]
(-a | -g group_number | -u user_name | -f user_list_filepath)
[-addAVP filepath] [-delAVP vendor_id application_id attribute_id] [-dumpAVP filename]
[-delPropHPP attribute_ID property_ID] [-delEntHPP attribute_ID entity_name]
```

[Table C-1](#) shows the options that you can use with the **CSUtil** command.

Table C-1 CSUtil Options

Syntax	Use to ...
-q	Use Quiet mode. Does not prompt, use before other options.
-b backup_filename	Create a system backup.
-d [-p secret_key] dump_filename	Dump users and groups database to <i>dump.txt</i> or a named file. You should provide a secret key to encrypt user passwords in the dump file.
-e number	Decode error number to ASCII message.
-g group_number	Dump group information only to <i>group.txt</i> .
-i file	Import users or NASs from <i>import.txt</i> or named file.
-p secret_key	Reset password-aging counters during users' and groups' database dump (-d).
-l filename [-passwd secret_key]	Empty the user table, initialize profiles, and load users and groups database from <i>dump.txt</i> or named file. If you used an encrypt key when dumping the information, you must provide a key to decrypt user passwords and other sensitive information in the dump file.
-n	Empty the user table and shared profile components table, initialize user, group, and network access profiles, and create a new database.
-r all users config backup_file	Restore a system backup.
-u	List users by group to <i>users.txt</i> .
-listUDV	List currently installed user defined vendors (UDVs).
-addUDVslot filename.ini	Install user-defined vendor or vendor-specific-attribute (VSA) data from the <i>.ini</i> file.

Table C-1 CSUtil Options (continued)

-delUDV <i>slot</i>	Remove a vendor or VSA.
-dumpUDV <i>database_dump_file</i>	Dump currently installed vendors to the System UDV's folder.
-t -filepath <i>full_filepath</i> -passwd <i>password</i> <i>-machine</i> (-a -g <i>group_number</i> -u <i>user_name</i> -f <i>user_list_filepath</i>)	Generate protected access credentials (PAC) files for use with Extensible Authentication Protocol-Flexible Authentication via Secure Tunnelling (EAP-FAST) clients. You can generate a user PAC or a machine PAC.
-addAVP <i>filename</i>	Add attributes from <i><filename></i> .
-delAVP <i>vendor_id application_id attribute_id</i>	Remove an AVP attribute
-dumpAVP <i>filename</i>	Dump AVP attributes into <i><filename></i>
-delPropHPP <i>attribute_ID property_ID</i>	Remove specific Property from an extended attribute under Cisco:Host.
-delEntHPP <i>attribute_ID entity_name</i>	Remove specific Entity from an extended attribute under Cisco:Host.

**Caution**

Most **CSUtil** options require that you stop the **CSAuth** service. While the **CSAuth** service is stopped, ACS does not authenticate users. To determine if an option requires that you stop **CSAuth**, refer to the detailed topics about the option.

You can combine many of the options in a single use of **CSUtil.exe**. If you are new to using **CSUtil.exe**, we recommend performing only one option at a time, with the exception of those options, such as **-p**, which must be used in conjunction with other options.

Experienced **CSUtil.exe** users might find it useful to combine **CSUtil.exe** options, such as in the following example, which would first import AAA client configurations and then generate a dump of all ACS internal data:

```
CSUtil.exe -i newnases.txt -d
```

Backing Up ACS with CSUtil.exe

You can use the **-b** option to create a system backup of all ACS internal data. The resulting backup file has the same data as the backup files that are produced by the ACS Backup feature found in the web interface. For more information about the ACS Backup feature, see [ACS Backup, page 7-8](#).

**Note**

During the backup, all services are automatically stopped and restarted. No users are authenticated while the backup is occurring.

To back up ACS with **CSUtil.exe**:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).

Step 2 Type:

```
CSUtil.exe -b filename
```

where *filename* is the name of the backup file. Press **Enter**.

CSUtil.exe displays a confirmation prompt.

- Step 3** To confirm that you want to perform a backup and to halt all ACS services during the backup, type **Y** and press **Enter**.

CSUtil.exe generates a complete backup of all ACS internal data, including user accounts and system configuration. This process may take a few minutes.



Note **CSUtil.exe** displays the error message `Backup Failed` when it attempts to back up components of ACS that are empty, such as when no administrator accounts exist. These messages apply only to components that are empty, not to the overall success or failure of the backup.

Restoring ACS with CSUtil.exe

You can use the **-r** option to restore all ACS internal data. The backup file from which you restore ACS can be one generated by the **CSUtil.exe -b** option or by the ACS Backup feature in the web interface.

ACS backup files contain:

- User and group data.
- System configuration.

You can restore user and group data, or system configuration, or both. For more information about the ACS Backup feature, see [ACS Backup, page 7-8](#).



Note During the restoration, all services are automatically stopped and restarted. No users are authenticated while the restoration is occurring.

To restore ACS with **CSUtil.exe**:

- Step 1** On the computer running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).

- Step 2** Perform one of the following:

- To restore all data (user and group data, and system configuration), type:

```
CSUtil.exe -r all filename
```

where *filename* is the name of the backup file.

Press **Enter**.

- To restore only user and group data, type:

```
CSUtil.exe -r users filename
```

where *filename* is the name of the backup file.

Press **Enter**.

- To restore only the system configuration, type:

```
CSUtil.exe -r config filename
```

where *filename* is the name of the backup file.

Press **Enter**.

CSUtil.exe displays a confirmation prompt.

- Step 3** To confirm that you want to perform a restoration and to halt all ACS services during the restoration, type **Y** and press **Enter**.

CSUtil.exe restores the specified portions of your ACS data. This process may take a few minutes.



Note If the backup file is missing a database component, **CSUtil.exe** displays an error message. Such an error message applies only to the restoration of the missing component. The absence of a database component in a backup is usually intentional and indicates that the component was empty in ACS at the time the backup was created.

Initializing the ACS Internal Database

You can use the **-n** option to initialize the ACS internal database. The **-n** option empties the user table and shared profile components table, and initializes user, group, and network access profiles.



Note Using the **-n** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.



Caution Using the **-n** option erases all user information in the ACS internal database. Unless you have a current backup or dump of your ACS internal database, all user accounts are lost when you use this option.

To create an ACS internal database:

- Step 1** If you have not performed a backup or dump of the ACS internal database, do so now before proceeding. For more information about backing up the database, see [Backing Up ACS with CSUtil.exe, page C-3](#).
- Step 2** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).
- Step 3** If the **CSAuth** service is running, type:
- ```
net stop csauth
```
- Press **Enter**.
- The **CSAuth** service stops.
- Step 4** Type:
- ```
CSUtil.exe -n
```
- Press **Enter**.
- CSUtil.exe** displays a confirmation prompt.
- Step 5** To confirm that you want to initialize the ACS internal database, type **Y** and press **Enter**.
- The ACS internal database is initialized. This process may take a few minutes.
- Step 6** To resume user authentication, type:

```
net start csauth
```

Press **Enter**.

Creating an ACS Internal Database Dump File

You can use the **-d** option to dump all contents of the ACS internal database into a password-protected text file. You can provide a name for the file; otherwise, it is called *dump.txt*. The dump file provides a thorough and compressible backup of all ACS internal data.

Using the **-l** option, you can reload the ACS internal data from a dump file created by the **-d** option. For more information about the **-l** option, see [Loading the ACS Internal Database from a Dump File, page C-7](#).



Note

Using the **-d** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To dump all ACS internal data into a text file:

- Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).
 - Step 2 If the **CSAuth** service is running, type:

```
net stop csauth
```

 Press **Enter**.
 The **CSAuth** service stops.
 - Step 3 To dump to the default *dump.txt* file, type:

```
CSUtil.exe -d -p secret_key
```

 Press **Enter**.
CSUtil.exe displays a confirmation prompt.
 - Step 4 To dump to a named file, type:

```
CSUtil.exe -d -p secret_key dump_filename
```

 Press **Enter**.
CSUtil.exe displays a confirmation prompt.
 - Step 5 To confirm that you want to dump all ACS internal data into a text file, type **Y** and press **Enter**.
CSUtil.exe creates the dump text file. This process may take a few minutes.
 - Step 6 To resume user authentication, type:

```
net start csauth
```

 Press **Enter**.
-

Loading the ACS Internal Database from a Dump File

You can use the **-l** option to overwrite all ACS internal data from a dump text file. This option replaces the existing all ACS internal data with the data in the dump text file. In effect, the **-l** option initializes all ACS internal data before loading it from the dump text file. Dump text files are created by using the **-d** option. You must use the same password used to encrypt the dump files.

You can use the **-p** option in conjunction with the **-l** option to reset password-aging counters.



Note

Using the **-l** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To load all ACS internal data from a text file:

- Step 1** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files](#), page C-2.
- Step 2** If the **CSAuth** service is running, type:
net stop csauth
 Press **Enter**.
 The **CSAuth** service stops.
- Step 3** To load from the default *dump.txt* file, type:
CSUtil.exe -l -passwd secret_key
 where *secret_key* is the same password that was used to encrypt the dump text file. Press **Enter**.
- Step 4** To load from a named dump file and reset password-aging counters, type:
CSUtil.exe -p -l filename -passwd secret_key
 where *filename* is the name of the dump file that you want **CSUtil.exe** to use to load ACS internal data. *secret_key* is the same password that was used to encrypt the *dump.txt* file.



Note

You must enter **-p** before **-l** as shown in the command line example; otherwise, this operation will not work.

Press **Enter**.

CSUtil.exe displays a confirmation prompt for overwriting all ACS internal data with the data in the dump text file.



Note

Overwriting the database does not preserve any data; instead, after the overwrite, the database contains only what is specified in the dump text file.

- Step 5** To confirm that you want to replace all ACS internal data, type **Y** and press **Enter**.
CSUtil.exe initializes all ACS internal data, and then loads ACS with the information in the dump file specified. This process may take a few minutes.
- Step 6** To resume user authentication, type:
net start csauth

Press **Enter**.

Cleaning up the ACS Internal Database

Like many relational databases, the ACS internal database marks deleted records as deleted; but does not remove the records from the database. You can clean up the ACS internal database and remove all records marked for deletion by using the following **CSUtil.exe** options:

- **-d**—Export all ACS internal data to a text file, named *dump.txt*.
- **-n**—Create an ACS internal database and index.
- **-l**—Load all ACS internal data from the *dump.txt* file.

Additionally, if you want to automate this process, consider using the **-q** option to suppress the confirmation prompts that otherwise appear before **CSUtil.exe** performs the **-n** and **-l** options. This process does not necessarily reduce the size of the database.



Note

Cleaning up the ACS internal database requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To clean up the ACS internal database:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).

Step 2 If the **CSAuth** service is running, type:

```
net stop csauth
```

Press **Enter**.

The **CSAuth** service stops.

Step 3 Type:

```
CSUtil.exe -d -n -l
```

Press **Enter**.



Tip

If you include the **-q** option in the command, **CSUtil** does not prompt you for confirmation of initializing or loading the database.

If you do not use the **-q** option, **CSUtil.exe** displays a confirmation prompt for initializing the database and then for loading the database. For more information about the effects of the **-n** option, see [Initializing the ACS Internal Database, page C-5](#). For more information about the effects of the **-l** option, see [Loading the ACS Internal Database from a Dump File, page C-7](#).

Step 4 For each confirmation prompt that appears, type **Y** and press **Enter**.

CSUtil.exe dumps all ACS internal data to *dump.txt*, initializes the ACS internal database, and reloads all ACS internal data from *dump.txt*. This process may take a few minutes.

Step 5 To resume user authentication, type:

net start csauth

Press **Enter**.

User and AAA Client Import Option

You can use the **-i** option to update ACS with data from a colon-delimited text file. You can also update AAA client definitions.

For user accounts, you can add users, change user information such as passwords, or delete users. For AAA client definitions, you can add or delete AAA clients.

This section contains:

- [Importing User and AAA Client Information, page C-9](#)
- [User and AAA Client Import File Format, page C-10](#)
 - [About User and AAA Client Import File Format, page C-10](#)
 - [ONLINE or OFFLINE Statement, page C-11](#)
 - [ADD Statements, page C-11](#)
 - [UPDATE Statements, page C-12](#)
 - [DELETE Statements, page C-13](#)
 - [ADD_NAS Statements, page C-14](#)
 - [DEL_NAS Statements, page C-15](#)
 - [Import File Example, page C-15](#)

Importing User and AAA Client Information

To import user or AAA client information:

-
- | | |
|---------------|---|
| Step 1 | If you have not performed a backup or dump of ACS, do so now before proceeding. For more information about backing up the database, see Backing Up ACS with CSUtil.exe, page C-3 . |
| Step 2 | Create an import text file. For more information about what an import text file can or must contain, see User and AAA Client Import File Format, page C-10 . |
| Step 3 | Copy or move the import text file to the same directory as CSUtil.exe . For more information about the location of CSUtil.exe , see Location of CSUtil.exe and Related Files, page C-2 . |
| Step 4 | On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing CSUtil.exe . |
| Step 5 | Type:

<pre>CSUtil.exe -i filename</pre> where <i>filename</i> is the name of the import text file you want CSUtil.exe to use to update ACS. Press Enter .

CSUtil.exe displays a confirmation prompt for updating the database. |

Step 6 To confirm that you want to update ACS with the information from the import text file specified, type **Y** and press **Enter**.

ACS is updated with the information in the import text file specified. This process may take a few minutes.

If the import text file contained AAA client configuration data, **CSUtil.exe** warns you that you must restart CSTacacs and CSRADIUS for these changes to take effect.

Step 7 To restart CSRADIUS:

a. Type:

net stop csradius

Press **Enter**. The CSRADIUS service stops.

b. To start CSRADIUS, type:

net start csradius

Press **Enter**.

Step 8 To restart CSTACACS:

a. Type:

net stop cstacacs

Press **Enter**. The CSTACACS service stops.

b. To start CSTACACS, type:

net start cstacacs

Press **Enter**.

User and AAA Client Import File Format

This section contains:

- [About User and AAA Client Import File Format, page C-10](#)
- [ONLINE or OFFLINE Statement, page C-11](#)
- [ADD Statements, page C-11](#)
- [UPDATE Statements, page C-12](#)
- [DELETE Statements, page C-13](#)
- [ADD_NAS Statements, page C-14](#)
- [DEL_NAS Statements, page C-15](#)
- [Import File Example, page C-15](#)

About User and AAA Client Import File Format

The import file can contain six different line types, as discussed in following topics. The first line of the import file must be one of the tokens defined in [Table C-2](#).

Each line of a **CSUtil.exe** import file is a series of colon-separated tokens. Some of the tokens are followed by values. Values, like tokens, are colon-delimited. For tokens that require values, **CSUtil.exe** expects the value of the token to be in the colon-delimited field immediately following the token.

**Note**

There are no password character limitations in the ACS user interface, or when using the **CSUtil.exe** to import passwords.

ONLINE or OFFLINE Statement

CSUtil.exe requires an **ONLINE** or **OFFLINE** token in an import text file. The file must begin with a line that contains only an **ONLINE** or **OFFLINE** token. The **ONLINE** and **OFFLINE** tokens are described in [Table C-2](#).

Table C-2 *ONLINE/OFFLINE Statement Tokens*

Token	Required	Value Required	Description
ONLINE	ONLINE or OFFLINE must be present	—	The CSAuth service remains active while CSUtil.exe imports the text file. CSUtil.exe performance is slower when run in this mode, but ACS continues to authenticate users during the import.
OFFLINE	ONLINE or OFFLINE must be present	—	The CSAuth service is stopped while CSUtil.exe imports the text file. Although CSUtil.exe performance is fastest in this mode, no users are authenticated during the import. If you need to import a large amount of user information quickly, consider using the OFFLINE token. While performing an import in the OFFLINE mode stops authentication during the import, the import is much faster. For example, importing 100,000 users in the OFFLINE mode takes less than one minute.

ADD Statements

ADD statements are optional. Only the **ADD** token and its value are required to add a user to ACS. [Table C-3](#) lists the valid tokens for **ADD** statements.

**Note**

CSUtil.exe provides no means to specify a particular instance of an external user database type. If an external user database authenticates a user and ACS has multiple instances of the specified database type, **CSUtil.exe** assigns the user to the first instance of that database type. For example, if ACS has two LDAP external user databases configured, **CSUtil.exe** creates the user record and assigns the user to the LDAP database that was added to ACS first.

Table C-3 ADD Statement Tokens

Token	Required	Value Required	Description
ADD	Yes	username	Add user information to ACS. If the username already exists, no information is changed.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name. If you do not use the PROFILE token or fail to provide a group number, the user is added to the default group.
CHAP	No	CHAP password	Require a Challenge Authentication Handshake Protocol (CHAP) password for authentication.
CSDB	No	password	Authenticate the username with the ACS internal database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the ACS internal database, using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows external user database.
EXT_SDI	No	—	Authenticate the username with an RSA external user database.
EXT_ODBC	No	—	Authenticate the username with an Open Database Connectivity (ODBC) external user database.
EXT_LDAP	No	—	Authenticate the username with a generic Lightweight Directory Access Protocol (LDAP) external user database.
EXT_LEAP	No	—	Authenticate the username with a Lightweight and Efficient Application Protocol (LEAP) proxy Remote Access Dial-In User Service (RADIUS) server external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following **ADD** statement would create an account with the username *John*, assign it to Group 3, and specify that *John* should be authenticated by the ACS internal database with the password **closedmondays**:

ADD:John:PROFILE:3:CSDB:closedmondays

UPDATE Statements

UPDATE statements are optional. They make changes to existing user accounts. Only the UPDATE token and its value are required by **CSUtil.exe**, but if no other tokens are included, no changes are made to the user account. You can use the UPDATE statement to update the group that a user is assigned to or to update which database ACS uses to authenticate the user.

Table C-4 lists the valid tokens for UPDATE statements.

Table C-4 UPDATE Statement Tokens

Token	Required	Value Required	Description
UPDATE	Yes	username	Update user information to ACS.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name. Note If you do not specify a database token, such as CSDB or EXT_NT, updating a group assignment may erase a user's password.
CHAP	No	CHAP password	Require a CHAP password for authentication.
CSDB	No	password	Authenticate the username with the ACS internal database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the ACS internal database by using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows external user database.
EXT_ODBC	No	—	Authenticate the username with an ODBC external user database.
EXT_LDAP	No	—	Authenticate the username with a generic LDAP external user database.
EXT_LEAP	No	—	Authenticate the username with a LEAP proxy RADIUS server external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following UPDATE statement causes **CSUtil.exe** to update the account with username *John*, assign it to Group 50, specify that *John* should be authenticated by a UNIX-encrypted password, with a separate CHAP password **goodoldchap**:

```
UPDATE:John:PROFILE:50:CSDB_UNIX:3A13qf9:CHAP:goodoldchap
```

DELETE Statements

DELETE statements are optional. The DELETE token and its value are required to delete a user account from ACS. The DELETE token, detailed in [Table C-5](#), is the only token in a DELETE statement.

Table C-5 UPDATE Statement Tokens

Token	Required	Value Required	Description
DELETE	Yes	username	The name of the user account to delete.

For example, the following DELETE statement causes **CSUtil.exe** to permanently remove the account with username *John* from the ACS internal database:

```
DELETE:John
```

ADD_NAS Statements

ADD_NAS statements are optional. The **ADD_NAS**, **IP**, **KEY**, and **VENDOR** tokens and their values are required to add a AAA client definition to ACS.

[Table C-6](#) lists the valid tokens for ADD_NAS statements.

Table C-6 ADD_NAS Statement Tokens

Token	Required	Value Required	Description
ADD_NAS	Yes	AAA client name	The name of the AAA client to add.
IP	Yes	IP address	The IP address of the AAA client being added. Use a pipe () between IP addresses to import devices with multiple IPs.
KEY	Yes	Shared secret	The shared secret for the AAA client.
VENDOR	Yes	See description	<p>The authentication protocol that the AAA client uses. For RADIUS, this includes the VSA.</p> <p>Note The following values are valid. Quotation marks ("") are required, due to the spaces in the protocol names.</p> <ul style="list-style-type: none"> • "TACACS+ (Cisco IOS)" • "RADIUS (Cisco Aironet)" • "RADIUS (Cisco Airespace)" • "RADIUS (Cisco BBSM)" • "RADIUS (Cisco IOS/PIX 6.x)" • "RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)" • "RADIUS (Cisco VPN 5000)" • "RADIUS (IETF)" • "RADIUS (Ascend)" • "RADIUS (Juniper)" • "RADIUS (Nortel)" • "RADIUS (iPass)" • "RADIUS (3COMUSR)"
NDG	No	NDG name	The name of the Network Device Group to which to add the AAA client.
SINGLE_CON	No	Y or N	For AAA clients using TACACS+ only, the value set for this TOKEN specifies whether the Single Connect TACACS+ AAA Client option is enabled. For more information, see Adding AAA Clients, page 3-12 .
KEEPALIVE	No	Y or N	For AAA clients that are using TACACS+ only, the value set for this token specifies whether the Log Update or Watchdog Packets from this Access Server option is enabled. For more information, see Adding AAA Clients, page 3-12 .

For example, the following **ADD_NAS** statement causes **CSUtil.exe** to add the AAA client with the name **SVR2-T+**, using TACACS+ with the single connection and keep alive packet options enabled:

ADD_NAS:SVR2-T+:IP:IP address:KEY:shared secret:VENDOR:"TACACS+ (Cisco IOS)":NDG:"East Coast":SINGLE_CON:Y:KEEPALIVE:Y

DEL_NAS Statements

DEL_NAS statements are optional. The **DEL_NAS** token, detailed in [Table C-7](#), is the only token in a **DEL_NAS** statement. **DEL_NAS** statements delete AAA client definitions from ACS.

Table C-7 *DEL_NAS Statement Tokens*

Token	Required	Value Required	Description
DEL_NAS	Yes	AAA client name	The name of the AAA client to delete.

For example, the following **DEL_NAS** statement causes **CSUtil.exe** to delete a AAA client with the name **SVR2-T+**:

DEL_NAS:SVR2-T+

Import File Example

An example of the import text file is:

```
OFFLINE
ADD:user01:CSDB:userpassword:PROFILE:1
ADD:user02:EXT_NT:PROFILE:2
ADD:chapuser:CSDB:hello:CHAP:chappw:PROFILE:3
ADD:mary:EXT_NT:CHAP:achappassword
ADD:joe:EXT_SDI
ADD:vanessa:CSDB:vanessaspasword
ADD:juan:CSDB_UNIX:unixpassword
UPDATE:foobar:PROFILE:10
DELETE:paul
ADD_NAS:SVR2-T+:IP:209.165.202.136:KEY:A87il032bzig:VENDOR:"TACACS+ (Cisco IOS)":NDG:"East Coast"
DEL_NAS:SVR16-RAD
```

Exporting User List to a Text File

You can use the **-u** option to export a list of all users in the ACS internal database to a text file named *users.txt*. The *users.txt* file organizes users by group. Within each group, users are listed in the order that their user accounts were created in the ACS internal database. For example, if accounts were created for *Pat*, *Dana*, and *Lloyd*, in that order, *users.txt* lists them in that order as well; rather than alphabetically.



Note

Using the **-u** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

To export user information from the ACS internal database into a text file:

-
- Step 1** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).
- Step 2** If the **CSAuth** service is running, type:
- ```
net stop csauth
```
- Press **Enter**.
- The **CSAuth** service stops.
- Step 3** Type:
- ```
CSUtil.exe -u
```
- Press **Enter**.
- CSUtil.exe** exports information for all users in the ACS internal database to a file named *users.txt*.
- Step 4** To resume user authentication, type:
- ```
net start csauth
```
- Press **Enter**.
- 

## Exporting Group Information to a Text File

You can use the **-g** option to export group configuration data, including shared profile components, from the ACS internal database to a text file named *groups.txt*. The *groups.txt* file is useful primarily for debugging purposes while working with the TAC.



### Note

Using the **-g** option requires that you stop the **CSAuth** service. While **CSAuth** is stopped, no users are authenticated.

---

To export group information from the ACS internal database to a text file:

- 
- Step 1** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).
- Step 2** If the **CSAuth** service is running, type:
- ```
net stop csauth
```
- Press **Enter**.
- The **CSAuth** service stops.
- Step 3** Type:
- ```
CSUtil.exe -g
```
- Press **Enter**.
- CSUtil.exe** exports information for all groups in the ACS internal database to a file named *groups.txt*.
- Step 4** To resume user authentication, type:
-

