Configuration Guide for Cisco Secure ACS 4.1

December 2006

Corporate 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: 408 526-4100

Text Part Number: OL-9976-01

Configuration Guide for Cisco Secure ACS 4.1

CONTENTS

About This Guide

Audience

This guide is for system administrators who install and configure Cisco Secure ACS, hereafter referred to as ACS, and set up and maintain accounts and dial-in network security.

Organization

This document contains the following chapters:

- Chapter 1, "Overview of ACS Configuration"—Provides an overview of ACS configuration, including a summary of configuration steps and configuration flowchart that show the sequence of configuration steps.
- Chapter 2, "Deploy the Access Control Servers"—Describes factors to consider when deploying ACS, including the access type, network topology, and whether database synchronization and replication are required.
- Chapter 3, "Password Policy Configuration Scenario"—Describes how to configure Sarbanes-Oxley (SOX) support when adding administrators.
- Chapter 4, "Agentless Host Support Configuration Scenario"—Describes how to configure ACS for agentless host support (MAC authentication bypass).
- Chapter 5, "PEAP/EAP-TLS Configuration Scenario"—Describes how to configure ACS for PEAP/EAP-TLS support.
- Chapter 6, "Syslog Logging Configuration Scenario"—Describes how to configure ACS to log syslog messages.
- Chapter 7, "NAC Configuration Scenario"—Describes how to configure ACS in a Cisco Network Admission Control (NAC) environment.
- "Glossary"—Lists common terms used in ACS.

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	*italic* font
Displayed session and system information, paths and file names	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*italic screen* font
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

We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates. You can link to the documentation for Cisco Secure ACS for Windows is located from this location:

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

You can link to the documentation for Cisco Secure ACS Solution Engine from this location:

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

Table 1 describes the product documentation that is available.

Table 1 Product Documentation

Document Title	Available Formats
Documentation Guide for Cisco Secure ACS Release 4.1	• Shipped with product. • PDF on the product CD-ROM. • On Cisco.com at: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_documentation_roadmaps_list.html
Release Notes for Cisco Secure ACS Release 4.1	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_release_notes_list.html
User Guide for Cisco Secure Access Control Server 4.1	On Cisco.com http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html
Configuration Guide for Cisco Secure ACS Release 4.1	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_installation_and_configuration_guides_list.html
Installation Guide for Cisco Secure ACS for Windows Release 4.1	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html
Installation Guide for Cisco Secure ACS Solution Engine Release 4.1	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html
Regulatory Compliance and Safety Information for the Cisco Secure ACS Solution Engine Release 4.1	• Shipped with product. • PDF on the product CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html
Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.1	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html
Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.1	On Cisco.com: http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_device_support_tables_list.html
Installation and User Guide for Cisco Secure ACS User-Changeable Passwords	On Cisco.com at the following location http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html.html
Online Documentation	In the ACS HTML interface, click **Online Documentation**.
Online Help	In the ACS HTML interface, online help appears in the right pane when you are configuring a feature.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Technical Support & Documentation site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. (To register as a Cisco.com user, go to this URL: http://tools.cisco.com/RPF/register/register.do) Registered users can access the tool at this URL: https://www.cisco.com/web/siteassets/account/index.html

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the **Cisco Product Identification Tool** to locate your product serial number before submitting a request for service online or by phone. You can access this tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. On the Cisco.com home page, click the **Advanced Search** link under the Search box

and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Overview of ACS Configuration

This chapter describes the general steps for configuring Cisco Secure Access Control Server, hereafter referred to as ACS, and presents a flowchart showing the sequence of steps.

This chapter contains:

Summary of Configuration Steps

To configure ACS:

Step 1 Plan the ACS Deployment.

Determine how many ACS servers you need and their placement in the network.

For detailed information, see Chapter 2, "Deploy the Access Control Servers."

Step 2 Install the ACS Servers.

Install the ACS servers as required. For detailed installation instructions, refer to:

- *Installation Guide for Cisco Secure ACS for Windows Release 4.1*, available on Cisco.com at:

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

- *Installation Guide for Cisco Secure ACS Solution Engine Release 4.1*, available on Cisco.com at:

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

Step 3 Configure Additional Administrators.

When you install the Windows version of ACS, there are initially no administrative users. When you install Cisco Secure ACS Solution Engine (ACS SE), there is initially one administrator.