```
net start csauth
```

Press **Enter**.

## Decoding Error Numbers

You can use the **-e** option to decode error numbers in ACS service logs. These error codes are internal to ACS. For example, the CSRadius log could contain a message similar to:

```
CSRadius/Logs/RDS.log:RDS 05/22/2001 10:09:02 E 2152 4756 Error -1087 authenticating geddy
- no NAS response sent
```

In this example, the error code number that you could use **CSUtil.exe** to decode is -1087:

```
C:\Program Files\CiscoSecure ACS vX.X\Utils: CSUtil.exe -e -1087
CSUtil v3.0(1.14), Copyright 1997-2001, Cisco Systems Inc
Code -1087 : External database reported error during authentication
```



### Note

The **-e** option applies to ACS internal error codes only; not to Windows error codes that are sometimes captured in ACS logs, such as when Windows authentication fails.

For more information about ACS service logs, see [Service Logs, page 10-12](#).

To decode an error number from an ACS service log:

**Step 1** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).

**Step 2** Type:

```
CSUtil.exe -e -number
```

where *number* is the error number in the ACS service log.

Press **Enter**.



**Note** The hyphen (-) before *number* is required.

**CSUtil.exe** displays the text message that is equivalent to the error number specified.

## User-Defined RADIUS Vendors and VSA Sets

This section provides information and procedures about user-defined RADIUS vendors and VSAs.

This section contains:

- [About User-Defined RADIUS Vendors and VSA Sets, page C-18](#)
- [Adding a Custom RADIUS Vendor and VSA Set, page C-18](#)

- [Deleting a Custom RADIUS Vendor and VSA Set, page C-20](#)
- [Listing Custom RADIUS Vendors, page C-21](#)
- [Exporting Custom RADIUS Vendor and VSA Sets, page C-21](#)
- [RADIUS Vendor/VSA Import File, page C-22](#)

## About User-Defined RADIUS Vendors and VSA Sets

In addition to supporting a set of predefined RADIUS vendors and VSAs, ACS supports RADIUS vendors and VSAs that you define. We recommend that you use RDBMS Synchronization to add and configure custom RADIUS vendors; however, you can use **CSUtil.exe** to accomplish the same custom RADIUS vendor and VSA configurations that you can accomplish by using RDBMS Synchronization. Custom RADIUS vendor and VSA configurations that you create by using RDBMS Synchronization or **CSUtil.exe** can be modified by the other feature. Choosing one feature for configuring custom RADIUS vendors and VSAs does not preclude using the other feature. For more information about RDBMS Synchronization, see [RDBMS Synchronization, page 8-17](#).

Vendors that you add must be Internet Engineering Task Force (IETF)-compliant; therefore, all VSAs that you add must be subattributes of IETF RADIUS attribute number 26. You can define up to ten custom RADIUS vendors, numbered zero (0) through 9. **CSUtil.exe** allows only one instance of any given vendor, as defined by the unique vendor IETF ID number and the vendor name.



### Note

If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary ACSs, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy. For more information about database replication, see [ACS Internal Database Replication, page 8-1](#).

## Adding a Custom RADIUS Vendor and VSA Set

You can use the **-addUDV** option to add up to ten custom RADIUS vendors and VSA sets to ACS. Each RADIUS vendor and VSA set is added to one of ten possible user-defined RADIUS vendor slots.



### Note

While **CSUtil.exe** adds a custom RADIUS vendor and VSA set to ACS, all ACS services are automatically stopped and restarted. No users are authenticated during this process.

### Before You Begin

- Define a custom RADIUS vendor and VSA set in a RADIUS vendor/VSA import file. For more information, see [RADIUS Vendor/VSA Import File, page C-22](#).
- Determine the RADIUS vendor slot to which you want to add the new RADIUS vendor and VSAs. For more information, see [Listing Custom RADIUS Vendors, page C-21](#).

To add a custom RADIUS VSA to ACS:

- Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).
- Step 2 Type:

```
CSUtil.exe -addUDV slot-number filename
```

where *slot-number* is an unused ACS RADIUS vendor slot and *filename* is the name of a RADIUS vendor/VSA import file. The *filename* can include a relative or absolute path to the RADIUS vendor/VSA import file. Press **Enter**.

For example, to add the RADIUS vendor defined in `d:\acs\myvsa.ini` to slot 5, use the command:

```
CSUtil.exe -addUDV 5 d:\acs\myvsa.ini
```

**CSUtil.exe** displays a confirmation prompt.

- Step 3** To confirm that you want to add the RADIUS vendor and halt all ACS services during the process, type **Y** and press **Enter**.

**CSUtil.exe** halts ACS services, parses the vendor/VSA input file, and adds the new RADIUS vendor and VSAs to ACS. This process may take a few minutes. After it is complete, **CSUtil.exe** restarts ACS services.



**Note** We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the `\Utils` directory, where **CSUtil.exe** is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

## Support for User-Defined Vendors Extended VSA ID

ACS VSA ID lengths were restricted to one byte, the default value, and the VSA ID value could not be greater than 255. This release supports VSA ID lengths of 1, 2, or 4 bytes. In addition, you can specify whether the VSA has an internal length field or not.

Use **CSUtil** or **RDBMS Synchronization** to install dictionary components for vendors that require extended VSA ID length. For more information on how to configure ACS to use extended VSA IDs, see [Using the RDBMS Synchronization Action Codes to Install User-Defined Vendor or VSA Data](#), page E-27.

## Using the CSUtil.ini file to Install User-Defined Vendor or VSA Data

Use the **CSUtil -addUDV** option with the vendor *.ini* file to install VSA data for vendors that require extended VSA ID length. [Table 8](#) contains two additional codes and definitions in the vendor *.ini* file used to modify the vendor configuration.

**Table 8** CSUtil.ini file Options and Definitions for Vendor Configuration

| Option               | Value            | Description                                                                                             |
|----------------------|------------------|---------------------------------------------------------------------------------------------------------|
| Need Internal Length | TRUE or FALSE    | Sets the presence of Internal Length field in VSA. If not used, then the default is TRUE.               |
| ID Length            | 1, 2 or 4 bytes. | Sets the Vendor-Specific Attribute (VSA) Type length in bytes. If not used, then the default is 1 byte. |

**Note**

ACS supports hex-numbering for the VSA ID feature. Values starting with **0x** are assumed to be hex values.

Use the following sample format of the vendor *.ini* file for setting the ID length and VSA values. In this example the,

- Need Internal Length value is TRUE.
- ID Length is two bytes.
- vendor VSA ID values are 264 and 0x109.

```
[User Defined Vendor]
Name=vendor-name
IETF Code=vendor-IETF-code
Need Internal Length = TRUE
ID Length=2
VSA 264=Ascend-Max-RTP-Delay
VSA 0x109= Ascend-RTP-Port-Range

[Ascend-Max-RTP-Delay]
Type=INTEGER
Profile=OUT

[Ascend-RTP-Port-Range]
Type=STRING
Profile=OUT
```

## Deleting a Custom RADIUS Vendor and VSA Set

You can use the **-delUDV** option to delete a custom RADIUS vendor from ACS.

**Note**

While **CSUtil.exe** deletes a custom RADIUS vendor from ACS, all ACS services are automatically stopped and restarted. No users are authenticated while this process is occurring.

### Before You Begin

Verify that, in the Network Configuration section of the ACS web interface, no AAA client uses the RADIUS vendor. For more information about configuring AAA clients, see [Configuring AAA Clients, page 3-8](#).

Verify that your RADIUS accounting log does not contain attributes from the RADIUS vendor that you want to delete. For more information about configuring your RADIUS accounting log, see [Configuring ACS Logs, page 10-22](#).

To delete a custom RADIUS vendor and VSA set from ACS:

**Step 1**

On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).



- Step 2** Type:
- ```
CSUtil.exe -delUDV slot-number
```
- where *slot-number* is the slot containing the RADIUS vendor that you want to delete.
- Press **Enter**.



Note For more information about determining what RADIUS vendor a particular slot contains, see [Listing Custom RADIUS Vendors, page C-21](#).

CSUtil.exe displays a confirmation prompt.

- Step 3** To confirm that you want to halt all ACS services while deleting the custom RADIUS vendor and VSAs, type **Y** and press **Enter**.

CSUtil.exe displays a second confirmation prompt.

- Step 4** To confirm that you want to delete the RADIUS vendor, type **Y** and press **Enter**.

CSUtil.exe halts ACS services, deletes the specified RADIUS vendor from ACS. This process may take a few minutes. After it is complete, **CSUtil.exe** restarts ACS services.

Listing Custom RADIUS Vendors

You can use the **-listUDV** option to determine what custom RADIUS vendors are defined in ACS. You also use this option to determine which of the ten possible custom RADIUS vendor slots are in use and which RADIUS vendor occupies each used slot.

To list all custom RADIUS vendors that are defined in ACS:

- Step 1** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).

- Step 2** Type:

```
CSUtil.exe -listUDV
```

Press **Enter**.

CSUtil.exe lists each user-defined RADIUS vendor slot in slot number order. **CSUtil.exe** lists slots that do not contain a custom RADIUS vendor as **Unassigned**. An unassigned slot is empty. You can add a custom RADIUS vendor to any slot listed as **Unassigned**.

Exporting Custom RADIUS Vendor and VSA Sets

You can export all custom RADIUS vendor and VSA sets to files. Each vendor and VSA set is saved to a separate file. The files that this option creates are in the same format as RADIUS vendor/VSA import files. This option is particularly useful if you need to modify a custom RADIUS vendor and VSA set, and you have misplaced the original file that was used to import the set.

**Note**

Exporting a custom RADIUS vendor and VSA set does not remove the vendor and VSA set from ACS.

ACS places all exported vendor/VSA files in a subdirectory of the directory containing **CSUtil.exe**. The subdirectory is named `system UDV's`. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).

Each exported vendor/VSA file is named `UDV_n.ini`, where *n* is the slot number that the current custom RADIUS vendor currently occupies and VSA set. For example, if vendor Widget occupies slot 4, the exported file that **CSUtil.exe** creates is `UDV_4.ini`.

To export custom RADIUS vendor and VSA sets to files:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**. For more information about the location of **CSUtil.exe**, see [Location of CSUtil.exe and Related Files, page C-2](#).

Step 2 Type:

```
CSUtil.exe -dumpUDV
```

Press **Enter**.

For each custom RADIUS vendor and VSA set that is currently configured in ACS, **CSUtil.exe** writes a file in the `\System UDV's` subdirectory.

RADIUS Vendor/VSA Import File

To import a custom RADIUS vendor and VSA set into ACS, you must define the RADIUS vendor and VSA set in an import file. This section details the format and content of RADIUS VSA import files.

We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the `\Utils` directory, where **CSUtil.exe** is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

This section contains:

- [About the RADIUS Vendor/VSA Import File, page C-22](#)
- [Vendor and VSA Set Definition, page C-23](#)
- [Attribute Definition, page C-23](#)
- [Enumeration Definition, page C-24](#)
- [Example RADIUS Vendor/VSA Import File, page C-25](#)

About the RADIUS Vendor/VSA Import File

RADIUS Vendor/VSA import files use a Windows `.ini` file format. Each RADIUS vendor/VSA import file comprises three types of sections, detailed in [Table C-9](#). Each section comprises a section header, and a set of keys and values. The order of the sections in the RADIUS vendor/VSA import file is irrelevant.

Table C-9 *RADIUS VSA Import File Section Types*

Section	Required	Number	Description
Vendor and VSA set definition	Yes	1	Defines the RADIUS vendor and VSA set. For more information, see Vendor and VSA Set Definition, page C-23 .
Attribute definition	Yes	1 to 255	Defines a single attribute of the VSA set. For more information, see Attribute Definition, page C-23 .
Enumeration	No	0 to 255	Defines enumerations for attributes with integer data types. For more information, see Enumeration Definition, page C-24 .

Vendor and VSA Set Definition

Each RADIUS vendor/VSA import file must have one vendor and VSA set section. The section header must be [User Defined Vendor]. [Table C-10](#) lists valid keys for the vendor and VSA set section.

Table C-10 *Vendor and VSA Set Keys*

Keys	Required	Value Required	Description
Name	Yes	Vendor name	The name of the RADIUS vendor.
IETF Code	Yes	An integer	The IETF-assigned vendor number for this vendor.
VSA <i>n</i> (where <i>n</i> is the VSA number)	Yes—you can define 1 to 255 VSAs	Attribute name	<p>The name of a VSA. For each VSA named here, the file must contain a corresponding attribute definition section.</p> <p>Note Attribute names must be unique within the RADIUS vendor/VSA import file, and within the set of all RADIUS attributes in ACS. To facilitate unique names, we recommend that you prefix the vendor name to each attribute name, such as <code>widget-encryption</code> for an encryption-related attribute for the vendor Widget. This naming convention also makes accounting logs easier to understand.</p>

For example, the following vendor and VSA set section defines the vendor `widget`, whose IETF-assigned vendor number is 9999. Vendor Widget has 4 VSAs (thus requiring 4 attribute definition sections):

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
```

Attribute Definition

Each RADIUS vendor/VSA import file must have one attribute definition section for each attribute that is defined in the vendor and VSA set section. The section header of each attribute definition section must match the attribute name that is defined for that attribute in the vendor and VSA set section. [Table C-10](#) lists the valid keys for an attribute-definition section.

Table C-11 Attribute Definition Keys

Keys	Required	Value Required	Description
Type	Yes	See description	<p>The data type of the attribute. It must be one of:</p> <ul style="list-style-type: none"> • STRING • INTEGER • IPADDR <p>If the attribute is an integer, the Enums key is valid.</p>
Profile	Yes	See description	<p>The attribute profile defines if the attribute is used for authorization or accounting, or both. The Profile key definition must contain at least one of these values:</p> <ul style="list-style-type: none"> • IN—The attribute is used for accounting. After you add the attribute to ACS, you can configure your RADIUS accounting log to record the new attribute. For more information about RADIUS accounting logs, see AAA-Related Logs, page 10-1. • OUT—The attribute is used for authorization. <p>In addition, you can use the value MULTI to allow several instances of the attribute per RADIUS message.</p> <p>Combinations are valid. For example:</p> <p>Profile=MULTI OUT</p> <p>or</p> <p>Profile=IN OUT</p>
Enums	No (only valid when the TYPE value is INTEGER)	Enumeration section name	<p>The name of the enumeration section.</p> <p>Note Several attributes can reference the same enumeration section. For more information, see Enumeration Definition, page C-24.</p>

For example, the following attribute definition section defines the widget-encryption VSA, which is an integer used for authorization, and for which enumerations exist in the Encryption-Types enumeration section:

```
[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types
```

Enumeration Definition

You can use enumeration definitions to associate a text-based name for each valid numeric value of an integer-type attribute. In the Group Setup and User Setup sections of the ACS web interface, the text values that you define appear in lists that are associated with the attributes that use the enumerations. Enumeration definition sections are required only if an attribute definition section references them. Only attributes that are integer-type can reference an enumeration definition section.

The section header of each enumeration definition must match the value of an Enums key that references it. More than one **Enums** key can reference an enumeration definition section; thus, allowing for reuse of common enumeration definitions. An enumeration definition section can have up to 1000 keys.

Table C-12 lists the valid keys for an enumeration definition section.

Table C-12 Enumerations Definition Keys

Keys	Required	Value Required	Description
<i>n</i> (See description.)	Yes	String	<p>For each valid integer value of the corresponding attribute, an enumerations section must have one key.</p> <p>Each key defines a string value that is associated with an integer value. ACS uses these string values in the web interface.</p> <p>For example, if 0 through 4 are valid integer values for a given attribute, its enumeration definition would contain:</p> <pre>0=value0 1=value1 2=value2 3=value3 4=value4</pre>

For example, the following enumerations definition section defines the Encryption-Types enumeration, which associates the string value 56-bit with the integer 0 and the string value 128-bit with the integer 1:

```
[Encryption-Types]
0=56-bit
1=128-bit
```

Example RADIUS Vendor/VSA Import File

The following example RADIUS vendor/VSA import file defines the vendor Widget, whose IETF number is 9999. The vendor Widget has 5 VSAs. Of those attributes, 4 are for authorization and one is for accounting. Only one attribute can have multiple instances in a single RADIUS message. Two attributes have enumerations for their valid integer values and they share the same enumeration definition section.

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
VSA 5=widget-remote-address
```

```
[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types
```

```
[widget-admin-interface]
Type=IPADDR
Profile=OUT
```

```
[widget-group]
```

```

Type=STRING
Profile=MULTI OUT

[widget-admin-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-remote-address]
Type=STRING
Profile=IN

[Encryption-Types]
0=56-bit
1=128-bit
2=256-bit

```

PAC File Generation

You can use the **-t** option to generate PAC files for use with EAP-FAST clients. You can generate PACs for users or for machines. For more information about PACs and EAP-FAST, see [EAP-FAST Authentication, page 9-9](#).

This section contains:

- [PAC File Options and Examples, page C-26](#)
- [Generating PAC Files, page C-28](#)

PAC File Options and Examples

When you use the **-t** option to generate PAC files with **CSUtil.exe**, you have the following additional options.

- **-filepath *full_filepath***—Specifies the location of the generated files.
- **-machine**—Use this option to generate PACs for machines instead of users.
- **User specification options**—You must choose one of the four options for specifying the users for whom you want PAC files; otherwise, **CSUtil.exe** displays an error message because no users are specified. User specification options are:
 - **-a**—**CSUtil.exe** generates a PAC file for each user in the ACS internal database. For example, if you have 3278 users in the ACS internal database and ran **CSUtil.exe -t -a**, **CSUtil.exe** would generate 3278 PAC files, one for each user.



Note

Using the **-a** option restarts the **CSAuth** service. No users are authenticated while **CSAuth** is unavailable.

- **-g *N***—**CSUtil.exe** generates a PAC file for each user in the user group specified by the variable (*N*). ACS has 500 groups, numbered from zero (0) to 499. For example, if Group 7 has 43 users and you ran **CSUtil.exe -t -g 7**, **CSUtil.exe** would generate 43 PAC files, one for each user who is a member of Group 7.



Note Using the **-g** option restarts the **CSAuth** service. No users are authenticated while **CSAuth** is unavailable.

- **-u username**—**CSUtil.exe** generates a PAC file for the user specified by the variable (*username*). For example, if you ran **CSUtil.exe -t -u seaniemop**, **CSUtil.exe** would generate a single PAC file, named *seaniemop.pac*.



Tip

You can also specify a domain-qualified username by using the format *DOMAIN\username*. For example, if you specify *ENGINEERING\augustin*, ACS generates a PAC file named *ENGINEERING_augustin.pac*.

- **-f list**—**CSUtil.exe** generates a PAC file for each username in the file that is specified, where *list* represents the full path and filename of the list of usernames.

Lists of usernames should contain one username per line, with no additional spaces or other characters.

For example, if *list.txt* in *d:\temp\pacs* contains the following usernames:

```
seaniemop
jwiedman
echamberlain
```

and you ran **CSUtil.exe -t -f d:\temp\pacs\list.txt**, **CSUtil.exe** generates three PAC files:

```
seaniemop.pac
jwiedman.pac
echamberlain.pac.
```



Tip

You can also specify domain-qualified usernames by using the format *DOMAIN\username*. For example, if you specify *ENGINEERING\augustin*, ACS generates a PAC file named *ENGINEERING_augustin.pac*.

- **-passwd password**—**CSUtil.exe** uses the password specified, rather than the default password, to protect the PAC files that it generates. The password that you specify is required when the PACs it protects are loaded into an EAP-FAST end-user client.



Note We recommend that you use a password that you devise, rather than the default password.

PAC passwords can contain any characters and are case-sensitive. They must contain between four and 128 characters. While **CSUtil.exe** does not enforce strong password rules, we recommend that you use a strong password.

Your PAC password should:

- Be very long.
- Contain uppercase and lowercase letters.
- Contain numbers in addition to letters.
- Contain no common words or names.

Generating PAC Files



Note

If you use the **-a** or **-g** option during PAC file generation, **CSUtil.exe** restarts the **CSAuth** service. No users are authenticated while **CSAuth** is unavailable.

For more information about PACs, see [About PACs, page 9-12](#).

To generate PAC files:

-
- Step 1** Use the discussion in [PAC File Options and Examples, page C-26](#), to determine the following:
- Which users for whom you want to generate PAC files. If you want to use a list of users, create it now.
 - What password to use to protect the PAC files that you generate. If necessary, create a password. Your PAC password should:
 - Be very long.
 - Contain uppercase and lowercase letters.
 - Contain numbers in addition to letters.
 - Contain no common words or names.
 - The full path to the directory in which you want the PAC files. If necessary, create the directory.
- Step 2** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**.
- Step 3** To create a PAC file for a user, type:
- ```
CSUtil.exe -t additional arguments
```
- where *additional arguments* represents at least one option for specifying the users for whom to generate PAC files. You can also use the options to specify filepath and password.
- Press **Enter**.
- To create a PAC file for a machine, type:
- ```
CSUtil.exe -t -machine additional arguments
```
- where *additional arguments* represents at least one option for specifying the users for whom to generate PAC files. You can also use the options to specify filepath and password.
- Press **Enter**.
- CSUtil.exe** generates the PAC files for each user that is specified. The PAC files are named with the username plus a *.pac* file extension. For example, a PAC file for the username *seaniemop* would be *seaniemop.pac* and a PAC file for the domain-qualified username **ENGINEERING\augustin** would be *ENGINEERING_augustin.pac*.
- If you specified a filepath, the PAC files are saved to the location that you specified. You can distribute the PAC files to the applicable end-user clients.
-

Posture-Validation Attributes

You can use **CSUtil.exe** to export, add, and delete posture-validation attributes, which are essential to Network Admission Control (NAC). For more information about NAC, see [Chapter 13, “Posture Validation.”](#)

This section contains:

- [Posture-Validation Attribute Definition File, page C-29](#)
- [Exporting Posture-Validation Attribute Definitions, page C-32](#)
- [Importing Posture-Validation Attribute Definitions, page C-32](#)
- [Deleting a Posture-Validation Attribute Definition, page C-34](#)
- [Default Posture-Validation Attribute Definition File, page C-36](#)

Posture-Validation Attribute Definition File

A posture-validation attribute definition file is a text file that contains one or more posture-validation attribute definitions. Each definition comprises a definition header and several of the following described values. For an example of the contents of a posture-validation attribute definition file, see [Default Posture-Validation Attribute Definition File, page C-36](#).

With the exception of the attribute definition header, each attribute definition value must be formatted:

name=value

where *name* is the value name and *value* is a string or integer, as specified in the following list.

**Tip**

Use a semicolon (;) to identify lines that are comments.

[Example C-1](#) shows an example of a posture-validation attribute definition, including a comment after the attribute definition:

Example C-1 Example Attribute Definition

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer

; attribute 1 is reserved for the APT
```

A posture-validation attribute is uniquely defined by the combination of its vendor ID, application ID, and attribute ID. The following list provides details of these values and of each line that is required in an attribute definition:

- **[attr#*n*]**—Attribute definition header, where *n* is a unique, sequential integer, beginning with zero (0). **CSUtil.exe** uses the definition header to distinguish the beginning of a new attribute definition. Each attribute definition *must* begin with a line containing the definition header. The first attribute definition in the file *must* have the header [attr#0], the second attribute definition in a file must have the header [attr#1], and so on. A break in the numbering causes **CSUtil.exe** to ignore attribute definitions at the break and beyond. For example, if, in a file with 10 attribute definitions, the fifth attribute is defined as [attr#5] instead of [attr#4], **CSUtil.exe** ignores the attribute that is defined as [attr#5] and the remaining five attributes that follow it.



Tip

The value of *n* is irrelevant to any of the ID values in the attribute definition file. For example, the 28th definition in a file must have the header [attr#27], but this does not limit or otherwise define valid values for vendor-id, application-id, or attribute-id. Neither does it limit or define the number of posture-validation attributes that ACS supports.

- **vendor-id**—An unsigned integer, the vendor number is of the vendor associated with the posture-validation attribute. The vendor number should be the number that is assigned to the vendor in the [IANA Assigned Numbers RFC](#). For example, vendor-id 9 corresponds to Cisco Systems, Inc. Vendor IDs have one or more applications that are associated with them, identified by the application-id value.
- **vendor-name**—A string, the vendor-name appears in the ACS web interface and logs for the associated posture-validation attribute. For example, any attribute definition with a vendor-name of 9 could have the vendor name **Cisco**.



Note

The vendor name cannot differ for each attribute that shares the same vendor-id. For example, you cannot add an attribute with a vendor-id of 9 if the vendor-name is not **Cisco**.

- **application-id**—An unsigned integer, the application-id uniquely identifies the vendor application associated with the posture-validation attribute. For example, if the vendor-id is 9 and the application-id is 1, the posture-validation attribute is associated with the Cisco application with an application-id of 1, which is the Cisco Trust Agent, also known as a posture agent (PA).
- **application-name**—A string, the application-name appears in the ACS web interface and logs for the associated posture-validation attribute. For example, if the vendor-id is 9 and the application-id is 1, the application-name would be PA, an abbreviation of posture agent, which is another term for the Cisco Trust Agent.



Note

The application-name cannot differ for each attribute that shares the same vendor-id and application-id pair. For example, you cannot add an attribute with a vendor-id of 9 and application-id of 1 if the application-name is not PA.

- **attribute-id**—An unsigned integer in the range of 1 to 65535, the attribute-id uniquely identifies the posture-validation attribute for the vendor-id and attribute-id specified.

**Note**

For each application, attributes 1 and 2 are reserved. If you add attributes that imply a new application, **CSUtil.exe** automatically creates attribute 1 as `Application-Posture-Token` and attribute 2 as `System-Posture-Token`.

- **attribute-name**—A string, the `attribute-name` appears in the ACS web interface and logs for the associated posture-validation attribute. For example, if the `vendor-id` is 9, the `application-id` is 1, and the `attribute-id` is 1, the `attribute-name` is `Application-Posture-Token`.
- **attribute-profile**—A string, the attribute profile specifies whether ACS can send the attribute in a posture-validation response, can receive the attribute in a posture-validation request, or can both send and receive the attribute during posture validation. Valid values for `attribute-profile` are:
 - **in**—ACS accepts the attribute in posture-validation requests and can log the attribute, and you can use it in internal policy rule definitions. Attributes with an `in` `attribute-profile` are also known as inbound attributes.
 - **out**—ACS can send the attribute in posture-validation responses but you cannot use it in internal policy rule definitions. Attributes with an `out` `attribute-profile` are also known as outbound attributes. The only outbound attributes that you can configure ACS to log are the attributes for Application Posture Tokens and System Posture Tokens; however, these are system-defined attributes that you cannot modify.
 - **in out**—ACS accepts the attribute in posture-validation requests and can send the attribute in posture-validation responses. Attributes with an `in out` `attribute-profile` are also known as inbound and outbound attributes.
- **attribute-type**—A string, the `attribute-type` specifies the kind of data that is valid in the associated attribute. For attributes whose `attribute-profile` is `in` or `in out`, the `attribute-type` determines the types of operators that are available for defining internal policy rules that use the attribute. An example of an inbound attribute is the `ServicePacks` attribute that the Cisco Trust Agent sends. An example of an outbound attribute is the `System-Posture-Token` attribute, which is sent to the Cisco Trust Agent.

Valid values of `attribute-type` are:

- `boolean`
- `string`
- `integer`
- `unsigned integer`
- `ipaddr`
- `date`
- `version`
- `octet-array`

For more information about attribute data types, see [Posture Validation Attribute Data Types](#), page 13-6.

Exporting Posture-Validation Attribute Definitions

The **-dumpAVP** option exports the current posture-validation attributes to an attribute definition file. For an explanation of the contents of a posture-validation attribute definition file, see [Posture-Validation Attribute Definition File, page C-29](#). For an example of an attribute-definition file, see [Default Posture-Validation Attribute Definition File, page C-36](#).

To export posture-validation attributes:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**.

Step 2 Type:

```
CSUtil.exe -dumpavp filename
```

where *filename* is the name of the file in which you want **CSUtil.exe** to write all attribute definitions.

Press **Enter**.



Tip

When you specify *filename*, you can prefix the filename with a relative or absolute path, too. For example, **CSUtil.exe -dumpavp c:\temp\allavp.txt** writes the file *allavp.txt* in *c:\temp*.

Step 3 If you are prompted to confirm overwriting a file with the same path and name that you specified in [Step 2](#), do one of the following:

- To overwrite the file, type **Y** and press **Enter**.



Tip

To force **CSUtil.exe** to overwrite an existing file, use the **-q** option: **CSUtil.exe -q -dumpavp filename**.

- To preserve the file, type **N**, press **Enter**, and return to [Step 2](#).

CSUtil.exe writes all posture-validation attribute definitions in the file specified. To view the contents of the file, use the text editor of your choice.

Importing Posture-Validation Attribute Definitions

The **-addAVP** option imports posture-validation attribute definitions into ACS from an attribute definition file. For an explanation of the contents of a posture-validation attribute definition file, see [Posture-Validation Attribute Definition File, page C-29](#). For an example of an attribute definition file, see [Default Posture-Validation Attribute Definition File, page C-36](#).

Before You Begin

Because completing this procedure requires restarting the **CSAuth** service, which temporarily suspends authentication services, consider performing this procedure when demand for ACS services is low.

Use the steps in [Exporting Posture-Validation Attribute Definitions, page C-32](#), to create a backup of posture-validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of current posture-validation attributes.

To import posture-validation attributes:

-
- Step 1** Use the discussion in [Posture-Validation Attribute Definition File, page C-29](#), to create a properly formatted attribute definition file. Place the file in the directory containing **CSUtil.exe** or a directory that is accessible from the computer that is running ACS.
- Step 2** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**.
- Step 3** Type:
- ```
CSUtil.exe -addavp filename
```
- where *filename* is the name of the file in which you want **CSUtil.exe** to write all attribute definitions. Press **Enter**.




---

**Tip** When you specify *filename*, you can prefix the filename with a relative or absolute path, too. For example, **CSUtil.exe -addavp c:\temp\addavp.txt** writes the file *addavp.txt* in *c:\temp*.

---

**CSUtil.exe** adds or modifies the attributes that are specified in the file. An example of a successful addition of nine posture-validation attributes is:

```
C:\...\Utils 21: csutil -addavp myavp.txt
...
Attribute 9876:1:11 (Calliope) added to dictionary
Attribute 9876:1:3 (Clio) added to dictionary
Attribute 9876:1:4 (Erato) added to dictionary
Attribute 9876:1:5 (Euterpe) added to dictionary
Attribute 9876:1:6 (Melpomene) added to dictionary
Attribute 9876:1:7 (Polyhymnia) added to dictionary
Attribute 9876:1:8 (Terpsichore) added to dictionary
Attribute 9876:1:9 (Thalia) added to dictionary
Attribute 9876:1:10 (Urania) added to dictionary
```

AVPs from 'myavp.txt' were successfully added

- Step 4** If you are ready for the imported attribute definitions to take effect, restart the **CSAuth** and **CSAdmin** services.



**Caution**

---

While **CSAuth** is stopped, no users are authenticated.

---

To restart the **CSAuth**, **CSLog**, and **CSAdmin** services, enter the following commands at the command prompt, allowing the computer time to perform each command:

```
net stop csauth
net start csauth
net stop cslog
net start cslog
net stop csadmin
net start csadmin
```

ACS begins using the imported posture-validation attributes. Attributes that have an attribute type of **in** or **in out** are available in the web interface when you define internal policy rules.

---

## Importing External Audit Posture-Validation Servers

To create an audit vendor file to import into the ACS dictionary:

- 
- Step 1** On the computer that is running ACS, open an MS-DOS command prompt and change to the *\bin* directory (the directory containing **CSUtil.exe**).
- Step 2** Type:
- ```
CSUtil.exe -addavp filename
```
- where *filename* is the name of the file that contains the audit server vendor data. If the file is not located in the *\bin* directory, you must add the full path name.
- The format of the file should be:
- ```
[attr#0]
 vendor-id=<the vendor identifier number>
 vendor-name=<the name of the vendor>
 application-id=6
 application-name=Audit
```
- Step 3** Press **Enter**.
- Step 4** Restart the CSAdmin CSAuth, and CSLog services. You can restart these services manually from the command prompt, or choose Windows **Programs > Administrative Tools > Services**.
- 

## Deleting a Posture-Validation Attribute Definition

The **-delAVP** option deletes a single posture-validation attribute from ACS.

### Before You Begin

Because completing this procedure requires restarting the **CSAuth** service, which temporarily suspends authentication services, consider performing this procedure when demand for ACS services is low.

Use the steps in [Exporting Posture-Validation Attribute Definitions, page C-32](#), to create a backup of posture-validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of the posture-validation attribute you want to delete.

To delete posture-validation attributes:

- 
- Step 1** On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**.
- Step 2** Type:
- ```
CSUtil.exe -delavp vendor-ID application-ID attribute-ID
```
- For more information about vendor, application, and attribute IDs, see [Posture-Validation Attribute Definition File, page C-29](#).
- CSUtil.exe** prompts you to confirm the attribute deletion.
- Step 3** Examine the confirmation prompt and then:
- If you are certain that you want to delete the attribute identified by the confirmation prompt, type **Y** and press **Enter**.



Tip You can use the **-q** option to suppress the confirmation prompt.

- If you do not want to delete the attribute that the confirmation prompt identifies, type **N**, press **Enter**, and return to [Step 2](#).

CSUtil.exe deletes the posture-validation attribute that you specified from its internal database. In the following example, **CSUtil.exe** deleted an attribute with a vendor ID of 9876, an application ID of 1, and an attribute ID of 1.

```
Are you sure you want to delete vendor 9876; application 1; attribute 1? (y/n)
y
```

```
Vendor 9876; application 1; attribute 1 was successfully deleted
```

Step 4 For the attribute deletion to take effect, restart the **CSAuth** and **CSAdmin** services.



Caution While **CSAuth** is stopped, no users are authenticated.

To restart the **CSAuth**, **CSLog**, and **CSAdmin** services, enter the following commands at the command prompt, allowing the computer time to perform each command:

```
net stop csauth
net start csauth
net stop cslog
net start cslog
net stop csadmin
net start csadmin
```

Deleted posture-validation attributes are no longer available in ACS.

Deleting an Extended Posture-Validation Attribute Definition

To delete the extended posture-validation Property attribute contained in the Cisco:Host application:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**.

Step 2 Type:

```
CSUtil.exe -delPropHPP <attribute ID> <property ID>
```

This command removes the specific **PROPERTY** from an Extended attribute under **Cisco:Host**.

For more information about vendor, application, and attribute IDs, see [Posture-Validation Attribute Definition File, page C-29](#).

To delete extended posture-validation **ENTITY** attributes in the **Cisco:Host** application:

Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change directories to the directory containing **CSUtil.exe**.

Step 2 Type:

```
CSUtil.exe -delEntHPP <attribute ID> <entity name>
```

This command removes the specific **ENTITY** from an Extended attribute under **Cisco:Host**.

For more information about vendor, application, and attribute IDs, see [Posture-Validation Attribute Definition File, page C-29](#).



Note

Extended attributes are supported only as descendants of the **Cisco:Host** application.

Default Posture-Validation Attribute Definition File

[Example C-2](#) provides the definitions for the posture-validation attributes that we provide with ACS. This example is contained in the file *acs4.0_avp.txt*, in the *\Utils* folder. If you need to reset the default attributes to their original definitions, use the syntax in [Example C-2](#) to create a posture-validation attribute definition file. For more information about the format of an attribute definition file, see [Posture-Validation Attribute Definition File, page C-29](#).

Example C-2 Default Posture-Validation Attribute Definitions

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#1]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00002
attribute-name=System-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer
```

```
[attr#2]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00003
attribute-name=PA-Name
attribute-profile=in out
attribute-type=string
```

```
[attr#3]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00004
attribute-name=PA-Version
```



```
attribute-profile=in out
attribute-type=version

[attr#4]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00005
attribute-name=OS-Type
attribute-profile=in out
attribute-type=string

[attr#5]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00006
attribute-name=OS-Version
attribute-profile=in out
attribute-type=version

[attr#6]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00007
attribute-name=PA-User-Notification
attribute-profile=out
attribute-type=string

[attr#7]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00008
attribute-name=OS-Release
attribute-profile=in out
attribute-type=string

[attr#8]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00009
attribute-name=Kernel-Version
attribute-profile=in out
attribute-type=version

[attr#9]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00010
attribute-name=Action
attribute-profile=out
attribute-type=string

[attr#10]
```

```

vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00011
attribute-name=Machine-Posture-State
attribute-profile=in out
attribute-type=unsigned integer

[attr#11]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00001
attribute-name=Application-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#12]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00002
attribute-name=System-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#13]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00006
attribute-name=ServicePacks
attribute-profile=in
attribute-type=string

[attr#14]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00007
attribute-name=HotFixes
attribute-profile=in
attribute-type=string

[attr#15]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00008
attribute-name=HostFQDN
attribute-profile=in
attribute-type=string

[attr#16]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host

```

```

attribute-id=00100
attribute-name=Package
attribute-profile=in
attribute-type=string

[attr#17 (extended)]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00100
attribute-name=Package
entities-list=acrobat;cpio;cups;curl;cvs;cyrus-sasl;emacs;enscript;ethereal;evolution;gaim;
gd;gdk-pixbuf;glibc;gnome-vfs2;gnupg;gtk2;httpd;ia32el;imagemagick;imap;imlib;iproute;ips
ec-tools;kdegraphics;kdelibs;kdenetwork;kdepim;kernel;krb5;less;lftp;lha;libpng;libtiff;li
bxml;libxml2;mailman;mod_python;mozilla;mutt;mysql;mysql-server;nasm;net-snmp;netpbm;nfs-u
tils;openmotif;openoffice.org;openssh;openssl;perl;perl-dbi;php;postgresql;pwlib;python;qt
;realplayer;redhat-config-nfs;rh-postgresql;rsh;rsync;ruby;samba;sharutils;slocate;sox;spa
massassin;squid;squirrelmail;sysstat;tcpdump;telnet;tetex;utempter;vim;xchat;xemacs;xfree8
6;xloadimage;xpdf;zip;
property-id=4
property-name=Version
attribute-profile=in
attribute-type=version

[attr#18 (extended)]
vendor-id=9
vendor-name=Cisco
application-id=2
application-name=Host
attribute-id=00100
attribute-name=Package
entities-list=acrobat;cpio;cups;curl;cvs;cyrus-sasl;emacs;enscript;ethereal;evolution;gaim;
gd;gdk-pixbuf;glibc;gnome-vfs2;gnupg;gtk2;httpd;ia32el;imagemagick;imap;imlib;iproute;ips
ec-tools;kdegraphics;kdelibs;kdenetwork;kdepim;kernel;krb5;less;lftp;lha;libpng;libtiff;li
bxml;libxml2;mailman;mod_python;mozilla;mutt;mysql;mysql-server;nasm;net-snmp;netpbm;nfs-u
tils;openmotif;openoffice.org;openssh;openssl;perl;perl-dbi;php;postgresql;pwlib;python;qt
;realplayer;redhat-config-nfs;rh-postgresql;rsh;rsync;ruby;samba;sharutils;slocate;sox;spa
massassin;squid;squirrelmail;sysstat;tcpdump;telnet;tetex;utempter;vim;xchat;xemacs;xfree8
6;xloadimage;xpdf;zip;
property-id=5
property-name=Version-String
attribute-profile=in
attribute-type=string

[attr#19]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00001
attribute-name=Application-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

[attr#20]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00002
attribute-name=System-Posture-Assessment
attribute-profile=out
attribute-type=unsigned integer

```

```

[attr#21]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00005
attribute-name=CSAVersion
attribute-profile=in
attribute-type=version

[attr#22]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=00009
attribute-name=CSAOperationalState
attribute-profile=in
attribute-type=unsigned integer

[attr#23]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32768
attribute-name=CSAMCName
attribute-profile=in
attribute-type=string

[attr#24]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32769
attribute-name=CSAStates
attribute-profile=in
attribute-type=string

[attr#25]
vendor-id=9
vendor-name=Cisco
application-id=5
application-name=HIP
attribute-id=32770
attribute-name=DaysSinceLastSuccessfulPoll
attribute-profile=in
attribute-type=unsigned integer

```

Adding External Audit Device Type Attributes

To create an audit device type attribute file to import into the ACS dictionary:

-
- Step 1 On the computer that is running ACS, open an MS-DOS command prompt and change to the `\bin` directory (the directory containing **CSUtil.exe**).
 - Step 2 Type:

```
CSUtil.exe -addavp filename
```

where *filename* is the name of the file that contains the audit server vendor data. If the file is not located in the `\bin` directory, you must add the full path name.

The format of the file should be:

```
[attr#0]
  vendor-id=<the vendor identifier number>
  vendor-name=<the name of the vendor>
  application-id=6
  application-name=Audit
  attribute-id=00012
  attribute-name=Device-Type
  attribute-profile=in out
  attribute-type=string
```

Step 3 Press **Enter**.

Step 4 Restart the CSAdmin CSAuth, and CSLog services. You can restart these services manually from the command prompt, or choose Windows **Programs > Administrative Tools > Services**.

Adding and Editing Devices Using the CSUtil Utility

ACS supports use of the **CSUtil import.txt** file for adding and editing authentication, authorization, and accounting (AAA) devices. You can edit all attributes of the AAA devices, including the:

- IP address
- Shared secret
- Vendor
- Network device group
- Single connection
- Keepalive settings



APPENDIX D

VPDN Processing

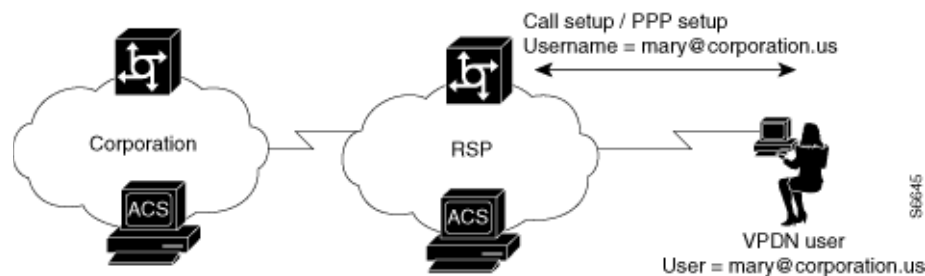
The Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, supports authentication forwarding of virtual private dial-up network (VPDN) requests. There are two basic types of roaming users: Internet and intranet; VPDN addresses the requirements of roaming intranet users. This chapter provides information about the VPDN process and how it affects the operation of ACS.

VPDN Process

This section describes the steps for processing VPDN requests in a standard environment.

1. A VPDN user dials in to the network access server (NAS) of the regional service provider (RSP). The standard call/point-to-point protocol (PPP) setup is done. A username and password are sent to the NAS in the format *username@domain* (for example, *mary@corporation.us*). See [Figure D-1](#).

Figure D-1 VPDN User Dials In



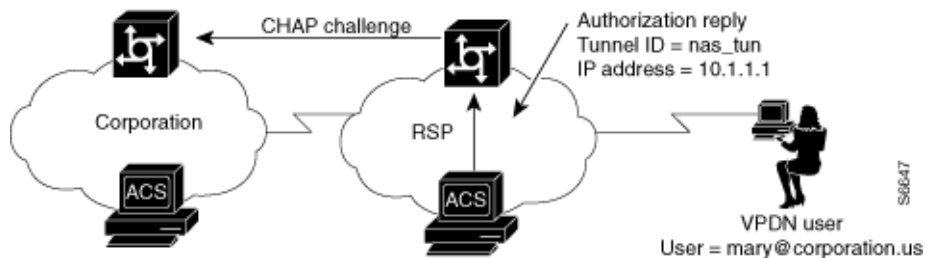
2. If VPDN is enabled, the NAS assumes that the user is a VPDN user. The NAS strips off the *username@* (*mary@*) portion of the username and authorizes (not authenticates) the domain portion (*corporation.us*) with the ACS. See [Figure D-2](#).

Figure D-2 NAS Attempts to Authorize Domain

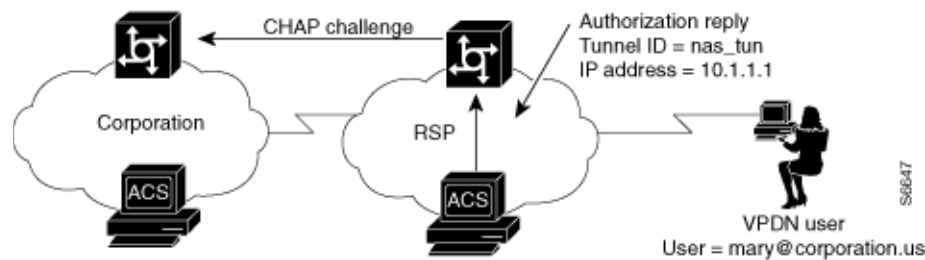
3. If the domain authorization fails, the NAS assumes that the user is not a VPDN user. The NAS then authenticates (not authorizes) the user as if the user is a standard non-VPDN dial user. See [Figure D-3](#).

Figure D-3 Authorization of Domain Fails

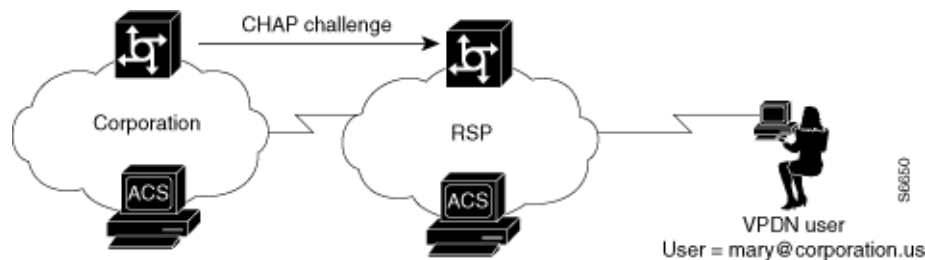
If the ACS authorizes the domain, it returns the Tunnel ID and the IP address of the home gateway (HG); these are used to create the tunnel. See [Figure D-4](#).

Figure D-4 ACS Authorizes Domain

4. The HG uses its ACS to authenticate the tunnel, where the username is the name of the tunnel (`nas_tun`). See [Figure D-5](#).

Figure D-5 HG Authenticates Tunnel with ACS

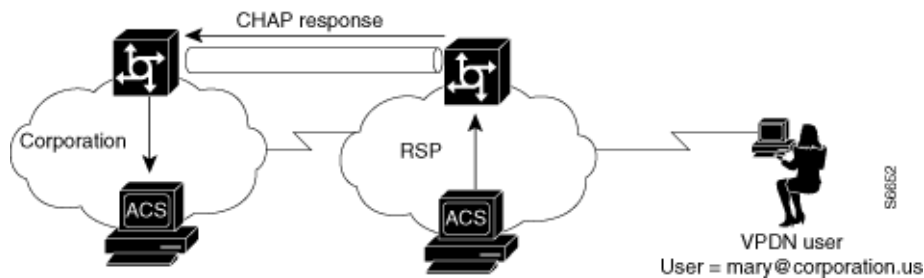
- The HG now authenticates the tunnel with the NAS, where the username is the name of the HG. This name is chosen based on the name of the tunnel, so the HG might have different names depending on the tunnel being set up. See [Figure D-6](#).

Figure D-6 HG Authenticates Tunnel with the NAS

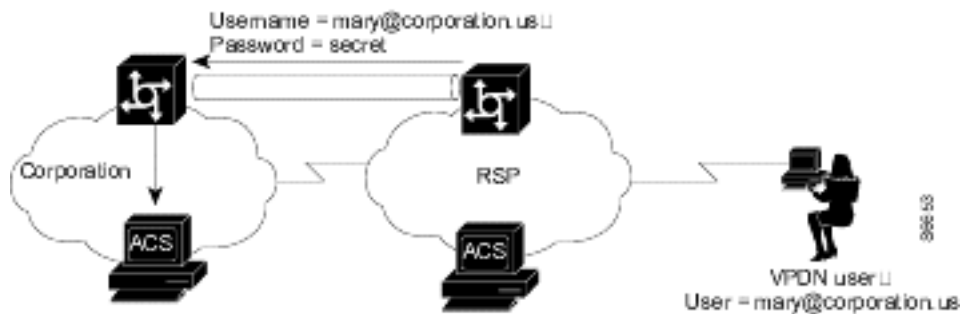
- The NAS now uses its ACS to authenticate the tunnel from the HG. See [Figure D-7](#).

Figure D-7 NAS Authenticates Tunnel with ACS

- After authenticating, the tunnel is established. Now the actual user (*mary@corporation.us*) must be authenticated. See [Figure D-8](#).

Figure D-8 VPDN Tunnel is Established

8. The HG now authenticates the user as if the user dialed directly in to the HG. The HG might now challenge the user for a password. The ACS at RSP can be configured to strip off the at symbol (@) and domain before it passes the authentication to the HG. (The user is passed as *mary@corporation.us*.) The HG uses its ACS to authenticate the user. See [Figure D-9](#).

Figure D-9 HG Uses ACS to Authenticate User

9. If another user (*sue@corporation.us*) dials in to the NAS while the tunnel is up, the NAS does not repeat the entire authorization and authentication process. Instead, it passes the user through the existing tunnel to the HG. See [Figure D-10](#).

Figure D-10 Another User Dials In While Tunnel is Up



RDBMS Synchronization Import Definitions

ACS for Windows

RDBMS synchronization import definitions are a listing of the action codes allowable in an `accountActions` table. The RDBMS Synchronization feature of the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS, uses a table named `accountActions` as input for automated or manual updates of the ACS internal database.

ACS SE

RDBMS synchronization import definitions are a listing of the action codes allowable in an `accountActions` file. The RDBMS Synchronization feature of ACS SE uses a comma-separated value (CSV) file named `accountActions` as input for automated or manual updates of the ACS internal database. Each line in `accountActions` represents one action, with the exception of the first line, which is ignored during synchronization events. This scenario permits the use of the first line of `accountActions` as field headers.

For more information about the RDBMS Synchronization feature and `accountActions`, see [RDBMS Synchronization Components, page 8-27](#).

This chapter contains:

- [accountActions Specification, page E-1](#)
- [Supported Versions for ODBC Data Sources \(ACS for Windows\), page E-3](#)
- [Action Codes, page E-3](#)
- [ACS Attributes and Action Codes, page E-23](#)
- [An Example of accountActions, page E-30](#)

accountActions Specification

Whether you create `accountActions` by hand in a text editor or through automation using a third-party system that writes to `accountActions`, you must adhere to the `accountActions` specification and must only use the action codes detailed in [Action Codes, page E-3](#). Otherwise, RDBMS Synchronization may import incorrect information into the ACS internal database or may fail to occur at all.

accountActions Format

Each row in accountActions has 14 fields (or columns). [Table E-1](#) lists the fields that compose accountActions. [Table E-1](#) also reflects the order in which the fields appear in accountActions.

The one-letter or two-letter abbreviations given in the Mnemonic column are a shorthand notation used to indicate required fields for each action code in [Action Codes](#), [page E-3](#).

To see an example accountActions, see [An Example of accountActions](#), [page E-30](#).

Table E-1 *accountActions Fields*

Field Name	Mnemonic	Type	Size (Max. Length)	Comments
SequenceId	SI	AutoNumber	32	The unique action ID.
Priority	P	Integer	1	The priority with which this update is to be treated. Zero (0) is the lowest priority.
UserName	UN	String	32	The name of the user to which the transaction applies.
GroupName	GN	String	32	The name of the group to which the transaction applies.
Action	A	Number	0-2 ¹⁶	The action required. (See Action Codes , page E-3 .)
ValueName	VN	String	255	The name of the parameter to change.
Value1	V1	String	255	The new value (for numeric parameters, this is a decimal string).
Value2	V2	String	255	The name of a TACACS+ protocol; for example, <i>ip</i> or RADIUS VSA Vendor ID.
Value3	V3	String	255	The name of a TACACS+ service; for example, <i>ppp</i> or the RADIUS VSA attribute number.
DateTime	DT	DateTime	—	The date and time the action was created.
MessageNo	MN	Integer	—	Used to number related transactions for audit purposes.
ComputerNames	CN	String	32	RESERVED by CSDBSync.
AppId	AI	String	255	The type of configuration parameter to change.
Status	S	Number	32	TRI-STATE:0=not processed, 1=done, 2=failed. This value should normally be set to 0.

accountActions Mandatory Fields

For all actions, the following fields cannot be empty and must have a valid value:

- Action
- SequenceID
- Status

In addition to the previous required fields, the DateTime, UserName and GroupName fields are also often required to have a valid value:

- If a transaction is acting upon a user account, a valid value is required in the UserName field.
- If a transaction is acting upon a group, a valid value is required in the GroupName field.

- If a transaction is acting upon a AAA client configuration, neither the UserName field nor the GroupName field require a value.

**Note**

The UserName and GroupName fields are mutually exclusive; only one of these two fields can have a value and neither field is always required.

accountActions Processing Order

ACS reads rows from accountActions and processes them in a specific order. ACS determines the order first by the values in the Priority fields (mnemonic: P) and then by the values in the Sequence ID fields (mnemonic: SI). ACS processes the rows with the highest Priority field. The lower the number in the Priority field, the higher the priority. For example, if row A has the value 1 in its Priority field and row B has the value 2 in its Priority field, ACS would process row A first, regardless of whether row B has a lower sequence ID or not. If rows have an equal priority, ACS processes them by their sequence ID, with the lowest sequence ID processed first.

Thus, the Priority field (P) enables transactions of higher importance to occur first, such as deleting a user or changing a password. In the most common implementations of RDBMS Synchronization, a third-party system writes to accountActions in batch mode, with all actions (rows) assigned a priority of zero (0).

**Note**

When changing transaction priorities, be careful that they are processed in the correct order; for example, a user account must be created before the user password is assigned.

You can use the MessageNo field (mnemonic: MN) to associate related transactions, such as the addition of a user and subsequent actions to set password values and status. You can use the MessageNo field to create an audit trail for a third-party system that writes to accountActions.

Supported Versions for ODBC Data Sources (ACS for Windows)

The following versions are supported for RDBMS synchronization through ODBC.

- MS-SQL version 3.80 later
- ODBC version 3.80 or later

Action Codes

This section provides the action codes valid for use in the Action field (mnemonic: A) of accountActions. The Required column uses the field mnemonic names to indicate which fields should be completed, except for the mandatory fields, which are assumed. For more information about the mnemonic names of accountActions fields, see [Table E-1](#). For more information about the mandatory fields, see [accountActions Mandatory Fields](#), page E-2.

If an action can be applied to a user or group, UN|GN appears, using the vertical bar (|) to indicate that either one of the two fields is required. To make the action affect only the user, leave the group name empty; to make the action affect only the group, leave the user name empty.

This section contains:

- [Action Codes for Setting and Deleting Values, page E-4](#)
- [Action Codes for Creating and Modifying User Accounts, page E-5](#)
- [Action Codes for Initializing and Modifying Access Filters, page E-10](#)
- [Action Codes for Modifying TACACS+ and RADIUS Group and User Settings, page E-13](#)
- [Action Codes for Modifying Network Configuration, page E-18](#)
- [ACS Attributes and Action Codes, page E-23](#)

Action Codes for Setting and Deleting Values

The two most fundamental action codes are SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2), described in [Table E-2](#).

The SET_VALUE (action code: 1) and DELETE_VALUE (action code: 2) actions, described in [Table E-2](#), instruct RDBMS Synchronization to assign a value to various internal attributes in ACS. Unless a Cisco representative asks you to use these action codes for other purposes, you can only use these action codes for assigning values to user-defined fields (see [User-Specific Attributes, page E-24](#)).

Table E-2 Action Codes for Setting and Deleting Values

Action Code	Name	Required	Description
1	SET_VALUE	UN GN, AI, VN, V1, V2	<p>Sets a value (V1) named (VN) of type (V2) for App ID (AI).</p> <p>App IDs (AI) can be one of the following:</p> <ul style="list-style-type: none"> • APP_CSAUTH • APP_CSTACACS • APP_CSRADIUS • APP_CSADMIN <p>Value types (V2) can be one of the following:</p> <ul style="list-style-type: none"> • TYPE_BYTE—Single 8-bit number. • TYPE_SHORT—Single 16-bit number. • TYPE_INT—Single 32-bit number. • TYPE_STRING—Single string. • TYPE_ENCRYPTED_STRING—Single string to be saved encrypted. • TYPE_MULTI_STRING—Tab-separated set of substrings. • TYPE_MULTI_INT—Tab-separated set of 32-bit numbers. <p>For example:</p> <pre>UN = "fred" AI = "APP_CSAUTH" VN = "My Value" V2 = "TYPE_MULTI_STRING" V1 = "str1tabstr2tabstr3"</pre>
2	DELETE_VALUE	UN GN, AI, VN	Deletes value (VN) for App ID (AI) and user (UN) or group (GN).

Action Codes for Creating and Modifying User Accounts

[Table E-3](#) lists the action codes for creating, modifying, and deleting user accounts.



Note

Before you can modify a user account, such as assigning a password, you must create the user account, in the web interface or by using the ADD_USER action (action code: 100).

Transactions using these codes affect the configuration that appears in the User Setup section of the web interface. For more information about the User Setup section, see [Chapter 6, “User Management.”](#)

Table E-3 User Creation and Modification Action Codes

Action Code	Name	Required	Description
100	ADD_USER	UN GN, V1	Creates a user (32 characters maximum). V1 is used as the initial password. Optionally, the user can also be assigned to a group.

Table E-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
101	DELETE_USER	UN	Removes a user.
102	SET_PAP_PASS	UN, V1	Sets the PAP password for a user (64 ASCII characters maximum). CHAP/ARAP will also default to this.
103	SET_CHAP_PASS	UN, V1	Sets the CHAP/ARAP password for a user (64 characters maximum).
104	SET_OUTBOUND_CHAP_PASS	UN, V1	Sets the CHAP/ARAP password for a user (32 characters maximum).
105	SET_T+_ENABLE_PASS	UN, VN, V1, V2, V3	<p>Sets the TACACS+ enable password (V1) (32 characters maximum) and Max Privilege level (V2) (0-15).</p> <p>The enable type (V3) should be one of the following:</p> <ul style="list-style-type: none"> • ENABLE_LEVEL_AS_GROUP—Max privilege taken from group setting. • ENABLE_LEVEL_NONE—No T+ enable configured. • ENABLE_LEVEL_STATIC—Value set in V2 used during enable level check. <p>You can use VN to link the enable password to an external authenticator, as per action 108 SET_PASS_TYPE.</p>
106	SET_GROUP	UN, GN	Sets the ACS group assignment of the user.
108	SET_PASS_TYPE	UN GN, V1	<p>Sets the password type of the user. This can be one of the ACS internal database password types or any of the external databases supported:</p> <ul style="list-style-type: none"> • PASS_TYPE_CSDB—CSDB internal password. • PASS_TYPE_CSDB_UNIX—CSDB internal password (UNIX encrypted). • PASS_TYPE_NT—External Windows user database password. • PASS_TYPE_LDAP—External generic LDAP database password. • PASS_TYPE_LEAP—External LEAP proxy RADIUS server database password. • PASS_TYPE_RADIUS_TOKEN—External RADIUS token server database password.

Table E-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
109	REMOVE_PASS_STATUS	UN,V1	Removes a password status flag. This action results in the status states being linked in a logical XOR condition. V1 should contain one of the following: <ul style="list-style-type: none"> PASS_STATUS_EXPIRES—Password expires on a given date. PASS_STATUS_NEVER—Password never expires. PASS_STATUS_WRONG—Password expires after a given number of login attempts using the wrong password. PASS_STATUS_DISABLED—The account has been disabled.
110	ADD_PASS_STATUS	UN, V1	Defines how a password should be expired by ACS. To set multiple password states for a user, use multiple instances of this action. This action results in the status states being linked in a logical XOR condition. V1 should contain one of the following: <ul style="list-style-type: none"> PASS_STATUS_EXPIRES—Password expires on a given date. PASS_STATUS_NEVER—Password never expires. PASS_STATUS_WRONG—Password expires after a given number of login attempts by using the wrong password. PASS_STATUS_RIGHT—Password expires after a given number of login attempts by using the correct password. PASS_STATUS_DISABLED—The account has been disabled.
112	SET_PASS_EXPIRY_WRONG	UN,V1	Sets the maximum number of bad authentications allowed (automatic reset on good password if not exceeded) and resets the current count.
113	SET_PASS_EXPIRY_DATE	UN,V1	Sets the date on which the account expires. The date format should be YYYYMMDD.
114	SET_MAX_SESSIONS	UN GN, V1	Sets the maximum number of simultaneous sessions for a user or group. V1 should contain one of the following values: <ul style="list-style-type: none"> MAX_SESSIONS_UNLIMITED MAX_SESSIONS_AS_GROUP 1-65534
115	SET_MAX_SESSIONS_GROUP_USER	GN,V1	Sets the max sessions for a user of the group to one of the following values: <ul style="list-style-type: none"> MAX_SESSIONS_UNLIMITED 1-65534

Table E-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
260	SET_QUOTA	VN,V1, V2	<p>Sets a quota for a user or group.</p> <p>VN defines the quota type. Valid values are:</p> <ul style="list-style-type: none"> • online time—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2. • sessions—The quota limits the user or group by the number of sessions on the network for the period defined in V2. <p>V1 defines the quota. If VN is set to sessions, V1 is the maximum number of sessions in the period defined in V2. If VN is set to online time, V1 is the maximum number of seconds.</p> <p>V2 holds the period for the quota. Valid values are:</p> <ul style="list-style-type: none"> • QUOTA_PERIOD_DAILY—The quota is enforced in 24-hour cycles, from 12:01 A.M. to midnight. • QUOTA_PERIOD_WEEKLY—The quota is enforced in 7-day cycles, from 12:01 A.M. Sunday until midnight Saturday. • QUOTA_PERIOD_MONTHLY—The quota is enforced in monthly cycles, from 12:01 A.M. on the first of the month until midnight on the last day of the month. • QUOTA_PERIOD_ABSOLUTE—The quota is enforced in an ongoing basis, without an end.
261	DISABLE_QUOTA	UN GN, VN	<p>Disables a group or user usage quota.</p> <p>VN defines the quota type. Valid values are:</p> <ul style="list-style-type: none"> • online time—The quota limits the user or group by the number of seconds logged in to the network for the period defined in V2. • sessions—The quota limits the user or group by the number of sessions on the network for the period defined in V2.
262	RESET_COUNTERS	UN GN	Resets usage quota counters for a user or group.
263	SET_QUOTA_APPLY_TYPE	V1	<p>Defines whether a user usage quota is determined by the user group quota or by a quota unique to the user. V1 makes this specification. Valid values for V1 are:</p> <ul style="list-style-type: none"> • ASSIGNMENT_FROM_USER • ASSIGNMENT_FROM_GROUP

Table E-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
270	SET_DCS_TYPE	UN GN, VN,V1, Optional-ly V2	<p>Sets the type of device command set (DCS) authorization for a group or user.</p> <p>VN defines the service. Valid service types are:</p> <ul style="list-style-type: none"> • shell—Cisco IOS shell command authorization. • pixshell—Cisco PIX command authorization. <p>Note If additional DCS types have been added to your ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as:</p> <p>PIX Shell (pixshell)</p> <p>V1 defines the assignment type. The valid values for VN are:</p> <ul style="list-style-type: none"> • none—Sets no DCS for the user or group. • as group—For users only, this value signifies that the user DCS settings for the service specified should be the same as the user group DCS settings. • static—Sets a DCS for the user or group for all devices enabled to perform command authorization for the service specified. <p>If V1 is set to static, V2 is required and must contain the name of the DCS to assign to the user or group for the given service.</p> <ul style="list-style-type: none"> • ndg—Specifies that command authorization for the user or group is to be done on a per-NDG basis. Use action 271 to add DCS to NDG mappings for the user or group. <p>Note Changing a user or group assignment type (V1) results in clearing previous data, including NDG to DCS mappings (defined by action 271).</p>

Table E-3 User Creation and Modification Action Codes (continued)

Action Code	Name	Required	Description
271	SET_DCS_NDG_MAP	UN GN, VN,V1, V2	<p>Use this action code to map between the device command set and the NDG when the assignment type specified by a 270 action code is ndg.</p> <p>VN defines the service. Valid service types are:</p> <ul style="list-style-type: none"> • shell—Cisco IOS shell command authorization. • pixshell—Cisco PIX command authorization. <p>Note If additional DCS types have been added to your ACS, you can find the valid value in the Interface Configuration page for TACACS+ (Cisco IOS). The valid values appear in parentheses after the service title, such as:</p> <pre>PIX Shell (pixshell)</pre> <p>V1 defines the name of the NDG. Use the name of the NDG as it appears in the web interface. For example, if you have configured an NDG named <i>East Coast NASs</i> and want to use action 271 to apply a DCS to that NDG, V1 should be <i>East Coast NASs</i>.</p> <p>V2 defines the name of the DCS. Use the name of the DCS as it appears in the web interface. For example, if you have configured a DCS named <i>Tier2 PIX Admin DCS</i> and want to use action 271 to apply it to an NDG, V2 should be <i>Tier2 PIX Admin DCS</i>.</p>

Action Codes for Initializing and Modifying Access Filters

Table E-4 lists the action codes for initializing and modifying AAA client access filters. AAA client access filters control Telnet access to a AAA client. Dial access filters control access by dial-up users.

Transactions using these codes affect the configuration that appears in the User Setup and Group Setup sections of the web interface. For more information about the User Setup section, see [Chapter 6, “User Management.”](#) For more information about the Group Setup section, see [Chapter 5, “User Group Management.”](#)

Table E-4 Action Codes for Initializing and Modifying Access Filters

Action Code	Name	Required	Description
120	INIT_NAS_ACCESS_CONTROL	UN GN,V1	<p>Clears the AAA client access filter list and initialize permit or deny for any forthcoming filters. V1 should be one of the following values:</p> <ul style="list-style-type: none"> ACCESS_PERMIT ACCESS_DENY
121	INIT_DIAL_ACCESS_CONTROL	UN GN,V1	<p>Clears the dial-up access filter list and initialize permit/deny for any forthcoming filters. V1 should be one of the following values:</p> <ul style="list-style-type: none"> ACCESS_PERMIT ACCESS_DENY
122	ADD_NAS_ACCESS_FILTER	UN GN,V1	<p>Adds a AAA client filter for the user group.</p> <p>V1 should contain a single (AAA client name, AAA client port, remote address, CLID) tuple; for example:</p> <pre>NAS01, tty0, 0898-69696969</pre> <p>Optionally, the AAA client name can be <i>All AAA clients</i> to specify that the filter applies to all configured AAA clients and an asterisk (*) to represent all ports.</p>
123	ADD_DIAL_ACCESS_FILTER	UN GN, V1, V2	<p>Adds a dial-up filter for the user group.</p> <p>V1 should contain one of the following values:</p> <ul style="list-style-type: none"> Calling station ID Called station ID Calling and called station ID; for example: <pre>01732-875374, 0898-69696969</pre> <ul style="list-style-type: none"> NAS IP address, NAS port; for example: <pre>10.45.6.123, tty0</pre> <p>V2 should contain the filter type as one of the following values:</p> <ul style="list-style-type: none"> CLID—The user is filtered by the calling station ID. DNIS—The user is filtered by the called station ID. CLID/DNIS—The user is filtered by calling and called station IDs. NAS/PORT—The user is filtered by NAS IP and NAS port address.
130	SET_TOKEN_CACHE_SESSION	GN, V1	Enables or disables token caching for an entire session; V1 is 0=disable, 1=enable.
131	SET_TOKEN_CACHE_TIME	GN, V1	Sets the duration that tokens are cached. V1 is the token cache duration in seconds.

Table E-4 Action Codes for Initializing and Modifying Access Filters (continued)

Action Code	Name	Required	Description
140	SET_TODDOW_ACCESS	UN GN, V1	Sets periods during which access is permitted. V1 contains a string of 168 characters. Each character represents a single hour of the week. A 1 represents an hour that is permitted, while a 0 represents an hour that is denied. If this parameter is not specified for a user, the group setting applies. The default group setting is 111111111111 and so on.
150	SET_STATIC_IP	UN, V1, V2	<p>Configures the (TACACS+ and RADIUS) IP address assignment for this user.</p> <p>V1 holds the IP address in the following format: xxx.xxx.xxx.xxx</p> <p>V2 should be one of the following:</p> <ul style="list-style-type: none"> • ALLOC_METHOD_STATIC—The IP address in V1 is assigned to the user in the format xxx.xxx.xxx.xxx. • ALLOC_METHOD_NAS_POOL—The IP pool named in V1 (configured on the AAA client) will be assigned to the user. • ALLOC_METHOD_AAA_POOL—The IP pool named in V1 (configured on the AAA server) will be assigned to the user. • ALLOC_METHOD_CLIENT—The dial-in client will assign its own IP address. • ALLOC_METHOD_AS_GROUP—The IP address assignment configured for the group will be used.