Note After you install Cisco Secure ACS Solution Engine, the administrative user can access the ACS SE only by using the command line interface (CLI) through a serial port connection. To enable an administrative user who can access the ACS SE by using the ACS web GUI, you must create an administrative GUI user by using the **add-guiadmin** command. For information on the **add-guiadmin** command, see Appendix A of the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*, "Command Reference."

To set up additional administrative accounts:

a. Add Administrators.

b. For each administrator, specify administrator privileges.

c. As needed, configure the following optional administrative policies:

- **Access Policy**—Specify IP address limitations, HTTP port restrictions, and secure socket layer (SSL) setup.
- **Session Policy**—Specify timeouts, automatic local logins, and response to invalid IP address connections.
- **Password Policy**—Configure the password policy for administrators.

For detailed information, see Chapter 3, "Password Policy Configuration Scenario."

Step 4 Configure the Web Interface:

a. Add AAA clients and specify the authorization protocols that the clients will use.

b. Click **Interface Configuration**.

c. On the Interface Configuration page, configure the interface to include one or more of:

- **RADIUS Configuration Options**—For detailed information, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, "Using the Web Interface."
- **TACACS+ Configuration Options**—For detailed information, see "Displaying TACACS+ Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, "Using the Web Interface."
- **Advanced Options**—For detailed information, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, "Using the Web Interface."
- **Customized User Options**—For detailed information, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, "Using the Web Interface."

Step 5 Configure Basic ACS System Settings:

a. Click **System Configuration**.

b. Configure:

- Service Control
- Logging
- Date Format Control
- Local Password Management
- ACS Backup
- ACS Restore
- ACS Service Management

- (optional) IP Pools Server
- (optional) IP Pools Address Recovery

For detailed instructions, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, "Using the Web Interface."

Step 6 Configure Users:

a. As required for your network security setup, configure users. You can configure users:

- Manually, by using the ACS web interface
- By using the **CSUtil** utility to import users from an external database
- By using database synchronization
- By using database replication

For detailed instructions, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, "Using the Web Interface."

Step 7 Configure Certificates.

This step is required if you are using EAP-TLS, Secure Sockets Layer (SSL), or Cisco Network Admission Control (NAC).

For detailed instructions, see Step 3: Install and Set Up an ACS Security Certificate, page 4-6.

Step 8 Configure Global Authentication Settings.

Configure the security protocols that ACS uses to authenticate users. You can configure the following global authentication methods:

- PEAP
- EAP-FAST
- EAP-TLS
- LEAP
- EAP-MD5
- Legacy authentication protocols, such as MS-CHAP Version 1 and Version 2

For detailed instructions, see "Global Authentication Setup" in Chapter 8 of the *User Guide for Cisco Secure ACS 4.1*, "System Configuration: Authentication and Certificates."

Step 9 Configure Shared Profile Components.

You can configure the following shared profile components:

- Downloadable IP ACLs
- Network Access Filtering
- RADIUS Authorization Components
- Network Access Restrictions
- Command Authorization Sets

For detailed instructions, see Chapter 3 of the *User Guide for Cisco Secure ACS 4.1*, "Shared Profile Components."

Step 10 Set Up Network Device Groups.

You can set up network device groups to simplify configuration of common devices. For detailed information, see the *User Guide for Cisco Secure ACS 4.1*.

Step 11 Add AAA Clients.

You can add RADIUS clients or TACACS+ clients. For detailed instructions, see Step 2: Configure a RADIUS AAA Client, page 4-5.

Step 12 Set Up User Groups.

Set up user groups to apply common configuration settings to groups of users. For detailed instructions, see Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, "User Group Management."

Step 13 Configure Posture Validation.

If you are using ACS with NAC, configure posture validation. For detailed instructions, see Step 11: Set Up Network Access Profiles, page 7-16 and Step 13: Configure Posture Validation for NAC, page 7-29

Step 14 Set Up Network Access Profiles.