151	SET_CALLBACK_NO	UN GN, V1	<p>Sets the callback number for this user or group (TACACS+ and RADIUS). V1 should be one of the following:</p> <ul style="list-style-type: none"> • Callback number—The phone number the AAA client is to call back. • none—No callback is allowed. • roaming—The dial-up client determines the callback number. • as group—Use the callback string or method defined by the group.

Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Table E-5 lists the action codes for creating, modifying, and deleting TACACS+ and RADIUS settings for ACS groups and users. In the event that ACS has conflicting user and group settings, user settings always override group settings.

Transactions using these codes affect the configuration displayed in the User Setup and Group Setup sections of the web interface. For more information about the User Setup section, see [Chapter 6, “User Management.”](#) For more information about the Group Setup section, see [Chapter 5, “User Group Management.”](#)

Table E-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings

Action Code	Name	Required	Description
161	DEL_RADIUS_ATTR	UN GN, VN, Optionally V2, V3	<p>Deletes the named RADIUS attribute for the group or user, where:</p> <ul style="list-style-type: none"> • VN = “Vendor-Specific” • V2 = IETF vendor ID • V3 = VSA attribute ID <p>For example, to specify the Cisco IOS/PIX vendor ID and the Cisco AV Pair:</p> <pre>VN = "Vendor-Specific" V2 = "9" V3 = "1"</pre>

Table E-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
163	ADD_RADIUS_ATTR	UN GN, VN, V1, Optionally V2, V3	<p>Adds to the attribute named (VN) the value (V1) for the user/group (UN GN). For example, to set the IETF RADIUS Reply-Message attribute (attr. 18) for a group:</p> <pre>GN = "Group 1" VN = "Reply-Message" V1 = "Greetings"</pre> <p>As another example, to set the IETF RADIUS Framed-IP-Address attribute (attr. 9) for a user:</p> <pre>UN = "fred" VN = "Framed-IP-Address" V1 = "10.1.1.1"</pre> <p>To add a vendor-specific attribute (VSA), set VN = "Vendor-Specific" and use V2 and V3 as follows:</p> <ul style="list-style-type: none"> • V2 = IETF vendor ID • V3 = VSA attribute ID <p>For example, to add the Cisco IOS/PIX RADIUS cisco-av-pair attribute with a value of "addr-pool=pool1":</p> <pre>VN="Vendor-Specific" V1 = "addr-pool=pool1" V2 = "9" V3 = "1"</pre> <p>RADIUS attribute values can be one of the following:</p> <ul style="list-style-type: none"> • INTEGER • TIME • IP ADDRESS • STRING
170	ADD_TACACS_SERVICE	UN GN, VN, V1, V3, Optionally V2	<p>Permits the service for that user or group of users. For example:</p> <pre>GN = "Group 1" V1 = "ppp" V2 = "ip"</pre> <p>or</p> <pre>UN = "fred" V1 = "ppp" V2 = "ip"</pre> <p>or</p> <pre>UN = "fred" V1= "exec"</pre> <p>Note If a protocol is not specified for the PPP service, the default protocol is IP.</p>

Table E-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
171	REMOVE_TACACS_SERVICE	UN GN, V1 Optionally V2	<p>Denies the service for that user or group of users. For example:</p> <p>GN = "Group 1" V1 = "ppp" V2 = "ip"</p> <p>or</p> <p>UN = "fred" V1 = "ppp" V2 = "ip"</p> <p>or</p> <p>UN = "fred" V1 = "exec"</p> <p>This also resets the valid attributes for the service.</p>
172	ADD_TACACS_ATTR	UN GN, VN, V1, V3 Optionally V2	<p>Sets a service-specific attribute. The service must already have been permitted via the web interface or using Action 170:</p> <p>GN = "Group 1" VN = "routing" V1 = "ppp" V2 = "ip" V3 = "true"</p> <p>or</p> <p>UN = "fred" VN = "route" V1 = "ppp" V2 = "ip" V3 = 10.2.2.2</p>
173	REMOVE_TACACS_ATTR	UN GN, VN, V1 Optionally V2	<p>Removes a service-specific attribute:</p> <p>GN = "Group 1" V1 = "ppp" V2 = "ip" VN = "routing"</p> <p>or</p> <p>UN = "fred" V1 = "ppp" V2 = "ip" VN = "route"</p> <p>Note If a protocol is not specified for the ppp service, the default protocol is IP. In previous releases, all the protocols were enabled for the PPP service which caused the groups to enter an invalid state.</p>

Table E-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
174	ADD_IOS_COMMAND	UN GN, VN, V1	<p>Authorizes the given Cisco IOS command and determines if any arguments given to the command are to be found in a defined set or are not to be found in a defined set. The defined set is created using Actions 176 and 177:</p> <p>GN = "Group 1" VN = "telnet" V1 = "permit"</p> <p>or</p> <p>UN = "fred" VN = "configure" V1 = "deny"</p> <p>The first example permits the Telnet command to be authorized for users of Group 1. Any arguments can be supplied to the Telnet command as long as they are not matched against any arguments defined via Action 176.</p> <p>The second example permits the configure command to be authorized for user <i>fred</i>, but only if the arguments supplied are permitted by the filter defined by a series of Action 176.</p>
175	REMOVE_IOS_COMMAND	UN GN, VN	<p>Removes command authorization for the user or group:</p> <p>GN = "Group 1" VN = "telnet"</p> <p>or</p> <p>UN = "fred" VN = "configure"</p> <p>Users of Group 1 can no longer use the Cisco IOS telnet command.</p> <p>User fred can no longer use the configure command.</p>

Table E-5 Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)

Action Code	Name	Required	Description
176	ADD_IOS_COMMAND_ARG	UN GN, VN, V1, V2	<p>Specifies a set of command-line arguments that are permitted or denied for the Cisco IOS command contained in VN. The command must have already been added via Action 174:</p> <p>GN = "Group 1" VN = "telnet" V1 = "permit" V2 = "10.1.1.2"</p> <p>or</p> <p>UN = "fred" VN = "show" V1 = "deny" V2 = "run"</p> <p>The first example will allow the telnet command with argument 10.1.1.2 to be used by any user in Group 1.</p> <p>The second example ensures that user fred cannot issue the Cisco IOS command show run.</p>
177	REMOVE_IOS_COMMAND_ARG	UN GN, VN, V2	<p>Removes the permit or deny entry for the given Cisco IOS command argument:</p> <p>GN = "Group 1" VN = "telnet" V2 = "10.1.1.1"</p> <p>or</p> <p>UN = "fred" VN = "show" V2 = "run"</p>
178	SET_PERMIT_DENY_UNMATCHED_IOS_COMMANDS	UN GN, V1	<p>Sets unmatched Cisco IOS command behavior. The default is that any Cisco IOS commands not defined via a combination of Actions 174 and 175 will be denied. This behavior can be changed so that issued Cisco IOS commands that do not match any command/command argument pairs are authorized:</p> <p>GN = "Group 1" V1 = "permit"</p> <p>or</p> <p>UN = "fred" V1 = "deny"</p> <p>The first example will permit any command not defined by Action 174.</p>
179	REMOVE_ALL_IOS_COMMANDS	UN GN	This action removes all Cisco IOS commands defined for a particular user or group.
210	RENAME_GROUP	GN,V1	Renames an existing group to the name supplied in V1.

Table E-5 *Action Codes for Modifying TACACS+ and RADIUS Group and User Settings (continued)*

Action Code	Name	Required	Description
211	RESET_GROUP	GN	Resets a group back to the factory default.
212	SET_VOIP	GN, V1	Enables or disables Voice over IP (VoIP) support for the group named: <ul style="list-style-type: none"> GN = name of group V1 = ENABLE or DISABLE

Action Codes for Modifying Network Configuration

[Table E-6](#) lists the action codes for adding AAA clients, AAA servers, network device groups, and proxy table entries. Transactions using these codes affect the configuration that appears in the Network Configuration section of the web interface. For more information about the Network Configuration section, see [Chapter 3, “Network Configuration.”](#)

Table E-6 Action Codes for Modifying Network Configuration

Action Code	Name	Required	Description
220	ADD_NAS	VN, V1, V2, V3	<p>Adds a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and vendor (V3). Valid vendors are:</p> <ul style="list-style-type: none"> • VENDOR_ID_IETF_RADIUS—For IETF RADIUS. • VENDOR_ID_CISCO_RADIUS—For Cisco IOS/PIX RADIUS. • VENDOR_ID_CISCO_TACACS—For Cisco TACACS+. • VENDOR_ID_AIRSPACE_RADIUS—For Cisco Airespace RADIUS. • VENDOR_ID_ASCEND_RADIUS—For Ascend RADIUS. • VENDOR_ID_ALTIGA_RADIUS—For Cisco 3000/ASA/PIX 7.x+ RADIUS. • VENDOR_ID_AIRONET_RADIUS—For Cisco Aironet RADIUS. • VENDOR_ID_NORTEL_RADIUS—For Nortel RADIUS. • VENDOR_ID_JUNIPER_RADIUS—For Juniper RADIUS. • VENDOR_ID_CBBMS_RADIUS—For Cisco BBMS RADIUS. • VENDOR_ID_3COM_RADIUS—For Cisco 3COMUSR RADIUS. <p>For example:</p> <pre>VN = AS5200-11 V1 = 192.168.1.11 V2 = byZantine32 V3 = VENDOR_ID_CISCO_RADIUS</pre>
221	SET_NAS_FLAG	VN, V1	<p>Sets one of the per-AAA client flags (V1) for the named AAA client (VN). Use the action once for each flag required. Valid values for per-AAA client flags are:</p> <ul style="list-style-type: none"> • FLAG_SINGLE_CONNECT • FLAG_LOG_KEEP_ALIVE • FLAG_LOG_TUNNELS
222	DEL_HOST	VN	Deletes the named AAA client (VN).
223	ADD_NAS_BY_IETF_CODE	VN,V1, V2, V3	Adds a new AAA client (named in VN) with an IP address (V1), shared secret key (V2), and the enterprise code for the vendor (V3).

Table E-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
224	UPDATE_NAS	VN, V1, V2, V3	VN = AAA client Name V1 = IP-Address V2 = shared secret key V3 = vendor
225	READ_NAS	VN, V1(optional)	VN = output_file_name The output_file_name specifies the appliance filename in the FTP server. If the filename is not specified, the default filename <i>DumpNAS.txt</i> is used. An example of the absolute path for the ACS Windows version is: <i>C:\MyNAS\dump.txt</i> If no value is specified, the AAA client lists will be dumped to <i>ACS\bin\DumpNAS.txt</i> V1 = NDG name (optional). V1 should contain a valid NDG name.
230	ADD_AAA_SERVER	VN, V1, V2	Adds a new AAA server named (VN) with IP address (V1), shared secret key (V2).
231	SET_AAA_TYPE	VN, V1	Sets the AAA server type for server (VN) to value in V1, which should be one of the following: <ul style="list-style-type: none"> • TYPE_ACS • TYPE_TACACS • TYPE_RADIUS The default is AAA_SERVER_TYPE_ACS.
232	SET_AAA_FLAG	VN, V1	Sets one of the per-AAA client flags (V1) for the named AAA server (VN): <ul style="list-style-type: none"> • FLAG_LOG_KEEP_ALIVE • FLAG_LOG_TUNNELS Use the action once for each flag required.
233	SET_AAA_TRAFFIC_TYPE	VN, V1	Sets the appropriate traffic type (V1) for the named AAA server (VN): <ul style="list-style-type: none"> • TRAFFIC_TYPE_INBOUND • TRAFFIC_TYPE_OUTBOUND • TRAFFIC_TYPE_BOTH The default is TRAFFIC_TYPE_BOTH.
234	DEL_AAA_SERVER	VN	Deletes the named AAA server (VN).

Table E-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
240	ADD_PROXY	VN, V1, V2, V3	<p>Adds a new proxy markup (VN) with markup type (V1) strip markup flag (V2) and accounting flag (V3).</p> <p>The markup type (V1) must be one of the following:</p> <ul style="list-style-type: none"> • MARKUP_TYPE_PREFIX • MARKUP_TYPE_SUFFIX <p>The markup strip flag should be TRUE if the markup is to be removed from the username before forwarding.</p> <p>The accounting flag (V3) should be one of the following:</p> <ul style="list-style-type: none"> • ACCT_FLAG_LOCAL • ACCT_FLAG_REMOTE • ACCT_FLAG_BOTH
241	ADD_PROXY_TARGET	VN, V1	<p>Adds to named proxy markup (VN) the host name (V1). The host should already be configured in ACS.</p> <p>Note The order in which proxy targets are added sets the proxy search order; the first target added is the first target proxied to, and so on. The order must be changed through the web interface.</p>
242	DEL_PROXY	VN	Deletes the named proxy markup (VN).
250	ADD_NDG	VN	Creates a network device group (NDG) named (VN).
251	DEL_NDG	VN	Deletes the named NDG.
252	ADD_HOST_TO_NDG	VN, V1	Adds to the named AAA client/AAA server (VN) the NDG (V1).
270	SET_DCS_ASSIGNMENT	—	—
271	ADD_NDG_TO_DCS_MAPPING	—	—
300	RESTART_PROTO_MODULES	—	Restarts the CSRadius and CSTacacs services to apply new settings.

Table E-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
350	ADD_UDV	VN, V1, V2	<p>Adds a RADIUS vendor to the ACS vendor database. Vendors added to ACS by this method are known as User-Defined Vendors (UDV).</p> <p>VN contains the name of the Vendor.</p> <p>Note ACS adds <i>RADIUS(...)</i> to the name entered in the Variable Name field. For example, if you enter the name <i>MyCo</i>, ACS displays <i>RADIUS (MyCo)</i> in the web interface.</p> <p>V1 contains the user-defined vendor slot number or AUTO_ASSIGN_SLOT. ACS has ten vendor slots, numbered 0 through 9. If you specify AUTO_ASSIGN_SLOT, ACS selects the next available slot for your vendor.</p> <p>Note If you want to replicate UDV's between ACSs, you must assign the UDV to the same slot number on both ACSs.</p> <p>V2 contains the IANA-assigned enterprise code for the vendor.</p>
351	DEL_UDV	V1	<p>Removes the vendor with the IETF code specified in V1 and any defined VSAs.</p> <p>Note Action code 351 does not remove any instances of VSAs assigned to ACS groups or users. If ACS has AAA clients configured with the UDV specified in V1, the delete operation fails.</p>
352	ADD_VSA	VN, V1, V2, V3	<p>Adds a new VSA to the vendor specified by the vendor IETF code in V1.</p> <p>VN is the VSA name. If the vendor name is <i>MyCo</i> and the attribute is assigned a group ID, we recommend prefixing the vendor name or an abbreviation to all VSAs. For example, VSAs could be <i>MyCo-Assigned-Group-Id</i>.</p> <p>Note VSA names must be unique to the vendor and to the ACS dictionary. For example, <i>MyCo-Framed-IP-Address</i> is allowed but <i>Framed-IP-Address</i> is not, because <i>Framed-IP-Address</i> is used by IETF action code 8 in the RADIUS attributes.</p> <p>V2 is the VSA number. This must be in the 0-255 range.</p> <p>V3 is the VSA type as one of the following values:</p> <ul style="list-style-type: none"> • INTEGER • STRING • IPADDR <p>By default, VSAs are assumed to be outbound (or authorization) attributes. If the VSA is either multi-instance or used in accounting messages, use SET_VSA_PROFILE (Action code 353).</p>

Table E-6 Action Codes for Modifying Network Configuration (continued)

Action Code	Name	Required	Description
353	SET_VSA_PROFILE	V1, V2, V3	<p>Sets the inbound/outbound profile of the VSA. The profile specifies usage IN for accounting, OUT for authorization, or MULTI if more than a single instance is allowed per RADIUS message. Combinations are allowed.</p> <p>V1 contains the vendor IETF code.</p> <p>V2 contains the VSA number.</p> <p>V3 contains the profile, one of the following:</p> <p>IN OUT IN OUT MULTI OUT MULTI IN OUT</p>
354	ADD_VSA_ENUM	VN, V1, V2, V3	<p>Sets meaningful enumerated values, if the VSA attribute has enumerated. In the User Setup section, the ACS web interface displays the enumeration strings in a list.</p> <p>VN contains the VSA Enum Name.</p> <p>V1 contains the vendor IETF code.</p> <p>V2 contains the VSA number.</p> <p>V3 contains the VSA Enum Value.</p> <p>Example:</p> <p>VN = Disabled V1 = 9034 V2 = MyCo-Encryption V3 = 0</p> <p>or</p> <p>VN = Enabled V1 = 9034 V2 = MyCo-Encryption V3 = 1</p>
355	ADOPT_NEW_UDV_OR_VSA	—	<p>Restarts the CSAdmin, CSRadius, and CSLog services. These services must be restarted before new UDV or VSAs can become usable.</p>

ACS Attributes and Action Codes

This section complements the previous section by providing an inverse reference; it provides topics with tables that list ACS attributes, their data types and limits, and the action codes you can use to act upon the ACS attributes.

This section contains:

- [User-Specific Attributes, page E-24](#)
- [User-Defined Attributes, page E-25](#)

- [Group-Specific Attributes, page E-26](#)

User-Specific Attributes

[Table E-7](#) lists the attributes that define an ACS user, including their data types, limits, and default values. It also provides the action code you can use in accountActions to affect each attribute. Although there are many actions available, adding a user requires only one transaction: `ADD_USER`. You can safely leave other user attributes at their default values. The term NULL is not simply an empty string, but means not set; that is, the value will not be processed. Some features are processed only if they have a value assigned to them. For more information about action codes, see [Action Codes, page E-3](#).

Table E-7 *User-Specific Attributes*

Attribute	Actions	Logical Type	Limits	Default
Username	100, 101	String	1-64 characters	—
ASCII/PAP Password	100, 102	String	4-32 characters	Random string
CHAP Password	103	String	4-32 characters	Random string
Outbound CHAP Password	104	String	4-32 characters	NULL
TACACS+ Enable Password	105	String Password	4-32 characters	NULL
		Integer privilege level	0-15 characters	NULL
Group	106	String	0-100 characters	Default Group
Password Supplier	107	Enum	See Table E-3 .	LIBRARY_CSDB
Password Type	108	Enum	See Table E-3 .	PASS_TYPE_CSDB (password is cleartext PAP)
Password Expiry Status	109, 110	Bitwise Enum	See Table E-3 .	PASS_STATUS_NEVER (never expires)
Expiry Data	112, 113	Short wrong max/current	0-32,767	—
		Expiry date	—	—
Max Sessions	114	Unsigned short	0-65535	MAX_SESSIONS_AS_GROUP
TODDOW Restrictions	140	String	168 characters	111111111111
NAS Access Control	120, 122	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	
		ACL String (See Table E-4 .)	0-31 KB	
Dial-Up Access Control	121, 123	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	NULL
		ACL String (See Table E-4 .)	0-31 KB	NULL

Table E-7 *User-Specific Attributes (continued)*

Attribute	Actions	Logical Type	Limits	Default
Static IP Address	150	Enum scheme	(See Table E-4.)	Client
		String IP/Pool name	0-31 KB	NULL
Callback Number	151	String	0-31 KB	NULL
TACACS+ Attributes	170, 173	Formatted String	0-31 KB	NULL
RADIUS Attributes	160, 162	Formatted String	0-31 KB	NULL
UDF 1	1, 2	String Real Name	0-31 KB	NULL
UDF 2	1, 2	String Description	0-31 KB	NULL
UDF 3	1, 2	String	0-31 KB	NULL
UDF 4	1, 2	String	0-31 KB	NULL
UDF 5	1, 2	String	0-31 KB	NULL

User-Defined Attributes

User-defined attributes (UDAs) are string values that can contain any data, such as social security number, department name, telephone number, and so on. You can configure ACS to include UDAs on accounting logs about user activity. For more information about configuring UDAs, see [Customizing User Data, page 2-5](#).

RDBMS Synchronization can set UDAs by using the SET_VALUE action (code 1) to create a value called USER_DEFINED_FIELD_0 or USER_DEFINED_FIELD_1. For accountActions rows defining a UDA value, the AppId (AI) field must contain APP_CSAUTH and the Value2(V2) field must contain TYPE_STRING.

[Table E-8](#) lists the data fields that define UDAs. For more information about action codes, see [Action Codes, page E-3](#).

Table E-8 *User-Defined Attributes*

Action	Username (UN)	ValueName (VN)	Value1 (V1)	Value2 (V2)	AppId (AI)
1	fred	USER_DEFINED_FIELD_0	SS123456789	TYPE_STRING	APP_CSAUTH
1	fred	USER_DEFINED_FIELD_1	Engineering	TYPE_STRING	APP_CSAUTH
1	fred	USER_DEFINED_FIELD_2	949-555-1111	TYPE_STRING	APP_CSAUTH


Note

If more than two UDAs are created, only the first two are passed to accounting logs.

Group-Specific Attributes

[Table E-9](#) lists the attributes that define an ACS group, including their data types, limits, and default values. It also provides the action code that you can use in your accountActions table to affect each field. For more information about action codes, see [Action Codes](#), [page E-3](#).

Table E-9 *Group-Specific Attributes*

Attribute	Actions	Logical Type	Limits	Default
Max Sessions	114	Unsigned short	0-65534	MAX_SESSIONS_UNLIMITED
Max Sessions for user of group	115	Unsigned short	0-65534	MAX_SESSIONS_UNLIMITED
Token caching for session	130	Bool	T/F	NULL
Token caching for duration	131	Integer time in seconds	0-65535	NULL
TODDOW Restrictions	140	String	168 characters	111111111111
NAS Access Control	120, 122	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	
		ACL String (See Table E-4 .)	0-31 KB	
Dial-Up Access Control	121, 123	Bool enabled	T/F	NULL
		Bool permit/deny	T/F	NULL
		ACL String (See Table E-4 .)	0-31 KB	NULL
Static IP Address	150	Enum scheme	(See Table E-4 .)	Client
		String IP/Pool name	0-31 KB	NULL
RADIUS Attributes	160, 162	Formatted String	0-31 KB	NULL
TACACS+ Attributes	170, 173	Formatted String	0-31 KB	NULL
VoIP Support	212	Bool disabled	T/F	NULL

Using the RDBMS Synchronization Action Codes to Install User-Defined Vendor or VSA Data

Use the RDBMS Synchronization action codes to install VSA data for vendors that require extended VSA ID length. [Table 10](#) contains two additional codes and definitions for modifying the vendor configuration.

Table 10 RDBMS Account Action Codes and Definition for Vendor Configuration

Action Code	Name	Required	Description
356	SET_VSA_ID_LEN	V1, V2	Sets the Vendor-Specific Attribute (VSA) Type length in bytes. <ul style="list-style-type: none"> V1 contains the vendor IETF code. V2 contains VSA-Type Length, which takes the values 1, 2 or 4.
357	SET_VSA_INTERNAL_LEN	V1, V2	Sets the presence of Internal Length field in VSA. <ul style="list-style-type: none"> V1 contains the vendor IETF code. V2 contains BOOL value. 1-(TRUE) if VSA requires the Internal Length field. 0-(FALSE) if the Internal Length field is not required.

Action Codes for dACL Attributes

[Table E-11](#) lists the action codes for creating, reading, updating, and deleting dACL attributes. Transactions by using these codes affect the Shared Profile Components at the User-level Downloadable ACL or Group-level Downloadable ACL levels. The **User-level Downloadable ACLs** or **Group-level Downloadable ACLs** check box must be checked in the **Interface > Advanced Options** of the web interface. For more information about the Web Interface configuration, see [Chapter 2, “Advanced Options \(for Interface Configuration\)”](#).

Action codes 385, 386, 387, and 388 enable you to Read, Update and Delete dACLs, respectively.

You can specify NAFs and then use the dACL attribute definitions for the NAF. By default the dACLs content will be applied to all AAA clients.

Table E-11 Action Codes for Modifying dACL Attributes

Action Code	Name	Required	Description
380	CREATE_USER_DACL	UN GN, VN	<p>This action code associates a specified dACL with a User or Group. The dACL name specified should be valid and should be present in ACS. The codes are:</p> <p>UN = valid Username</p> <p>GN = Valid Group name (optional)</p> <p>VN = dACL name. (This dACL must be defined in Shared Profile Components).</p>
381	UPDATE_USER_DACL	UN GN, VN	<p>UN = Valid Username</p> <p>GN=Valid Group name (optional)</p> <p>VN = dACL name. (This dACL must be defined in Shared Profile Components).</p>
382	DELETE_USER_DACL	UN GN	<p>UN = Valid Username</p> <p>GN=Valid Group name (optional)</p>
385	CREATE_DACL	VN	<p>Use this action code to create a dACL.</p> <p>VN = <i><input_file_name></i></p> <p>where <i>input_file_name</i> is a text file that contains definitions for dACLs.</p> <p>On ACS for Windows, this file resides in a directory on the Windows machine that is running ACS.</p> <p>On the ACS SE, this file resides on an FTP server used with the ACS SE.</p> <p>You can specify the absolute file path, for example: <i>C:\DACL\create_DACL_for_User_1.txt</i>) for ACS for Windows.</p> <p>The dACL definition is ignored if it is already present, or contains an invalid definition, content name, content definition, or NAF name.</p>

Table E-11 Action Codes for Modifying dACL Attributes

Action Code	Name	Required	Description
386	READ_DACL	VN V1(optional)	<p>VN = contains dACL name or * for all dACLs.</p> <p>V1 = <output_file_name></p> <p>The output_file_name contains the exported dACLs' definition.</p> <p>The output_file_name specifies the appliance file name in the FTP server. If the filename is not specified, the default filename <i>DumpDACL.txt</i> is used.</p> <p>An example of the absolute path for the ACS Windows version is: <i>C:\temp\DACL.txt</i> By default the information will be exported to <i>DumpDACL.txt</i> in <i>ACS\bin</i> directory</p>
387	UPDATE_DACL	VN, V1(optional)	<p>VN = <input_file_name></p> <p>The input_file_name specifies the file which contains the definition for the dACL to be updated and specifies the appliance file name in the FTP server.</p> <p>An example of the absolute path for the ACS Windows version is: <i>C:\DACL\dump.txt</i></p> <p>V1 = DACL_REPLACE or DACL_APPEND</p> <p>The default option is DACL_REPLACE. The DACL_REPLACE option replaces the existing dACL with the new one.</p> <p>DACL_APPEND appends the new dACL content and its definitions to the existing dACL.</p>
388	DELETE_DACL	VN	<p>VN = dACL name, to delete.</p> <p>Enter a wildcard (*) to delete all.</p> <p>By default all the dACLs are deleted</p> <p>Users and groups that were associated with the deleted dACL will no longer be identified with the deleted dACL.</p>

Sample File Format for dACLs: DumpDACL.txt

```
[DACL#1]
Name = My_dACL_name
Description = My_Description
Content #1= content1
Content #2= content2
; NAF for Content1
Naf#1=My_NAF_Name1
; First Definition for content1
Definition#1#1= ACL_Command1_For_Content1
; Second Definition for content1
Definition#1#2= ACL_Command2_For_Content1
; NAF for Content2
Naf#2=My_NAF_Name2
; First Definition for content2
Definition#2#1= ACL_Command1_For_Content2
; Second Definition for content2
Definition#2#2= ACL_Command2_For_Content2
```

Sample File Format for Dump NAS: DumpNAS.txt

```
ADD_NAS:AAA_client_name: IP: ip_address: Key: shared_secret: NDG: ndg_name
```

An Example of accountActions

Table E-12 presents an sample instance of accountActions that contains some of the action codes described in [Action Codes](#), page E-3. First user *fred* is created, along with his passwords, including a TACACS_ Enable password with privilege level 10. Fred is assigned to *Group 2*. His account expires after December 31, 1999, or after 10 incorrect authentication attempts. Attributes for Group 2 include Time-of-Day/Day-of-Week restrictions, token caching, and some RADIUS attributes.



Note

This example omits several columns that should appear in any accountActions table. The omitted columns are Sequence ID (SI), Priority (P), DateTime (DT), Status (S), and MessageNo (MN).

Table E-12 Example accountActions Table

Action	User name (UN)	Group Name (GN)	Value Name (VN)	Value1 (V1)	Value2 (V2)	Value3 (V3)	Appld (AI)
100	fred	—	—	fred	—	—	—
102	fred	—	—	freds_password	—	—	—
103	fred	—	—	freds_chap_password	—	—	—
104	fred	—	—	freds_outbound_password	—	—	—
105	fred	—	—	freds_enable_password	10	—	—
106	fred	Group 2	—	—	—	—	—
150	fred	—	—	123.123.123.123	—	—	—
151	fred	—	—	01832-123900	—	—	—

Table E-12 Example accountActions Table (continued)

Action	User name (UN)	Group Name (GN)	Value Name (VN)	Value1 (V1)	Value2 (V2)	Value3 (V3)	Appld (AI)
109	fred	—	—	PASS_STATUS_NEVER	—	—	—
110	fred	—	—	PASS_STATUS_WRONG	—	—	—
110	fred	—	—	PASS_STATUS_EXPIRES	—	—	—
112	fred	—	—	10	—	—	—
113	fred	—	—	19991231	—	—	—
114	fred	—	—	50	—	—	—
115	fred	—	—	50	—	—	—
120	fred	—	—	ACCESS_PERMIT	—	—	—
121	fred	—	—	ACCESS_DENY	—	—	—
122	fred	—	—	NAS01, tty0, 01732-975374	—	—	—
123	fred	—	—	01732-975374, 01622-123123	CLID/ DNIS	—	—
1	fred	—	USER_DEFINED_FIELD_0	Fred Jones	TYPE_STRING	—	APP_CSAUTH
140	—	Group 2	—	[a string of 168 ones (1)]	—	—	—
130	—	Group 2	—	DISABLE	—	—	—
131	—	Group 2	—	61	—	—	—
163	—	Group 2	Reply-Message	Welcome to Your Internet Service	—	—	—
163	—	Group 2	Vendor-Specific	addr-pool=pool2	9	1	—



APPENDIX F

Internal Architecture

This appendix describes the architectural components of the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS. ACS is modular and flexible to fit the needs of simple and large networks. This appendix includes the following topics:

- [Windows Services, page F-1](#)
- [Windows Registry \(ACS for Windows Only\), page F-2](#)
- [Solution Engine Services, page F-3](#)
- [CSAdmin, page F-7](#)
- [CSAgent \(ACS SE Only\), page F-8](#)
- [CSAuth, page F-9](#)
- [CSDBSync, page F-9](#)
- [CSLog, page F-9](#)
- [CSMon, page F-10](#)
- [CSTacacs and CSRADIUS, page F-12](#)
- [Disabling NetBIOS, page F-12](#)

Windows Services

ACS includes the following service modules:

- **CSAdmin**
- **CSAuth**
- **CSDBSync**
- **CSLog**
- **CSMon**
- **CSTacacs**
- **CSRADIUS**

You can stop or restart ACS services as a group, except for **CSAdmin**, by using the ACS web interface. For more information, see [Service Control, page 7-1](#).

ACS for Windows

You can start, stop, and restart individual ACS services from the Services window in the Control Panel.

ACS SE

You can start, stop, and restart individual ACS services from the appliance serial console. For more information about starting, stopping, and restarting services by using the serial console, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Windows Registry (ACS for Windows Only)



Warning

Do not modify the Windows Registry unless you have enough knowledge and experience to edit the file without destroying or corrupting crucial data.

Only general ACS application information (such as the installation directory location) will continue to use the Windows registry.

The ACS information is located in the following Windows Registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\CISCO`

Unless a Cisco representative advises you to do so, we strongly recommend that you do not modify Windows Registry settings pertaining to ACS.

SQL Registry

In order to create a unified data storage model, ACS has moved from multiple data storages to a standard SQL-based relational database.

The SQL registry contains table information on all user and configuration data. SQL data is not made available for viewing and is protected by an encrypted password.

SQL Tables	Description
ConfigKey	Information that is not stored in the other tables. The data corresponds to registry keys.
ConfigValue	Data corresponding to registry values.
DictKey	Tree of attribute keys. The data is corresponds to registry keys of the ACS dictionary.
DictValue	Values for attributes keys from the ACSDictionaryKeys table.
Host	Information regarding all hosts in ACS.
HostService	Additional data for hosts of type remote agent.
Admin	ACS administrators. The permissions for each administrator are represented as a bitset inside a binary blob.
NetworkModel	Network model section.
Users	All user-specific information that was previously stored in the <i>user.dat</i> file. This table structure represents ACS UDB_ACCOUNT structure. However, some fields will not appear.
VarsDB	Currently in use but will be moved to a new table.

Solution Engine Services

The ACS SE includes the CSAgent service in addition to the Windows services.

The operating system for the ACS SE is customized version of the Windows 2003 R2 operating system which is minimized for performance. The ACS SE removes all extraneous services, blocks all unused ports, and prevents all other access to the ACS server system, thereby dramatically increasing the security posture of the Solution Engine.

The minimization of the operating system's services is reflected as follows:

- [Operating System Services the ACS SE Automatically Runs](#), page F-3
- [Disabled Operating System Services in the ACS SE](#), page F-4

Operating System Services the ACS SE Automatically Runs

[Table F-1](#) lists the operating services that the ACS SE automatically runs.

Table F-1 *Operating Services that the ACS SE Automatically Runs*

Service Name	Description
COM+ Event System	Provides automatic distribution of events to subscribing COM components.
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.
DNS Client	Resolves and caches Domain Name System (DNS) names.
Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.
License Logging Service	Tracks Client Access License usage for a server product.
Logical Disk Manager	Performs the Logical Disk Manager Watchdog Service.
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view local area network and remote connections.
Plug and Play	Manages device installation and configuration and notifies programs of device changes.
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.
Removable Storage	Manages removable media, drives, and libraries.

Table F-1 *Operating Services that the ACS SE Automatically Runs*

Service Name	Description
RunAs Service	Enables starting processes under alternate credentials.
Security Accounts Manager	Stores security information for local user accounts.
Server	Provides RPC support and file, print, and named pipe sharing.
System Event Notification	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.
Telnet	Allows a remote user to log on to the system and run console programs by using the command line.
Windows Management Instrumentation	Provides system management information.
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.

Disabled Operating System Services in the ACS SE

[Table F-2](#) below lists the operating system services that are not run on the ACS SE.

Table F-2 *Operating System Services Not Run on the ACS SE*

Service Name	Description
Alerter	Notifies selected users and computers of administrative alerts.
Application Management	Provides software installation services such as Assign, Publish, and Remove.
Automatic Updates	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.
Background Intelligent Transfer Service	Transfers files in the background by using idle network bandwidth. If the service is stopped, features such as Windows Update, and MSN Explorer will be unable to automatically download programs and other information. If this service is disabled, any services
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.
Distributed File System	Manages logical volumes distributed across a local or wide area network.

Table F-2 **Operating System Services Not Run on the ACS SE (continued)**

Service Name	Description
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction-protected resource managers.
Fax Service	Helps you send and receive faxes.
File Replication	Maintains file synchronization of file directory contents among multiple servers.
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.
Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.
Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.
Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.
Logical Disk Manager Administrative Service	Performs administrative service for disk management requests.
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop by using NetMeeting.
Network DDE	Provides network transport and security for dynamic data exchange (DDE).
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.
Performance Logs and Alerts	Configures performance logs and alerts.
Print Spooler	Loads files to memory for later printing.
QoS RSVP	Provides network signaling and local traffic control setup functionality for Quality of Service (QoS)-aware programs and control applets.

Table F-2 **Operating System Services Not Run on the ACS SE (continued)**

Service Name	Description
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.
Remote Access Connection Manager	Creates a network connection.
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.
Remote Registry Service	Allows remote Registry manipulation.
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.
Task Scheduler	Enables a program to run at a designated time.
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.
Telephony API (TAPI)	Provides Telephony API (TAPI) support for programs that control telephony devices and IP-based voice connections on the local computer and, through the LAN, on servers that are also running the service.
Terminal Services	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.
Utility Manager	Starts and configures accessibility tools from one window.
WMDM PMSP Service	-
Workstation	Provides network connections and communications.
Windows Installer	Installs, repairs, and removes software according to instructions contained in the .msi files.
Windows Time	Sets the computer clock.

Packet Filtering

Packet Filtering is the service that blocks the traffic on all but necessary IP ports.

[Table F-3](#) lists the ports that are open for input traffic for the ACS SE.

Table F-3 *Input Traffic Open Ports for the Packet Filter*

Service Name	UDP	TCP
DHCP	68	
RADIUS authentication & authorization (original draft RFC)	1645	
RADIUS accounting (original draft RFC)	1646	
RADIUS authentication & authorization (revised RFC)	1812	
RADIUS accounting (original draft RFC)	1813	
Proxy DLLs (RSA)	5500-5509	
TACACS+ authentication, authorization & accounting		49
ACS replication		2000
ACS logging		2001
ACS distributed logging		2003
ACS HTTP admin		2002
ACS HTTPS admin		2002
ACS administration port range		Dynamic

CSAdmin

CSAdmin is the service that provides the web server for the ACS web interface. After ACS is installed, you must configure it from its web interface; therefore, **CSAdmin** must be running when you configure ACS.

Because the ACS web server uses port 2002, rather than the standard port 80 that is usually associated with HTTP traffic, you can use another web server on the same machine to provide other web services. We have not performed interoperability testing with other web servers, but unless a second web server is configured to use either port 2002 or one of the ports within the range specified in the HTTP Port Allocation feature, you should not encounter port conflicts for HTTP traffic. For more information about the HTTP Port Allocation feature, see [Configuring Access Policy, page 11-8](#) and [Access Policy Setup Page, page 11-18](#).

Although you can start and stop services from within the ACS web interface, you cannot start or stop **CSAdmin**.

ACS for Windows

If **CSAdmin** stops abnormally because of an external action, you cannot access ACS from any computer other than the Windows server on which it is running. You can start or stop **CSAdmin** from the Windows Control Panel.

ACS SE

If **CSAdmin** stops abnormally because of an external action, you can restart the service by using only the appliance serial console. For more information about starting, stopping, and restarting services by using the serial console, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

Both Platforms

CSAdmin is multi-threaded, which enables several ACS administrators to access it at the same time. Therefore, **CSAdmin** is well suited for distributed, multiprocessor environments.

CSAgent (ACS SE Only)

CSAgent is the service that is used for protecting the ACS SE from viruses, worms, and attacks. CSAgent operates in standalone mode on the Solution Engine. You can start, stop, and restart the CSAgent using the serial console. For more information about starting, stopping, and restarting services by using the serial console, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

**Note**

The CSAgent imposes the following restrictions on ACS when it is enabled. You cannot apply upgrades or patches by using the Appliance Upgrade Status page in the System Configuration section or the upgrade command on the appliance console. To upgrade ACS or apply patches, CSAgent must be disabled.

CSAgent Policies

The CSAgent service for the ACS SE is configured with the following policies:

- **Application Control**—CSAgent permits execution applications that are required for ACS to operate correctly.
- **File Access Control**—CSAgent permits file system access for applications that are required for ACS to operate correctly.
- **IP and Transport Control**—CSAgent provides the following protections:
 - Discards invalid IP headers.
 - Discards invalid transport headers.
 - Detects TCP/UDP port scans.
 - Cloaks the appliance to prevent port scans.
 - Prevents TCP blind session spoofing.
 - Prevents TCP SYN floods.
 - Blocks ICMP covert channels.
 - Blocks dangerous ICMP messages, including ping.
 - Prevents IP source routing.
 - Prevents trace routing.
- **E-mail Worm Protection**—CSAgent guards the appliance against e-mail worms.
- **Registry Access Control**—CSAgent permits registry access to only those applications requiring access for proper operation of the appliance.

- **Kernel Protection**—CSAgent does not allow kernel modules to be loaded after system startup is complete.
- **Trojan and Malicious Application Protection**—CSAgent provides the following protections. Applications cannot:
 - Write code to space owned by other applications.
 - Download and execute ActiveX controls.
 - Automatically execute downloaded programs.
 - Directly access operating system password information.
 - Write into memory owned by other processes.
 - Monitor keystrokes while accessing the network.

CSAuth

CSAuth is the authentication and authorization service. It permits or denies access to users by processing authentication and authorization requests. **CSAuth** determines if access should be granted and defines the privileges for a particular user. **CSAuth** is the ACS database manager.

To authenticate users, ACS can use the internal database or one of many external databases. When a request for authentication arrives, ACS checks the database that is configured for that user. If the user is unknown, ACS checks the database(s) configured for unknown users. For more information about how ACS handles authentication requests for unknown users, see [About Unknown User Authentication, page 15-3](#).

For more information about the various database types supported by ACS, see [Chapter 12, “User Databases.”](#)

When a user has authenticated, ACS obtains a set of authorizations from the user profile and the group to which the user is assigned. This information is stored with the username in the ACS internal database. Some of the authorizations included are the services to which the user is entitled, such as IP over PPP, IP pools from which to draw an IP address, access lists, and password-aging information. The authorizations, with the approval of authentication, are then passed to the **CSTacacs** or **CSRADIUS** modules to be forwarded to the requesting device.

CSDBSync

CSDBSync is the service used to synchronize the ACS database with third-party relational database management system (RDBMS) systems. **CSDBSync** synchronizes AAA client, AAA server, network device groups (NDGs) and Proxy Table information with data from a table in an external relational database. For information on RDBMS Synchronization, see [RDBMS Synchronization, page 8-17](#).

CSLog

CSLog is the service used to capture and place logging information. **CSLog** gathers data from the TACACS+ or RADIUS packet and **CSAuth**, and then manipulates the data to be placed into the comma-separated value (CSV) files. CSV files can be imported into spreadsheets that support this format.

CSMon

CSMon is a service that helps minimize downtime in a remote access network environment. **CSMon** works for TACACS+ and RADIUS and automatically detects which protocols are in use.

You can use the ACS web interface to configure the **CSMon** service. The ACS Active Service Management feature provides options for configuring **CSMon** behavior. For more information, see [ACS Active Service Management, page 7-18](#).



Note

CSMon is not intended as a replacement for system, network, or application management applications but is provided as an application-specific utility that can be used with other, more generic system management tools.

CSMon performs four basic activities, outlined in the following topics:

- [Monitoring, page F-10](#)
- [Recording, page F-11](#)
- [Notification, page F-11](#)
- [Response, page F-11](#)

Monitoring

CSMon monitors the overall status of ACS and the system on which it is running. **CSMon** actively monitors three basic sets of system parameters:

- **Generic host system state**—**CSMon** monitors the following key system thresholds:
 - Available hard disk space
 - Processor utilization
 - Physical memory utilization

All events related to generic host system state are categorized as warning events.

- **Application-specific performance**
 - **Application viability**—**CSMon** periodically performs a test login by using a special built-in test account (the default period is one minute). Problems with this authentication can be used to determine if the service has been compromised.
 - **Application performance thresholds**—**CSMon** monitors and records the latency of each test authentication request (the time it takes to receive a positive response). Each time this is performed, **CSMon** updates a variable containing the average response time value. Additionally, it records whether retries were necessary to achieve a successful response. By tracking the average time for each test authentication, **CSMon** can build up a picture of expected response time on the system in question. **CSMon** can therefore detect whether excess retries are required for each authentication or if response times for a single authentication exceed a percentage threshold over the average.
 - **System resource consumption by ACS**—**CSMon** periodically monitors and records the usage by ACS of a small set of key system resources and compares it against predetermined thresholds for indications of atypical behavior. The parameters monitored include the following:
 - Handle counts

- Memory utilization
- Processor utilization
- Thread used
- Failed log-on attempts

CSMon cooperates with **CSAuth** to keep track of user accounts being disabled by exceeding their failed attempts count maximum. This feature is more oriented to security and user support than to system viability. If configured, it provides immediate warning of brute-force attacks by alerting the administrator to a large number of accounts becoming disabled. In addition, it helps support technicians anticipate problems with individual users gaining access.

Recording

CSMon records exception events in logs that you can use to diagnose problems.

- **CSMon Log**—Like the other ACS services, **CSMon** maintains a CSV log of its own for diagnostic recording and error logging. Because this logging consumes relatively small amounts of resources, **CSMon** logging cannot be disabled.
- **Windows Event Log**—**CSMon** can log messages to the Windows Event Log. Logging to the Windows Event Log is enabled by default but can be disabled.

Notification

CSMon can be configured to notify system administrators in the following cases:

- Exception events
- Response
- Outcome of the response

Notification for exception events and outcomes includes the current state of ACS at the time of the message. The default notification method is simple mail-transfer protocol (SMTP) e-mail, but you can create scripts to enable other methods.

Response

CSMon detects exception events that affect the integrity of the service. For information about monitored events, see [Monitoring, page F-10](#). These events are application-specific and hard-coded into ACS. The two types of responses are:

- **Warning events**—Service is maintained but some monitored threshold is breached.
- **Failure events**—One or more ACS components stop providing service.

CSMon responds to the event by logging the event, sending notifications (if configured) and, if the event is a failure, taking action. The two types of actions are:

- **Predefined actions**—These actions are hard-coded into the program and are always carried out when a triggering event is detected. Because these actions are hard-coded, they are integral to the application and do not need to be configured. These actions include running the **CSSupport** utility, which captures most of the parameters dealing with the state of the system at the time of the event.

If the event is a warning event, it is logged and the administrator is notified. No further action is taken. **CSMon** also attempts to fix the cause of the failure after a sequence of retries and individual service restarts.

- **Customer-Definable Actions**—If the predefined actions built into **CSMon** do not fix the problem, **CSMon** can execute an external program or script.

CSTacacs and CSRADIUS

The **CSTacacs** and **CSRADIUS** services communicate between the **CSAuth** module and the access device that is requesting authentication and authorization services. For **CSTacacs** and **CSRADIUS** to work properly, the system must meet the following conditions:

- **CSTacacs** and **CSRADIUS** services must be configured from **CSAdmin**.
- **CSTacacs** and **CSRADIUS** services must communicate with access devices such as access servers, routers, switches, and firewalls.
- The identical shared secret (key) must be configured both in ACS and on the access device.
- The access device IP address must be specified in ACS.
- The type of security protocol being used must be specified in ACS.

CSTacacs is used to communicate with TACACS+ devices and **CSRADIUS** to communicate with RADIUS devices. Both services can run at the same time. When only one security protocol is used, only the applicable service needs to be running; however, the other service will not interfere with normal operation and does not need to be disabled. For more information about TACACS+ AV pairs, see [Appendix A, “TACACS+ Attribute-Value Pairs.”](#) For more information about RADIUS+ AV pairs, see [Appendix B, “RADIUS Attributes.”](#)

Disabling NetBIOS