If required, set up network access profiles. For detailed information, see Step 11: Set Up Network Access Profiles, page 7-16

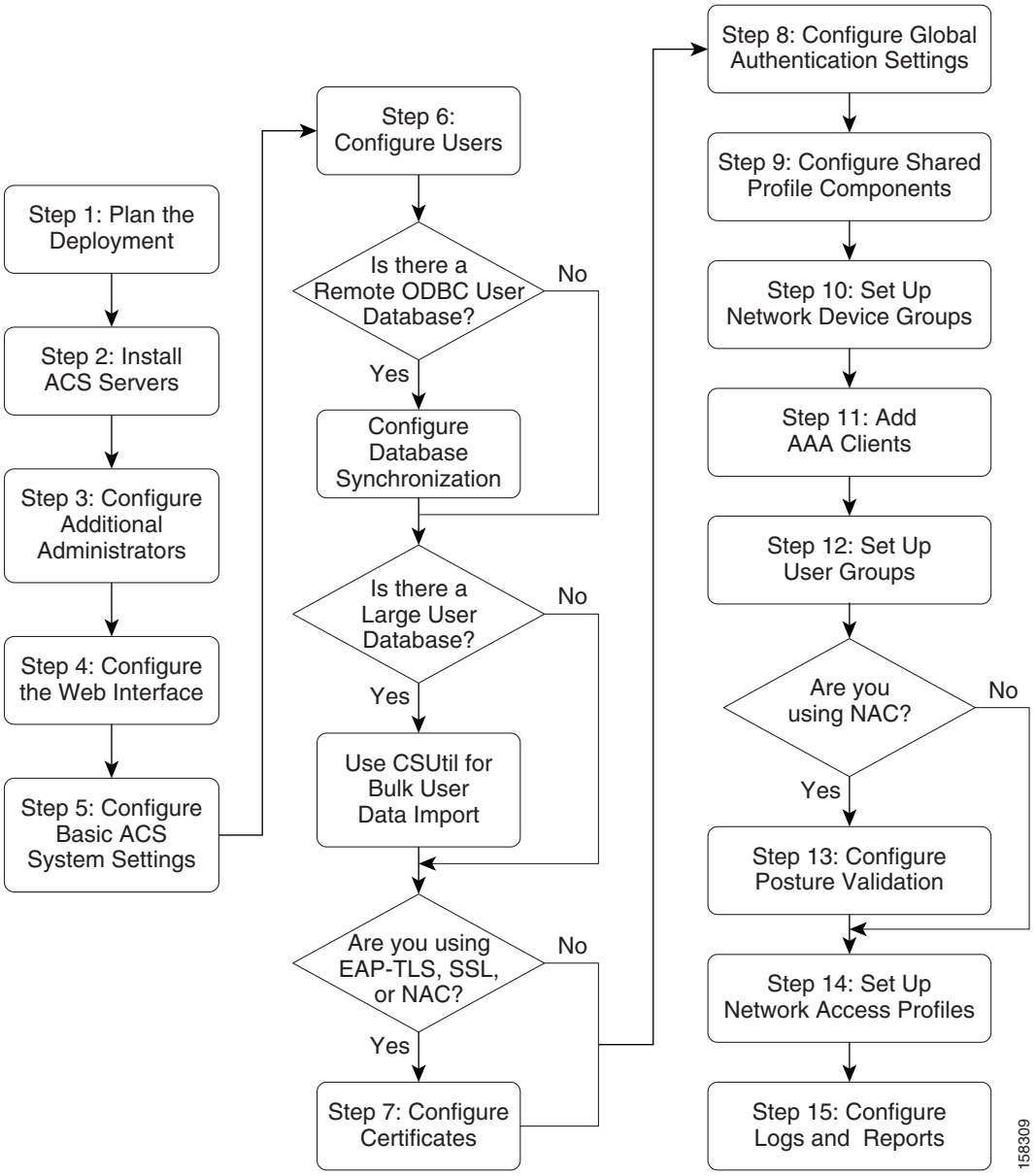
Step 15 Configure Logs and Reports.

Configure reports to specify how ACS logs data. You can also view the logs in HTML reports. For detailed instructions, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.1*, "Logs and Reports.

Configuration Flowchart

Figure 1-1 is a configuration flowchart that shows the main steps in ACS configuration.

Figure 1-1 ACS Configuration Flowchart



Refer to the list of steps in Summary of Configuration Steps, page 1-1 for information on where to find detailed descriptions of each step.

CHAPTER 2

Deploy the Access Control Servers

This chapter discusses topics that you should consider before deploying Cisco Secure Access Control Server, hereafter referred to as ACS.