NetBIOS (Network Basic Input/Output System) is a program that allows applications on different computers to communicate within a LAN. Since the late 1980s, Microsoft has adopted NetBIOS as its LAN Manager product, and, from there, it found its way into early versions of Windows and all the way into Windows NT.

Since the Windows 2000 release, DNS has become the default name resolution method for Windows-based networks and is required if you want to deploy Active Directory domains.

Although you can use Windows 2000, Windows XP, and Windows Server 2003 to disable NetBIOS over TCP/IP (NetBT), many corporate networks remain reluctant to do so, since most of them still have legacy (Windows 9x or Windows NT) machines on their network. These machines need NetBIOS to function properly on a network, since they use NetBIOS to log in to domains, find one another, and establish sessions for accessing shared resources.

However, with networks that are free of legacy systems, administrators may want to consider disabling the NetBT transport on all of the computers. ACS supports the Windows server with NetBIOS disabled.

For more details about disabling NetBIOS, refer to your Windows Operating system guide.



INDEX

Numerics

3COMUSR

settings [2-14](#)

A

AAA

See also AAA clients

See also AAA servers

pools for IP address assignment [6-7](#)

AAA clients [1-1](#)

adding and configuring [3-12](#)

configuration management [8-18](#)

configuring [3-8](#)

deleting [3-14](#)

editing [3-13](#)

IP pools [6-7](#)

multiple IP addresses for [3-8](#)

number of [1-22](#)

searching for [3-6](#)

table [3-1](#)

timeout values [15-6](#)

AAA protocols

TACACS+ and RADIUS [1-3](#)

AAA-related logs [10-1](#)

AAA servers [1-3](#)

adding [3-17](#)

configuring [3-15](#)

deleting [3-18](#)

editing [3-17](#)

enabling in interface (table) [2-15](#)

functions and concepts [1-3](#)

in distributed systems [3-2](#)

master [8-2](#)

overview [3-15](#)

primary [8-2](#)

replicating [8-2](#)

searching for [3-6](#)

secondary [8-2](#)

accessing Cisco Secure ACS

how to [2-3](#)

URL [1-21](#)

with SSL enabled [1-21](#)

Account Actions

RDBMS Setup [8-33](#)

accountActions codes

ADD_USER [E-5](#)

CREATE_DACL [E-28](#)

CREATE_USER_DACL [E-28](#)

deleting [8-26](#)

READ_DACL [8-25](#)

READ_NAS [8-23](#)

UPDATE_DACL [8-26](#)

UPDATE_NAS [8-23](#)

accountActions File [8-29](#)

accountActions table [8-27, 8-28](#)

account disablement

Account Disabled check box [6-3](#)

manual [6-38](#)

resetting [6-40](#)

setting options for [6-13](#)

accounting

See also logging

administrative [1-15](#)

overview [1-15](#)

- RADIUS [1-15](#)
- TACACS+ [1-15](#)
- VoIP [1-15](#)
- accounting logs
 - updating packets [10-37](#)
- Account Never Expires option [11-3](#)
- ACLs
 - See downloadable IP ACLs
 - default [14-12](#)
- ACS
 - additional features [1-5](#)
 - features, functions and concepts [1-3](#)
 - internal database [1-3](#)
 - introduction to [1-1](#)
 - managing and administrating [1-16](#)
 - specifications [1-22](#)
 - Windows Services [1-23](#)
- ACS internal database
 - See also databases
 - overview [12-1](#)
 - password encryption [12-2](#)
 - replication [2-15](#)
- action codes
 - for creating and modifying user accounts [E-5](#)
 - for initializing and modifying access filters [E-10](#)
 - for modifying network configuration [E-18](#)
 - for modifying TACACS+ and RADIUS settings [E-13](#)
 - for setting and deleting values [E-4](#)
 - in accountActions [E-3](#)
- Active Service Management
 - See Cisco Secure ACS Active Service Management
- ADD_USER [E-5](#)
- adding
 - external audit servers [13-25](#)
 - external servers [13-22, 13-23](#)
- ADF
 - importing for vendors [13-13](#)
- Administration Audit logs [10-5](#)
- administrative accounting [1-15](#)
- administrative sessions
 - and HTTP proxy [2-2](#)
 - network environment limitations of [2-1](#)
 - through firewalls [2-2](#)
 - through NAT (network address translation) [2-2](#)
- Administrator Entitlements reports [10-12](#)
- administrators
 - See also Administration Audit log
 - See also Administration Control
 - See also administrative access policies
 - deleting [11-7](#)
 - locked out [11-3](#)
 - locking out [11-18](#)
 - unlocking [11-3](#)
- Agentless Host for L2 and L3 template [14-20](#)
- AES 128 algorithm [12-2](#)
- age-by-date rules for groups [5-18](#)
- Agentless Host for L2 (802.1x Fallback) [14-17](#)
- Agentless Host for L2 Template [14-17](#)
- Agentless Request Processing [14-24](#)
- Aironet
 - AAA client configuration [3-10](#)
 - RADIUS parameters for group [5-30](#)
 - RADIUS parameters for user [6-27](#)
- anonymous TLS renegotiation [9-16](#)
- appliance
 - configuration [7-22](#)
- Appliance Administration Audit logs [10-5](#)
- Appliance Status report [10-11](#)
 - viewing [10-35](#)
- ARAP [1-9](#)
 - in User Setup [6-4](#)
- attribute definition file
 - see also ADF [13-13](#)
- attributes [13-5](#)
 - adding [8-47](#)
 - adding external audit device types [C-40](#)
 - definition file [8-44](#)
 - definition file sample [8-51](#)

- deleting [8-48](#)
- dumping [8-50](#)
- enabling in interface [2-5](#)
- exporting [8-50](#)
- extended entity [8-49](#)
- extended property [8-50](#)
- group-specific (table) [E-26](#)
- logging [10-3](#)
- management [8-44](#)
- NAC (posture validation) [8-44](#)
- per-group [2-5](#)
- per-user [2-5](#)
- posture validation (NAC) [8-44](#)
- user-specific (table) [E-25](#)
- attribute-value pairs
 - See AV (attribute value) pairs
- audit device types
 - external, adding attributes [C-40](#)
- audit logs [10-5](#)
- audit server
 - functionality [14-30](#)
 - setting up [13-25](#)
- audit servers
 - setting up [13-25](#)
- Authenticate MAC With [14-47](#)
- authentication [1-7](#)
 - configuration [9-21](#)
 - configuring policies [14-27](#)
 - considerations [1-7](#)
 - denying unknown users [15-9](#)
 - options [9-21](#)
 - overview [1-7](#)
 - protocol-database compatibility [1-8](#)
 - request handling [15-3](#)
 - user databases [1-7](#)
 - via external user databases [12-4](#)
 - Windows [12-7](#)
- authorization [1-12](#)
 - configuring policies [14-34](#)

- ordering rules [14-37](#)
- rules [14-34](#)
- sets
 - See command authorization sets
- setsSee command authorization sets
- AV (attribute value) pairs
 - See also RADIUS VSAs (vendor specific attributes)
- RADIUS
 - Cisco IOS [B-3](#)
 - IETF [B-11](#)
- TACACS+
 - accounting [A-3](#)
 - general [A-1](#)
- Available Credentials [14-48](#)
- AV pairs [14-11](#)

B

- Backup and Restore logs [10-5](#)
- backups
 - components backed up [7-9](#)
 - directory management [7-9](#)
 - disabling scheduled [7-14](#)
 - filename [7-9](#)
 - filenames [7-15](#)
 - locations [7-9](#)
 - manual [7-11](#)
 - options [7-10](#)
 - overview [7-8](#)
 - reports [7-10](#)
 - scheduled vs. manual [7-8](#)
 - scheduling [7-12](#)
 - vs. replication [8-6](#)
 - with CSUtil.exe [C-3](#)
- browsers
 - See also web interface [1-19](#)

C

cab file [7-25](#)

cached users

See discovered users

CA configuration [9-28](#)

callback options

in Group Setup [5-5](#)

in User Setup [6-6](#)

cascading replication [8-4, 8-9](#)

cautions

significance of [I-XXIX](#)

certificate database for LDAP servers [12-47](#)

DB path [12-30](#)

trusted root CA [12-30](#)

certificate trust list

see CTL

certification

See also EAP-TLS

See also PEAP

adding certificate authority certificates [9-26](#)

background [9-1](#)

backups [7-9](#)

Certificate Revocation Lists [9-29](#)

certificate signing request generation [9-32](#)

deleting the certificate from the Certificate Trust List [9-29](#)

editing the certificate trust list [9-28](#)

replacing certificate [9-36](#)

self-signed certificates

configuring [9-35](#)

NAC [13-13](#)

overview [9-33](#)

server certificate installation [9-22](#)

updating certificate [9-36](#)

Change Password page [11-4](#)

CHAP [1-9](#)

in User Setup [6-4](#)

Cisco

Identity-Based Networking Services (IBNS) [1-2](#)

Cisco Discovery Protocol [2-12](#)

Cisco IOS

RADIUS

AV (attribute value) pairs [B-2](#)

group attributes [5-28](#)

user attributes [6-26](#)

TACACS+ AV (attribute value) pairs [A-1](#)

Cisco Secure ACS Active Service Management

event logging configuration [7-20](#)

overview [7-18](#)

system monitoring

configuring [7-19](#)

custom actions [7-19](#)

Cisco Secure ACS administration overview [1-16](#)

Cisco Secure ACS backups

See backups

Cisco Secure ACS system restore

See restore

CiscoSecure Authentication Agent [5-16](#)

Cisco Secure DBSync [8-20](#)

Cisco Security Agent [1-17](#)

See also CSAgent

integration [1-17](#)

logging [1-17](#)

policies [1-18](#)

restrictions [1-18](#)

viewing logs [7-27](#)

CLID-based filters [4-20](#)

cloning

Network Access Profiles [14-6](#)

policies or rules [13-20](#)

codes

See action codes

collect log files

diagnostic log information [7-25](#)

collect previous days logs

archive system logs [7-25](#)

collect user database

- ACS internal database collection in support file [7-25](#)
- command authorization sets
 - See also shell command authorization sets
 - adding [4-29](#)
 - configuring [4-25, 4-29](#)
 - deleting [4-31](#)
 - editing [4-30](#)
 - overview [4-25](#)
 - pattern matching [4-28](#)
 - PIX command authorization sets [4-25](#)
- command-line database utility
 - See CSUtil.exe
- condition sets, defining [13-17](#)
- configuration provider
 - remote agent logs on [10-28](#)
- configuring
 - internal policies [13-17](#)
- configuring advanced filtering
 - Network Access Profiles [14-2](#)
- conventions [I-XXVIII](#)
- copying
 - policies or rules [13-20](#)
- CREATE_DACL [E-28](#)
- CREATE_USER_DACL [E-28](#)
- creating
 - external servers [13-22, 13-23](#)
- credentials [13-5](#)
- Credential Validation Databases [14-27, 14-46](#)
- critical loggers [10-23](#)
- Critical Loggers Configuration Page [10-38](#)
- CRLs [9-29](#)
- CSAdmin
 - Windows Services [1-23](#)
- CSAdmin service [7-2](#)
- CSAgent [F-8](#)
 - behavior [1-18](#)
 - disabling [7-22](#)
 - enabling [7-22](#)
 - logging [1-17](#)
 - overview [1-17](#)
 - policies [1-18](#)
- CSAgent service [1-17, 7-2](#)
- CSAuth
 - Windows Services [1-23](#)
- CSDBSync [8-27](#)
 - Windows Services [1-23](#)
- CSLog
 - Windows Services [1-23](#)
- CSMon
 - See also Cisco Secure ACS Active Service Management
 - configuration [F-10](#)
 - log [F-11](#)
 - windows Services [1-23](#)
- CSNTacctInfo [12-41, 12-42, 12-43](#)
- CSNTAuthUserPap [12-39](#)
- CSNTerrorString [12-41, 12-42, 12-43](#)
- CSNTextractUserClearTextPw [12-40](#)
- CSNTfindUser [12-40](#)
- CSNTgroups [12-41, 12-42, 12-43](#)
- CSNTpasswords [12-40, 12-42](#)
- CSNTresults [12-41, 12-42, 12-43](#)
- CSNTusernames [12-40, 12-41, 12-42](#)
- CSRadius [F-12](#)
 - Windows Services [1-23](#)
- CSTacacs [F-12](#)
 - Windows Services [1-23](#)
- CSUtil.exe
 - add and delete posture validation attributes [C-29](#)
 - adding external audit device type attributes [C-40](#)
 - backing up with [C-3](#)
 - cleaning up database with [C-8](#)
 - decoding error numbers with [C-17](#)
 - dumping database file with [C-6](#)
 - exporting data with [C-15](#)
 - exporting group information with [C-16](#)
 - import text file (example) [C-15](#)
 - initializing database with [C-5](#)

- loading database file with [C-7](#)
- overview [C-1](#)
- restoring with [C-4](#)
- updating database with [C-9](#)
- CSV (comma-separated values) logs
 - configuring [10-24](#)
 - downloading [10-33](#)
 - enabling and disabling [10-24](#)
 - filename formats [10-31](#)
 - locations [10-6](#)
 - logging to [10-6](#)
 - size and retention [10-7](#)
 - viewing [10-31](#)
- CSV file
 - local [8-18](#)
 - RDBMS Synchronization [8-18](#)
- CSV log File Configuration Page [10-40](#)
- CTL
 - external policy servers
- CTL editing [9-28](#)
- custom attributes
 - in group-level TACACS+ settings [5-22](#)
 - in user-level TACACS+ settings [6-15](#)
- customer support
 - collecting data for [10-29](#)
 - providing package.cab file [10-29](#)

D

- database group mappings
 - configuring
 - for token servers [16-2](#)
 - for Windows domains [16-6](#)
 - no access groups [16-4](#)
 - order [16-8](#)
 - deleting
 - group set mappings [16-7](#)
 - Windows domain configurations [16-7](#)
- Database Replication logs [10-5](#)

- databases
 - See also external user databases
 - ACS internal database [12-1](#)
 - authentication search process [15-3](#)
 - cleaning up [C-8](#)
 - deleting [12-57](#)
 - external
 - See also external user databases
 - See also Unknown User Policy
 - initializing [C-5](#)
 - remote agent selection [12-17](#)
 - replication
 - See replication
 - search order [15-7](#)
 - search process [15-7](#)
 - selecting user databases [12-1](#)
 - synchronization
 - See RDBMS synchronization
 - token cards
 - See token servers
 - types
 - See generic LDAP user databases
 - See LEAP proxy RADIUS user databases
 - See ODBC features
 - See RADIUS user databases
 - unknown users [15-1](#)
 - user databases [6-2](#)
 - user import methods [12-2](#)
 - Windows user databases [12-5](#)
- data source names
 - for ODBC logging [10-9](#)
 - for RDMBS synchronization [8-33](#)
 - using with ODBC databases [12-35, 12-44, 12-45](#)
- data types, NAC attribute [13-6](#)
- date and time setting [7-23](#)
- date format control [7-3](#)
- debug logs, detail levels [10-29](#)
- default ACLs [14-12](#)
- default group

- in Group Setup [5-2](#)
 - mapping for Windows [16-4](#)
- default time-of-day/day-of-week specification [2-14](#)
- default time-of-day access settings for groups [5-5](#)
- DELETE_DACL [8-26](#)
- deleting [14-6](#)
 - external audit servers [13-27](#)
 - external servers [13-23, 13-25](#)
 - logged-in users [10-34](#)
 - Network Access Profiles [14-6](#)
 - policies or rules [13-21](#)
- device command sets
 - See command authorization sets
- device management applications support [1-14](#)
- DHCP with IP pools [8-40](#)
- diagnostic logs [7-27, 10-12](#)
- dial-in permission to users in Windows [12-17](#)
- dial-up networking clients [12-6, 12-7](#)
- digital certificates
 - See certification
- Disabled Accounts report [10-11](#)
 - viewing [10-35](#)
- Disabling NETBIOS [F-12](#)
- discovered users [15-2](#)
- Distinguished Name Caching [12-26](#)
- distributed systems
 - See also proxy
 - AAA servers in [3-2](#)
 - overview [3-2](#)
 - settings
 - configuring [3-28](#)
 - default entry [3-3](#)
 - enabling in interface [2-15](#)
- distribution table
 - See Proxy Distribution Table
- DNIS-based filters [4-20](#)
- documentation
 - conventions [I-XXVIII](#)
 - objectives [I-XXVII](#)

- online [1-21](#)
 - related [I-XXXI, 1-24](#)
- Domain List
 - configuring [12-22](#)
 - inadvertent user lockouts [12-9, 12-21](#)
 - overview [12-9](#)
 - unknown user authentication [15-5](#)
- domain name and hostname configuration [7-24](#)
- domain names
 - Windows operating systems [12-8, 12-9](#)
- downloadable ACLs [14-9](#)
- downloadable IP ACLs
 - adding [4-15](#)
 - assigning to groups [5-22](#)
 - assigning to users [6-14](#)
 - deleting [4-17](#)
 - editing [4-16](#)
 - enabling in interface
 - group-level [2-15](#)
 - user-level [2-14](#)
 - overview [4-13](#)
- draft-ietf-radius-tunnel-auth [1-4](#)
- dump files
 - loading a database from [C-7](#)
 - loading a database to [C-6](#)
- dynamic administration logs [10-11](#)
 - viewing [10-34](#)
- dynamic usage quotas [1-13](#)
- dynamic users
 - removing [6-41](#)

E

- EAP (Extensible Authentication Protocol)
 - Configuration [14-25](#)
 - overview [1-10](#)
 - supported protocols [1-10](#)
 - with Windows authentication [12-10](#)
- EAP authentication

- protocol [1-8](#)
- EAP FAST
 - for anonymous TLS renegotiation [9-16](#)
- EAP-FAST [1-10](#)
 - enabling [9-19](#)
 - identity protection [9-11](#)
 - logging [9-10](#)
 - master keys
 - definition [9-11](#)
 - states [9-11](#)
 - master server [9-18](#)
 - overview [9-9](#)
 - PAC
 - automatic provisioning [9-14](#)
 - definition [9-12](#)
 - manual provisioning [9-15](#)
 - refresh [9-17](#)
 - states [9-14](#)
 - PAC Files Generation [9-37](#)
 - password aging [5-20](#)
 - phases [9-10](#)
 - replication [9-17](#)
- EAP-FAST PKI Authorization Bypass [9-16](#)
- EAPoUDP failure [14-24](#)
- EAPoUDP support [14-24](#)
- EAP-TLS [1-10](#)
 - See also certification
 - authentication configuration [9-21](#)
 - comparison methods [9-3](#)
 - enabling [9-4](#)
 - limitations [9-4](#)
 - options [9-42](#)
 - overview [9-2](#)
 - with RADIUS Key Wrap [14-25](#)
- EAP-TLS authentication
 - outer identity [9-44](#)
- editing
 - external audit servers [13-27](#)
 - external posture validation servers [13-23, 13-24](#)
 - internal policies [13-19](#)
 - Network Access Profiles [14-5](#)
- enable password options for TACACS+ [6-23](#)
- enable privilege options for groups [5-13](#)
- entitlement reports [10-11](#)
- entity field [13-6](#)
- error number decoding with CSUtil.exe [C-17](#)
- Event log
 - configuring [7-20](#)
 - exception events [F-11](#)
- event logging [7-20](#)
- exception events [F-11](#)
- exemption list
 - external audit [13-10](#)
- exports
 - of user lists [C-15](#)
- Extensible Authentication Protocol
 - See EAP (Extensible Authentication Protocol)
- Extensible Authentication Protocol (EAP) [1-2](#)
- external audit policy
 - what triggers an [13-10](#)
- external audit server
 - setting up [13-25](#)
- external audit servers
 - about [13-9](#)
 - adding [13-25](#)
 - deleting [13-27](#)
 - editing [13-27](#)
- external policies [13-8](#)
 - exemption list support [13-10](#)
- external servers
 - creating [13-22, 13-23](#)
 - deleting [13-23, 13-25](#)
 - editing [13-23, 13-24](#)
- external token servers
 - See token servers
- external user databases
 - See also databases
 - authentication via [12-4](#)

- configuring [12-3](#)
- deleting configuration [12-57](#)
- latency factors [15-6](#)
- search order [15-6, 15-8](#)
- supported [1-7](#)
- Unknown User Policy [15-1](#)

F

- Failed Attempts logs [10-2](#)
- failed log-on attempts [F-11](#)
- failure events
 - customer-defined actions [F-11](#)
 - predefined actions [F-11](#)
- fallbacks on failed connection [3-4](#)
- finding users [6-37](#)
- FTP server [7-8](#)

G

- gateways [D-2](#)
- generating [9-39](#)
- Generic LDAP [1-7](#)
- generic LDAP user databases
 - authentication [12-23](#)
 - certificate database downloading [12-47](#)
 - configuring
 - database [12-31](#)
 - options [12-27](#)
 - directed authentications [12-24](#)
 - domain filtering [12-24](#)
 - failover [12-25](#)
 - multiple instances [12-24](#)
 - organizational units and groups [12-24](#)
- Global Authentication Setup [9-21](#)
- global authentication setup
 - enabling posture validation [13-14](#)
- grant dial-in permission to users [12-6, 12-17](#)

- greeting after login [5-18](#)
- group-level interface enabling
 - downloadable IP ACLs [2-15](#)
 - network access restrictions [2-15](#)
 - network access restriction sets [2-15](#)
 - password aging [2-15](#)
- group-level network access restrictions
 - See network access restrictions
- groups
 - See also network device groups
 - assigning users to [6-5](#)
 - configuring RADIUS settings for
 - See RADIUS
 - Default Group [5-2, 16-4](#)
 - enabling VoIP (Voice-over-IP) support for [5-4](#)
 - exporting group information [C-16](#)
 - listing all users in [5-40](#)
 - mapping order [16-8](#)
 - mappings [16-1](#)
 - no access groups [16-4](#)
 - overriding settings [2-4](#)
 - relationship to users [2-4](#)
 - renaming [5-41](#)
 - resetting usage quota counters for [5-40](#)
 - settings for
 - callback options [5-5](#)
 - configuration-specific [5-12](#)
 - configuring common [5-3](#)
 - device management command authorization sets [5-26](#)
 - enable privilege [5-13](#)
 - IP address assignment method [5-21](#)
 - management tasks [5-40](#)
 - max sessions [5-9](#)
 - network access restrictions [5-6](#)
 - password aging rules [5-15](#)
 - PIX command authorization sets [5-25](#)
 - shell command authorization sets [5-23](#)
 - TACACS+ [5-2, 5-3, 5-22](#)

- time-of-day access [5-5](#)
- token cards [5-14](#)
- usage quotas [5-10](#)
- setting up and managing [5-1](#)
- specifications by ODBC authentications [12-41](#), [12-42](#), [12-43](#)

H

- handle counts [F-10](#)
- hard disk space [F-10](#)
- HCAP errors [10-4](#)
- host and domain names configuration [7-24](#)
- Host Credentials Authorization Protocol (HCAP) [9-6](#)
- host system state [F-10](#)
- HTML interface
 - logging off [2-4](#)
- HTTP port allocation
 - for administrative sessions [1-19](#)

I

- IEEE 802.1x [1-2](#)
- IETF 802.1x [1-10](#)
- IETF RADIUS attributes [1-4](#)
- importing passwords [C-9](#)
- imports with CSUtil.exe [C-9](#)
- inbound
 - authentication [1-10](#)
 - password configuration [1-11](#)
- installation
 - related documentation [I-XXXI](#), [1-24](#)
- Interface Configuration
 - See also HTML interface
 - advanced options [2-6](#)
 - configuring [2-1](#)
 - customized user data fields [2-5](#)
- Internal ACS Database [14-47](#)
- internal architecture [F-1](#)

- internal policies
 - editing [13-19](#)
 - steps to set up [13-17](#)
- invalid PAC [9-45](#)
- IP ACLs
 - See downloadable IP ACLs
- IP addresses
 - in User Setup [6-7](#)
 - multiple, for AAA client [3-8](#)
 - requirement for CSTacacs and CSRadius [F-12](#)
 - setting assignment method for user groups [5-21](#)
- IP pools
 - address recovery [8-44](#)
 - deleting [8-43](#)
 - DHCP [8-40](#)
 - editing IP pool definitions [8-42](#)
 - enabling in interface [2-15](#)
 - overlapping [8-40](#), [8-41](#)
 - refreshing [8-41](#)
 - resetting [8-42](#)
 - servers
 - adding IP pools [8-41](#)
 - overview [8-39](#)
 - replicating IP pools [8-39](#)
 - user IP addresses [6-7](#)

K

- Key Wrap
 - configuring for AAA client [3-9](#)
 - configuring for NDG [3-24](#)
- key wrap
 - enabling [14-26](#)
- Key Wrap, RADIUS [14-25](#)

L

- LAN manager [1-10](#)

LDAP

Admin Logon Connection Management [12-26](#)

Distinguished Name [12-26](#)

group attributes [14-24](#)

LDAP Server [14-47](#)

LEAP [1-10](#)

LEAP proxy RADIUS user databases

configuring external databases [12-49](#)

group mappings [16-1](#)

overview [12-48](#)

RADIUS-based group specifications [16-8](#)

list all users

in Group Setup [5-40](#)

in User Setup [6-37](#)

local policies

see internal policies

log files

storage directory [7-3](#)

Logged-In Users report [10-11](#)

deleting logged-in users [10-34](#)

viewing [10-34](#)

logging [10-1](#)

attributes [10-3](#)

configuring

configuring

logs [10-22](#)

configuring CSV (comma-separated values) [10-24](#)

configuring ODBC [10-25](#)

configuring remote logging server [10-26](#)

configuring service logs [10-29](#)

configuring syslog [10-24](#)

critical loggers [10-23](#)

CSAgent [1-17](#)

CSV (comma-separated values) [10-6](#)

custom RADIUS dictionaries [8-2](#)

debug logs, detail levels [10-29](#)

diagnostic logs [7-27](#)

enabling and disabling ODBC [10-25](#)

enabling CSV (comma-separated values) [10-24](#)

enabling syslog [10-24](#)

formats and targets [10-5](#)

ODBC [10-9](#)

RDBMS synchronization [8-2](#)

remote, configuring ACS to send data to [10-27](#)

remote, configuring and enabling [10-26](#)

remote, for ACS for Windows [10-10](#)

remote, hosts for [10-10](#)

remote agents, configuring logs on configuration provider [10-28](#)

remote agents, configuring to [10-27](#)

remote agents, sending data to [10-28](#)

remote agents for ACS SE remote agents

for remote logging for ACS SE [10-10](#)

See also logs

See also reports

service logs [10-12](#)

service logs for customer support [10-29](#)

syslog [10-7](#)

watchdog packets [10-37](#)

Logging Configuration Page [10-37](#)

Login Process Fail page [11-3](#)

login process test frequency [7-18](#)

logins

greeting upon [5-18](#)

password aging dependency [5-17](#)

logs [10-1](#)

AAA-related [10-1](#)

Administration Audit [10-5](#)

Appliance Administration Audit [10-5](#)

audit [10-5](#)

Backup and Restore [10-5](#)

Database Replication [10-5](#)

dynamic administration [10-11](#)

Failed Attempts [10-2](#)

logged-in users [10-11](#)

Passed Authentications [10-2](#)

RADIUS accounting [10-2](#)

RDBMS Synchronization [10-5](#)

See also logging
 See also reports
 service [10-12](#)
 Service Monitoring [10-5](#)
 TACACS+ accounting [10-2](#)
 TACACS+ administration [10-2](#)
 User Password Changes [10-5](#)
 viewing and downloading [10-30](#)
 VOIP accounting [10-2](#)

M

MAC address
 standard formats [14-24](#)
 machine authentication
 enabling [12-15](#)
 overview [12-10](#)
 with Microsoft Windows [12-13](#)
 management application support [1-14](#)
 mappings
 databases to AAA groups [16-1](#)
 master AAA servers [8-2](#)
 master key
 definition [9-11](#)
 states [9-11](#)
 max sessions [1-13](#)
 enabling in interface [2-15](#)
 group [1-13](#)
 in Group Setup [5-9](#)
 in User Setup [6-11](#)
 overview [1-13](#)
 user [1-13](#)
 member server [12-6, 12-8](#)
 memory utilization [F-10](#)
 Microsoft Health Registration Authority [9-5](#)
 Microsoft Network Policy Server (NPS) [9-6](#)
 Microsoft Text Driver [8-20](#)
 monitoring
 configuring [7-19](#)

CSMon [F-10](#)
 overview [7-18](#)
 services [7-26](#)
 MS-CHAP [1-9](#)
 configuring [9-21](#)
 overview [1-9](#)
 protocol supported [1-8](#)
 multiple IP addresses for AAA clients [3-8](#)

N

NAC [1-2](#)
 agentless hosts [13-9](#)
 attributes
 about [13-5](#)
 data types [13-6](#)
 deleting [C-29](#)
 exporting [C-29](#)
 configuring ACS for support for [13-13](#)
 credentials
 about [13-5](#)
 implementing [13-4](#)
 logging [13-14](#)
 overview
 policies
 about [13-16](#)
 external [13-8](#)
 internal [13-7](#)
 results [13-16](#)
 remediation server
 url-redirect attribute [B-6](#)
 rules
 about [13-8](#)
 default [13-32](#)
 self-signed certificates [13-13](#)
 tokens
 definition [13-3](#)
 descriptions of [13-3](#)
 returned by internal policies [13-7](#)

- NAC Agentless Host [14-18](#)
 - NAC L2 IP [14-11](#)
 - NAC L3 IP [14-9](#)
 - NAFs
 - See network access filters
 - NAR
 - See network access restrictions
 - NAS
 - See AAA clients
 - Network Access Filter (NAF)
 - editing [4-5](#)
 - Network Access Filters (NAF) [14-2](#)
 - adding [4-3](#)
 - deleting [4-6](#)
 - overview [4-2](#)
 - Network Access Profiles [14-1, 14-6, 14-23](#)
 - cloning [14-6](#)
 - configuring advanced filtering [14-2](#)
 - editing [14-5](#)
 - network access quotas [1-13](#)
 - network access restrictions
 - deleting [4-24](#)
 - editing [4-23](#)
 - enabling in interface
 - group-level [2-15](#)
 - user-level [2-14](#)
 - in Group Setup [5-6](#)
 - interface configuration [2-15](#)
 - in User Setup [5-6, 6-8](#)
 - non-IP-based filters [4-20](#)
 - overview [4-18](#)
 - network access servers
 - See AAA clients
 - Network Admission Control
 - see NAC
 - network configuration [3-1](#)
 - network device groups
 - adding [3-24](#)
 - assigning AAA clients to [3-25](#)
 - assigning AAA servers to [3-25](#)
 - configuring [3-23](#)
 - deleting [3-27](#)
 - editing [3-26](#)
 - enabling in interface [2-15](#)
 - reassigning AAA clients to [3-26](#)
 - reassigning AAA servers to [3-26](#)
 - network devices
 - searches for [3-6](#)
 - network time protocol
 - See NTP server
 - noncompliant devices [1-2](#)
 - non-EAP authentication
 - protocol [1-8](#)
 - NTP server [7-23](#)
-
- O
- ODBC features
 - authentication
 - CHAP [12-38](#)
 - EAP-TLS [12-38](#)
 - overview [12-35](#)
 - PAP [12-38](#)
 - preparation process [12-37](#)
 - process with external user database [12-36](#)
 - result codes [12-43](#)
 - case-sensitive passwords [12-39](#)
 - CHAP authentication sample procedure [12-40](#)
 - configuring [12-44](#)
 - data source names [12-35](#)
 - DSN (data source name) configuration [12-44](#)
 - EAP-TLS authentication sample procedure [12-40](#)
 - features supported [12-36](#)
 - group mappings [16-1](#)
 - group specifications
 - CHAP [12-42](#)
 - EAP-TLS [12-43](#)
 - PAP [12-41](#)

- vs. group mappings [16-2](#)
- PAP authentication sample procedures [12-39](#)
- password case sensitivity [12-39](#)
- stored procedures
 - CHAP authentication [12-41](#)
 - EAP-TLS authentication [12-42](#)
 - implementing [12-38](#)
 - PAP authentication [12-40](#)
 - type definitions [12-38](#)
- user databases [12-35](#)
- ODBC log Configuration Page [10-42](#)
- ODBC logging [10-9](#)
 - configuring [10-25](#)
 - data source names [10-9](#)
 - enabling and disabling [10-25](#)
 - preparing for [10-9](#)
- One-time Passwords (OTPs) [1-7](#)
- online documentation [1-21](#)
- online help [1-21](#)
 - location in HTML interface [1-20](#)
 - using [1-21](#)
- online user guide [1-22](#)
- ordering rules, in policies [13-8](#)
- outbound password configuration [1-11](#)
- outer identity
 - EAP-TLS authentication [9-44](#)
- overview of Cisco Secure ACS [1-1](#)

P

PAC

- automatic provisioning [9-14](#)
- definition [9-12](#)
- manual provisioning [9-15](#)
- refresh [9-17](#)

PAC File Generation

- options [9-37](#)

PAC files [9-39](#)

- generating [9-39](#)

PAC Free EAP-FAST [9-16](#)

package.cab file, for customer support [10-29](#)

PAP [1-9](#)

- in User Setup [6-4](#)
- vs. ARAP [1-9](#)
- vs. CHAP [1-9](#)

Passed Authentications logs [10-2](#)

password

- automatic change password configuration [8-16](#)

password aging [1-11](#)

- age-by-uses rules [5-17](#)
- Cisco IOS release requirement for [5-16](#)
- EAP-FAST [12-16](#)
- interface configuration [2-15](#)
- in Windows databases [5-19](#)
- MS-CHAP [12-16](#)
- overview [1-11](#)
- PEAP [12-16](#)
- rules [5-15](#)

password configurations

- basic [1-10](#)

passwords

See also password aging

- case sensitive [12-39](#)

- CHAP/MS-CHAP/ARAP [6-5](#)

configurations

- caching [1-11](#)
- inbound passwords [1-11](#)
- outbound passwords [1-11](#)
- separate passwords [1-10](#)
- single password [1-10](#)
- token caching [1-11](#)
- token cards [1-11](#)

- encryption [12-2](#)

- expiration [5-17](#)

- import utility [C-9](#)

- local management [7-4](#)

- post-login greeting [5-18](#)

- protocols supported [1-8](#)

- remote change [7-4](#)
- user-changeable [1-12](#)
- validation options in System Configuration [7-4](#)
- patch
 - overview [7-28](#)
 - process [7-29](#)
- pattern matching in command authorization [4-28](#)
- PEAP [1-10](#)
 - See also certification
 - configuring [9-21](#)
 - enabling [9-8](#)
 - identity protection [9-7](#)
 - overview [9-6](#)
 - password aging [5-19](#)
 - phases [9-6](#)
 - with Unknown User Policy [9-8](#)
- performance monitoring [F-10](#)
- performance specifications [1-22](#)
- per-group attributes
 - See also groups
 - enabling in interface [2-5](#)
- per-user attributes
 - enabling in interface [2-5](#)
 - TACACS+/RADIUS in Interface Configuration [2-14](#)
- ping command [1-18](#)
- PIX ACLs
 - See downloadable IP ACLs
- PIX command authorization sets
 - See command authorization sets
- PKI (public key infrastructure)
 - See certification
- Point-to-Point Protocol (PPP) [1-23](#)
- policies
 - agentless hosts [13-9](#)
 - cloning [13-20](#)
 - configuring [13-15](#)
 - copying [13-20](#)
 - deleting [13-21](#)
 - external [13-8](#)
 - internal [13-7](#)
 - local
 - see internal policies
 - overview [13-5](#)
 - renaming [13-20](#)
 - rule order [13-8](#)
 - setting up an external audit server [13-25](#)
 - setting up external servers [13-22, 13-23](#)
- Populate from Global [14-13, 14-23, 14-46](#)
 - Network Access Profiles [14-23](#)
- port 2002
 - in HTTP port ranges [11-19](#)
 - in URLs [1-21](#)
- ports
 - See also HTTP port allocation
 - See also port 2002
 - RADIUS [1-3, 1-4](#)
 - TACACS+ [1-3](#)
- Posture Validation
 - for Agentless Hosts [14-33](#)
- posture validation
 - attributes [13-5](#)
 - adding [C-29](#)
 - configuring ACS for [13-13](#)
 - credentials [13-5](#)
 - CTL [13-13](#)
 - enabling [13-14](#)
 - failed attempts log [13-14](#)
 - implementing [13-4](#)
 - options [13-16](#)
 - passed authentications log [13-14](#)
 - policy overview [13-5](#)
 - and profile-based policies [13-3](#)
 - profiles, adding user groups [13-14](#)
 - rule
 - assigning posture tokens [13-14](#)
 - rules, about [13-8](#)
 - server certificate requirement [13-13](#)
- Posture Validation Policies

- configuring [14-29](#)
- PPP password aging [5-16](#)
- processor utilization [F-10](#)
- profile [14-1](#)
- Profile-based Policies [14-3](#)
- profile components
 - See shared profile components
- profiles [14-38](#)
- profile templates [14-7](#)
 - prerequisites [14-7](#)
- protocols supported [1-8](#)
- protocol support
 - EAP authentication [1-8](#)
 - non-EAP authentication [1-8](#)
- protocol types
 - Network Access Profiles [14-2](#)
- proxy
 - See also Proxy Distribution Table
 - character strings
 - defining [3-5](#)
 - stripping [3-5](#)
 - configuring [3-28](#)
 - in enterprise settings [3-4](#)
 - overview [3-3](#)
 - sending accounting packets [3-5](#)
- Proxy Distribution Table
 - See also proxy
 - adding entries [3-28](#)
 - configuring [3-28](#)
 - default entry [3-3, 3-28](#)
 - deleting entries [3-30](#)
 - editing entries [3-30](#)
 - match order sorting [3-29](#)
 - overview [3-28](#)

Q

quotas

See network access quotas

See usage quotas

R

RAC and Groups [4-7](#)

RADIUS [1-4](#)

See also RADIUS VSAs (vendor specific attributes)

accounting [1-15](#)

attributes

See also RADIUS VSAs (vendor specific attributes)

in User Setup [6-24](#)

AV (attribute value) pairs

See also RADIUS VSAs (vendor specific attributes)

Cisco IOS [B-3](#)

IETF [B-11](#)

overview [B-1](#)

Cisco Aironet [3-10](#)

IETF

in Group Setup [5-27](#)

interface configuration [2-9](#)

in User Setup [6-25](#)

interface configuration overview [2-7](#)

Key Wrap [14-25](#)

Key Wrap, configuring for AAA client [3-9](#)

Key Wrap, configuring for NDG [3-24](#)

key wrap, enabling [14-26](#)

password aging [5-19](#)

ports [1-3, 1-4](#)

specifications [1-4](#)

token servers [12-51](#)

vs. TACACS+ [1-3](#)

RADIUS user databases

configuring [12-52](#)

group mappings [16-1](#)

RADIUS-based group specifications [16-8](#)

RADIUS VSAs (vendor specific attributes)

3COM/USR

- in Group Setup [5-37](#)
- in User Setup [6-34](#)
- supported attributes [B-28](#)

Ascend

- in Group Setup [5-31](#)
- in User Setup [6-29](#)
- supported attributes [B-21](#)

Cisco Aironet

- in Group Setup [5-30](#)
- in User Setup [6-27](#)

Cisco BBSM (Building Broadband Service Manager)

- in Group Setup [5-38](#)
- in User Setup [6-35](#)
- supported attributes [B-10](#)

Cisco IOS/PIX

- in Group Setup [5-28](#)
- interface configuration [2-9](#)
- in User Setup [6-26](#)
- supported attributes [B-4](#)

Cisco VPN 3000

- in Group Setup [5-32](#)
- in User Setup [6-30](#)
- supported attributes [B-6](#)

Cisco VPN 5000

- in Group Setup [5-33](#)
- in User Setup [6-30](#)
- supported attributes [B-10](#)

custom

- about [8-27](#)
- in Group Setup [5-39](#)
- in User Setup [6-36](#)

Juniper

- in Group Setup [5-37](#)
- in User Setup [6-33](#)
- supported attributes [B-28](#)

Microsoft

- in Group Setup [5-34](#)
- in User Setup [6-31](#)

- supported attributes [B-19](#)

Nortel

- in Group Setup [5-36](#)
- in User Setup [6-33](#)
- supported attributes [B-28](#)

overview [B-1](#)**user-defined**

- about [8-27, C-17](#)
- action codes for [E-13](#)
- adding [C-18](#)
- deleting [C-20](#)
- import files [C-22](#)
- listing [C-21](#)
- replicating [8-27, C-18](#)

RDBMS Synchronization [8-17](#)**RDBMS synchronization** [E-1](#)**accountActions file**

- overview [8-29](#)

configuring [8-36](#)**data source name configuration** [8-32, 8-33](#)**disabling** [8-37](#)**enabling in interface** [2-15](#)**FTP configuration** [8-34](#)**group-related configuration** [8-21](#)**import definitions** [E-1](#)**manual initialization** [8-35](#)**network configuration** [8-22](#)**overview** [8-18](#)**partners** [8-34](#)**preparing to use** [8-30](#)**report and error handling** [8-30](#)**scheduling options** [8-34](#)**user-related configuration** [8-20](#)**RDBMS Synchronization logs** [10-5](#)**READ_DACL** [8-25](#)**READ_NAS** [8-23](#)**Registry** [F-2](#)**regular expressions syntax** [10-32](#)**rejection mode**

- general [15-3](#)
 - Windows user databases [15-4](#)
- related documentation [I-XXXI, 1-24](#)
- remote agent
 - selecting for authentication [12-17](#)
- remote agents
 - adding [3-21](#)
 - configuration options [3-19](#)
 - configuring [3-19](#)
 - configuring logging to [10-27](#)
 - configuring logs on configuration provider [10-28](#)
 - deleting [3-23](#)
 - editing [3-22](#)
 - overview [3-19](#)
 - Remote Agents table [3-2](#)
 - selecting for authentication [12-17](#)
 - sending data to [10-28](#)
- Remote Agents Reports Configuration Page [10-39](#)
- remote logging
 - configuring ACS to send data to [10-27](#)
 - configuring and enabling [10-26](#)
 - for ACS for Windows [10-10](#)
 - hosts [10-10](#)
 - remote agents, for ACS SE [10-10](#)
 - See also logging
 - server, configuring [10-26](#)
 - using remote agents [10-27](#)
- Remote Logging Setup Page [10-39](#)
- Remove Dynamic Users [6-41](#)
- removing
 - external audit servers [13-27](#)
 - external servers [13-23, 13-25](#)
 - policies or rules [13-21](#)
- removing dynamic users [6-41](#)
- renaming
 - policies [13-20](#)
- replication
 - ACS Service Management page [8-2](#)
 - auto change password settings [8-16](#)
 - backups recommended (Caution) [8-7](#)
 - cascading [8-4, 8-9](#)
 - certificates [8-2](#)
 - client configuration [8-11](#)
 - components
 - overwriting (Caution) [8-11](#)
 - overwriting (Note) [8-7](#)
 - selecting [8-7](#)
 - configuring [8-14](#)
 - corrupted backups (Caution) [8-7](#)
 - custom RADIUS dictionaries [8-2](#)
 - disabling [8-16](#)
 - EAP-FAST [9-17](#)
 - encryption [8-4](#)
 - external user databases [8-2](#)
 - frequency [8-5](#)
 - group mappings [8-2](#)
 - immediate [8-13](#)
 - implementing primary and secondary setups [8-10](#)
 - important considerations [8-5](#)
 - in System Configuration [8-14](#)
 - interface configuration [2-15](#)
 - IP pools [8-2, 8-39](#)
 - logging [8-7](#)
 - manual initiation [8-13](#)
 - master AAA servers [8-2](#)
 - notifications [8-17](#)
 - options [8-7](#)
 - overview [8-2](#)
 - partners
 - configuring [8-15](#)
 - options [8-9](#)
 - process [8-3](#)
 - scheduling [8-14](#)
 - scheduling options [8-9](#)
 - selecting data [8-7](#)
 - unsupported [8-2](#)
 - user-defined RADIUS vendors [8-6](#)
 - vs. backup [8-6](#)

- reports [10-1](#)
 - downloading CSV [10-33](#)
 - entitlement [10-11](#)
 - entitlement, viewing and downloading [10-36](#)
 - See also logging reports
 - See also logs
 - viewing and downloading [10-30](#)
 - viewing appliance status [10-35](#)
 - viewing CSV [10-31](#)
 - viewing disabled accounts [10-35](#)
 - viewing dynamic administration [10-34](#)
 - viewing logged-in users, [10-34](#)
- Reports and Activity
 - in interface [1-20](#)
- Reports Page Reference [10-44](#)
- request handling
 - general [15-3](#)
 - Windows user databases [15-4](#)
- Required Credential Types [14-48](#)
- resource consumption [F-10](#)
- restarting services [7-2](#)
- restore
 - components restored
 - configuring [7-16](#)
 - overview [7-16](#)
 - filenames [7-15](#)
 - in System Configuration [7-14](#)
 - on a different server [7-14](#)
 - overview [7-14](#)
 - performing [7-16](#)
 - reports [7-16](#)
 - with CSUtil.exe [C-4](#)
- restores
 - finding files [7-15](#)
- RFC2138 [1-4](#)
- RFC2139 [1-4](#)
- RSA user databases
 - configuring [12-54](#)
 - group mappings [16-1](#)

- rule [13-8](#)
- rules
 - about [13-8](#)

S

- search order of external user databases [15-8](#)
- security protocols
 - CSRadius [F-12](#)
 - CSTacacs [F-12](#)
 - RADIUS [1-3, B-1](#)
 - TACACS+
 - custom commands [2-12](#)
 - overview [1-3](#)
 - time-of-day access [2-12](#)
- Selected Credentials [14-48](#)
- server certificate installation [9-22](#)
- service control in System Configuration [10-29](#)
- Service Control Page Reference [10-43](#)
- service logs [10-12](#)
 - configuring [10-29](#)
 - for customer support [10-29](#)
- Service Monitoring logs [10-5](#)
- services
 - determining status of [7-2](#)
 - logs generated [10-12](#)
 - management [7-18](#)
 - monitoring [7-26](#)
 - starting [7-2](#)
 - stopping [7-2](#)
- shared profile components
 - See also command authorization sets
 - See also downloadable IP ACLs
 - See also network access filters
 - See also network access restrictions
 - overview [4-1](#)
- Shared Profile Components (SPC) [1-14](#)
- Shared RAC [14-35](#)
- shared secret [F-12](#)

shell command authorization sets

See also command authorization sets

in Group Setup [5-23](#)in User Setup [6-17](#)Simple Network Management Protocol (SNMP) [1-13](#)single password configurations [1-10](#)SMTP (simple mail-transfer protocol) [F-11](#)SNMP, support on appliance [7-23](#)

specifications

RADIUS

RFC2138 [1-4](#)RFC2139 [1-4](#)system performance [1-22](#)TACACS+ [1-4](#)SSL (secure sockets layer) [12-30](#)starting services [7-2](#)Statements of Health(SoHs) [9-5](#)static IP addresses [6-7](#)stopping services [7-2](#)

stored procedures

CHAP authentication

configuring [12-46](#)input values [12-41](#)output values [12-42](#)result codes [12-43](#)

EAP-TLS authentication

configuring [12-46](#)input values [12-42](#)output values [12-43](#)implementing [12-38](#)

PAP authentication

configuring [12-46](#)input values [12-40](#)output values [12-41](#)result codes [12-43](#)sample procedures [12-39](#)

type definitions

integer [12-38](#)string [12-38](#)

supplementary user information

in User Setup [6-4](#)setting [6-4](#)

support

Cisco Device-Management Applications [1-14](#)supported password protocols [1-8](#)Support Page [7-25](#)

synchronization

See RDBMS synchronization

Syslog log Configuration Page [10-41](#)

syslog logging

configuring [10-24](#)enabling and disabling [10-24](#)message format [10-7](#)message length limitations [10-8](#)

syslog logs

logging to [10-7](#)

system

configuration

advanced [8-1](#)authentication [9-1](#)basic [7-1](#)certificates [9-1](#)health [F-10](#)messages in interface [1-20](#)

monitoring

See monitoring

performance specifications [1-22](#)

services

See services

system monitoring

technical support file [7-25](#)

system performance

specifications [1-22](#)

T

TACACS+ [1-3, 1-4](#)accounting [1-15](#)

- accounting logs [10-2](#)
- administration logs [10-2](#)
- advanced TACACS+ settings
 - in Group Setup [5-2, 5-3](#)
 - in User Setup [6-21](#)
- AV (attribute value) pairs
 - accounting [A-3](#)
 - general [A-1](#)
- custom commands [2-12](#)
- enable password options for users [6-23](#)
- enable privilege options [6-22](#)
- interface configuration [2-6](#)
- outbound passwords for users [6-24](#)
- ports [1-3](#)
- SEDAUTH [1-11](#)
- settings
 - in Group Setup [5-2, 5-3, 5-22](#)
 - in User Setup [6-15](#)
- specifications [1-4](#)
- time-of-day access [2-12](#)
- vs. RADIUS [1-3](#)

Telnet

- See also command authorization sets
- password aging [5-16](#)

test login frequency internally [7-18](#)

thread used [F-11](#)

time and date setting [7-23](#)

time format control [7-3](#)

time-of-day/day-of-week specification

- See also date format control
- enabling in interface [2-14](#)

timeout values on AAA clients [15-6](#)

TLS (transport level security)

- See certification

token caching [1-11, 12-51](#)

token cards [1-23](#)

- password configuration [1-11](#)
- settings in Group Setup [5-14](#)

token servers

- ISDN terminal adapters [12-51](#)
- overview [12-50](#)
- RADIUS-enabled [12-51](#)
- RADIUS token servers [12-51](#)
- supported servers [1-7](#)
- token caching [12-51](#)

troubleshooting [14-38](#)

- debug logs [10-12](#)

trust lists

- See certification

trust relationships [12-6](#)

U

UNIX passwords [C-12](#)

unknown service user setting [6-21](#)

Unknown User Policy [12-18](#)

- See also unknown users
- configuring [15-8](#)
- in external user databases [12-2, 15-7](#)
- turning off [15-9](#)

unknown users

- See also Unknown User Policy
- authentication [15-3](#)
- authentication performance [15-6](#)
- authentication processing [15-6](#)
- network access authorization [15-6](#)

unmatched user requests [14-3](#)

UPDATE_DACL [8-26](#)

UPDATE_NAS [8-23](#)

updating packets in accounting logs [10-37](#)

upgrade

- applying [7-33](#)
- CSAgent [1-18](#)
- distribution server requirements [7-29](#)
- overview [7-28](#)
- process [7-29](#)
- restrictions [1-18](#)
- transferring [7-30](#)

- usage quotas
 - in Group Setup [5-10](#)
 - in Interface Configuration [2-15](#)
 - in User Setup [6-12](#)
 - overview [1-13](#)
 - resetting
 - for groups [5-40](#)
 - for single users [6-39](#)
- user-changeable passwords
 - overview [1-12](#)
 - with Windows user databases [12-16](#)
- user databases
 - See databases
- User Data Configuration [2-5](#)
- User Entitlements report [10-12](#)
- user groups
 - See groups
- user guide
 - online [1-22](#)
- user-level
 - downloadable ACLs interface [2-14](#)
 - network access restrictions
 - See also network access restrictions
 - enabling in interface [2-14](#)
- User Password Changes logs [10-5](#)
- users
 - See also User Setup
 - adding
 - basic steps [6-3](#)
 - assigning client IP addresses to [6-7](#)
 - assigning to a group [6-5](#)
 - callback options [6-6](#)
 - configuring [6-1](#)
 - configuring device management command authorization sets for [6-20](#)
 - configuring PIX command authorization sets for [6-19](#)
 - configuring shell command authorization sets for [6-17](#)
 - customized data fields [2-5](#)
 - deleting [10-34](#)
 - deleting accounts [6-39](#)
 - disabling accounts [6-3](#)
 - finding [6-37](#)
 - import methods [12-2](#)
 - in multiple databases [15-4](#)
 - listing all users [6-37](#)
 - number of [1-22](#)
 - RDBMS synchronization [8-20](#)
 - relationship to groups [2-4](#)
 - removing dynamic [6-41](#)
 - resetting accounts [6-40](#)
 - saving settings [6-41](#)
 - supplementary information [6-4](#)
 - types
 - discovered [15-2](#)
 - known [15-2](#)
 - unknown [15-2](#)
 - VPDN dialup [D-1](#)
- User Setup
 - account management tasks [6-37](#)
 - basic options [6-2](#)
 - configuring [6-1](#)
 - deleting user accounts [6-39](#)
 - saving settings [6-41](#)
- Users in Group button [5-40](#)

V

- validation of passwords [7-4](#)
- vendors
 - adding audit [13-25](#)
- vendor-specific attributes
 - See RADIUS VSAs (vendor specific attributes)
 - in RDBMS synchronization [4-8, 8-27](#)
- vendor-specific attributes (VSAs) [1-4](#)
- Viewing Dynamic Administration Reports [10-34](#)
- Virtual Private Dial-Up Networks (VPDNs) [1-13](#)
- Voice-over-IP

See VoIP (Voice-over-IP)

VoIP

accounting [1-15](#)

VoIP (Voice-over-IP)

accounting configuration [2-16, 7-21](#)

enabling in interface [2-15](#)

group settings in Interface Configuration [2-15](#)

in Group Setup [5-4](#)

VPDN

authentication process [D-1](#)

domain authorization [D-2](#)

home gateways [D-2](#)

IP addresses [D-2](#)

tunnel IDs [D-2](#)

users [D-1](#)

VSAs

See RADIUS VSAs (vendor specific attributes)

W

warning events [F-10, F-11](#)

warnings

significance of [I-XXIX](#)

watchdog packets

logging [10-37](#)

web interface

See also Interface Configuration

layout [1-19](#)

security [1-16](#)

uniform resource locator [1-21](#)

Windows Authentication Configuration [12-21](#)

Windows Callback [12-18](#)

Windows Database Callback [12-18](#)

Windows operating systems

authentication order [15-5](#)

Cisco Secure ACS-related services

services [7-2](#)

dial-up networking [12-6](#)

dial-up networking clients

domain field [12-7](#)

password field [12-7](#)

username field [12-7](#)

Domain List effect [15-5](#)

domains

domain names [12-8, 12-9, 15-4](#)

Event logs [F-11](#)

Registry [F-2](#)

Windows Services [1-23](#)

CSAdmin [1-23](#)

CSAuth [1-23](#)

CSDBSync [1-23](#)

CSLog [1-23](#)

CSMon [1-23](#)

CSRadius [1-23](#)

CSTacacs [1-23](#)

overview [1-23](#)

Windows user database [1-7](#)

passwords [1-8](#)

Windows user databases

See also databases

Active Directory [12-17](#)

configuring [12-22](#)

Domain list

inadvertent user lockouts [12-21](#)

domain mapping [16-6](#)

domains

trusted [12-6](#)

grant dial-in permission to users [12-6, 12-17](#)

group mappings

editing [16-6](#)

no access groups [16-4](#)

remapping [16-6](#)

overview [12-5](#)

password aging [5-19](#)

rejection mode [15-4](#)

request handling [15-4](#)

trust relationships [12-6](#)

user-changeable passwords [12-16](#)

user manager [12-17](#)