This document does not describe the software installation procedure for ACS or the hardware installation procedure for the ACS Solution Engine (ACS SE). For detailed installation information, refer to:

- *Installation Guide for Cisco Secure ACS for Windows Release 4.1*, available on Cisco.com at:

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

- *Installation Guide for Cisco Secure ACS Solution Engine Release 4.1*, available on Cisco.com at:

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

This chapter contains:

Determining the Deployment Architecture

How your enterprise network is configured and the network topology are likely to be the most important factors in deploying ACS. This section discusses:

- **Access types**—How users will access the network (through wireless access, LAN access through switches, and so on) and the security protocols used to control user access; for example, RADIUS, EAP- TLS, Microsoft Active Directory, and so on.
- **Network architecture**—How the network is organized (centrally through campus LANs, regional LANs, WLANs, and so on.

This section contains:

Access Types

This section contains:

Wired LAN Access

You can use wired LAN access in a small LAN environment, a campus LAN environment, or a regionally or globally dispersed network. The number of users determines the size of the LAN or WLAN:

Size	Users
small LAN	1 to 3,000
medium-sized LAN	3,000 to 25,000
large LAN	25,000 to 50,000
very large LAN or WLAN	over 50,000

The wired LAN environment uses the following security protocols:

- **RADIUS**—RADIUS is used to control user access to wired LANs. In broadcast or switch-based Ethernet networks, you can use RADIUS to provide virtual LAN identification information for each authorized user.
- **EAP**—Extensible Authentication Protocol (EAP), provides the ability to deploy RADIUS into Ethernet network environments. EAP is defined by Internet Engineering Task Force (IETF) RFC 2284 and the IEEE 802.1x standards.

  The 802.1x standard, also known as EAP over LAN (EAPoL), concerns the part of the wider EAP standard that relates to broadcast media networks. Upon connection, EAPoL provides a communications channel between an end user on a client LAN device to the AAA server through the LAN switch. The functionality is similar to what Point-to-Point Protocol (PPP) servers on point-to-point links provide.

  By supporting complex challenge-response dialogues, EAP facilitates the user-based authentication demands of both conventional one-way hashed password authentication schemes such as Challenge Handshake Authentication Protocol (CHAP) and of more advanced authentication schemes such as Transport Layer Security (TLS), or digital certificates.
- **EAP-TLS**—Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). EAP-TLS uses the TLS protocol (RFC 2246), which is the latest version of the Secure Socket Layer (SSL) protocol from the IETF. TLS provides a way to use certificates for user and server authentication and for dynamic session key generation.
- **PEAP**— Protected Extensible Authentication Protocol (PEAP) is an 802.1X authentication type for wireless LANs (WLANs). PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging. PEAP is based on an Internet Draft that Cisco Systems, Microsoft, and RSA Security submitted to the IETF.

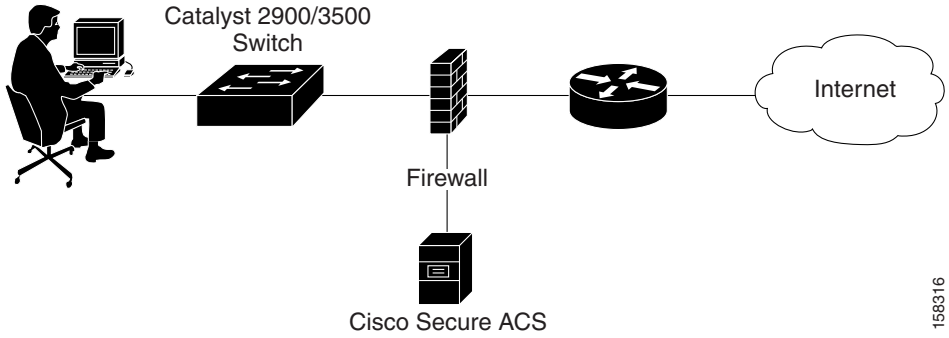
Small LAN Environment

In a small LAN environment (a LAN containing up to 3,000 users; see Figure 2-1), a single ACS is usually located close to the switch and behind a firewall. In this environment, the user database is usually small because few switches require access to ACS for AAA, and the workload is small enough to require only a single ACS.

However, you should still deploy a second ACS server for redundancy, and set up the second ACS server as a replication partner to the primary server; because, losing the ACS would prevent users from gaining access to the network. In Figure 2-1, an Internet connection via firewall and router are included because these are likely to be features of such a network; but, they are not strictly related to the Cisco Catalyst AAA setup or required as part of it.

You should also limit access to the system hosting the ACS to as small a number of users and devices as necessary. As shown in Figure 2-1, you set access by connecting the ACS host to a private LAN segment on the firewall. Access to this segment is limited only to the Cisco Catalyst Switch client and those user machines that require HTTP access to the ACS for administrative purposes. Users should not be aware that the ACS is part of the network.

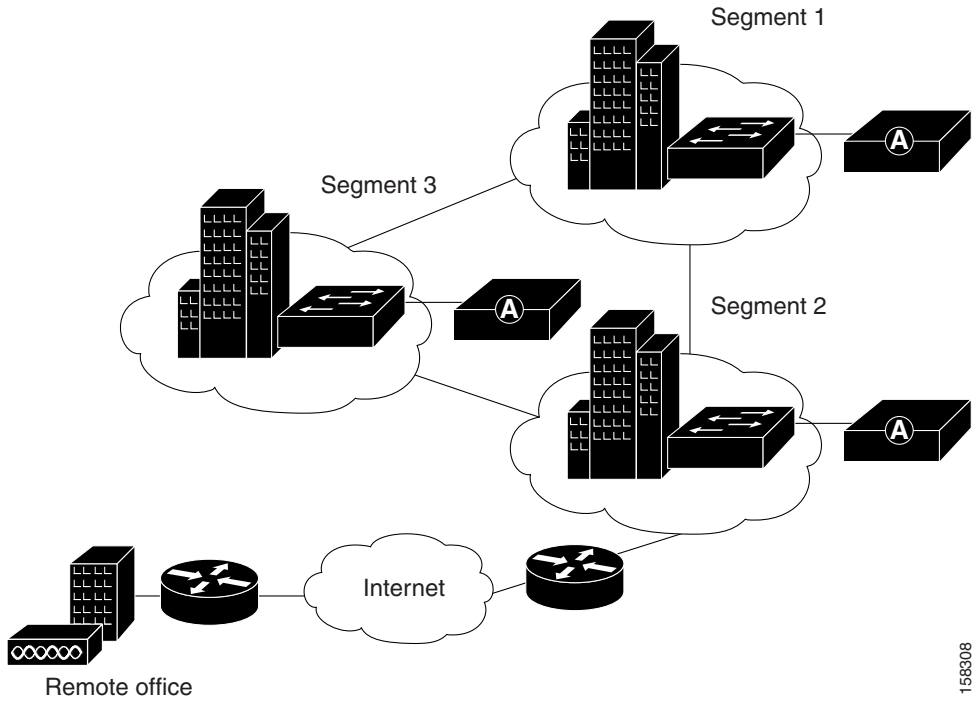
Figure 2-1 ACS Server in a Small LAN Environment



Campus LAN

You can use ACS for wired access in a campus LAN. A campus LAN is typically divided into subnets. Figure 2-2 shows an ACS deployment in a wired campus LAN.

Figure 2-2 ACS in a Campus LAN



The illustration in Figure 2-2 shows a possible distribution of ACS in a wired campus LAN. In this campus LAN, buildings are grouped into three segments. Each segment consists of 1 to 3 buildings and all the buildings in the segment are on a common LAN. All interbuilding and intersegment network connections use one-gigabyte fiber-optic technology. Primary network access is through switch ports over wired Ethernet.

You use ACS to provide RADIUS authentication for the network access servers, and you configure it to use an external database. One ACS is deployed for each segment of 5 to 10 buildings. A Cisco LocalDirector content switch is placed before each ACS for load balancing and failover.

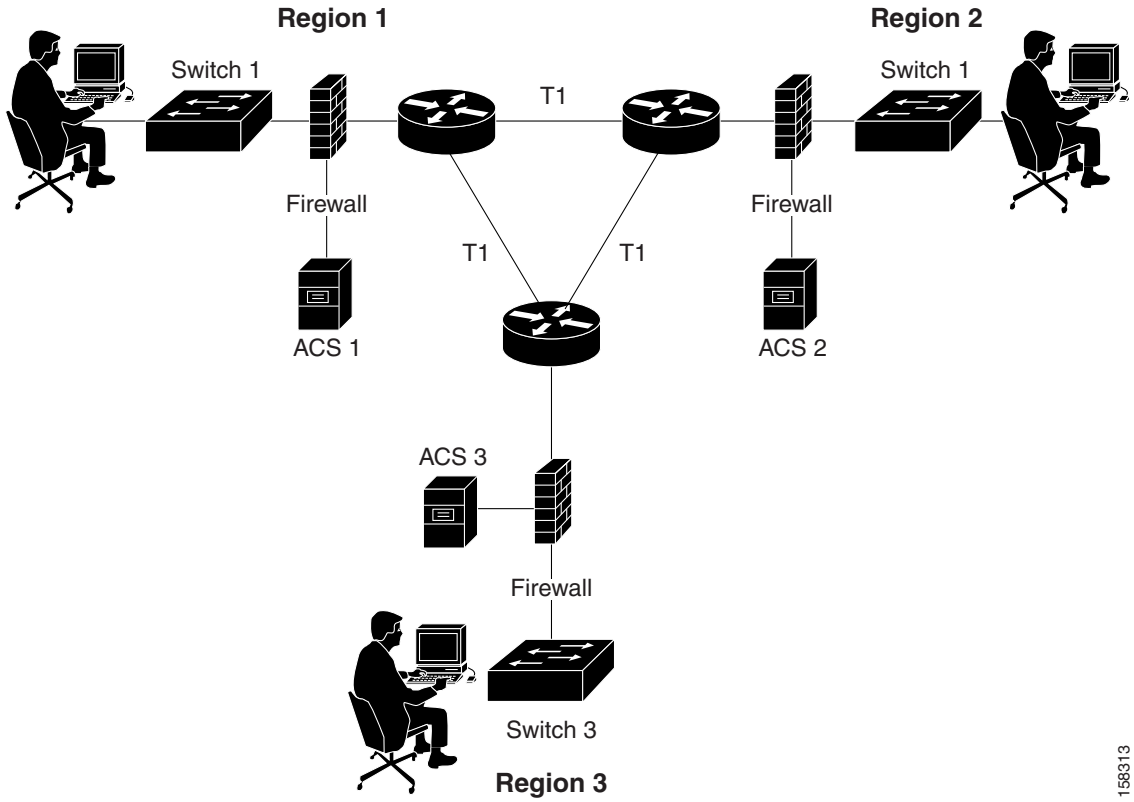
Geographically Dispersed Wired LAN

In a larger network that is geographically dispersed, speed, redundancy, and reliability are important in determining whether to use a centralized ACS service or a number of geographically dispersed ACS units. As with many applications, AAA clients rely on timely and accurate responses to their queries. Network speed is an important factor in deciding how to deploy ACS; because delays in authentication that the network causes can result in timeouts at the client side or the switch.

A useful approach in large extended networks, such as for a globally dispersed corporation, is to have at least one ACS deployed in each major geographical region. Depending on the quality of the WAN links, these servers may act as backup partners to servers in other regions to protect against failure of the ACS in any particular region.

Figure 2-3 shows ACS deployed in a geographically dispersed wired LAN. In the illustration, Switch 1 is configured with ACS 1 as its primary AAA server but with ACS 2 of Region 2 as its secondary. Switch 2 is configured with ACS 2 as its primary but with ACS 3 as its secondary. Likewise, Switch 3 uses ACS 3 as its primary but ACS 1 as its secondary. Using a local ACS as the primary AAA server minimizes AAA WAN traffic. When necessary, using the primary ACS from another region as the secondary further minimizes the number of ACS units.

Figure 2-3 ACS in a Geographically Dispersed LAN



Wireless Access Topology

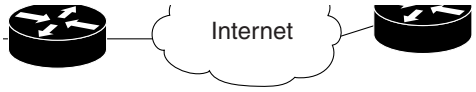
A wireless access point (AP), such as the Cisco Aironet series, provides a bridged connection for mobile end-user clients into the LAN. Authentication is absolutely necessary, due to the ease of access to the AP. Encryption is also necessary because of the ease of eavesdropping on communications.

Scaling can be a serious issue in the wireless network. The mobility factor of the WLAN requires considerations similar to those given to the dial-up network. Unlike the wired LAN, however, you can more readily expand the WLAN. Though WLAN technology does have physical limits as to the number of users who can connect via an AP, the number of APs can grow quickly. As with the dial-up network, you can structure your WLAN to allow full access for all users, or provide restricted access to different subnets among sites, buildings, floors, or rooms. This capability raises a unique issue with the WLAN: the ability of a user to roam among APs.

Simple WLAN

A single AP might be installed in a simple WLAN (Figure 2-4). Because only one AP is present, the primary issue is security. An environment such as this generally contains a small user base and few network devices. Providing AAA services to the other devices on the network does not cause any significant additional load on the ACS.

Figure 2-4 Simple WLAN



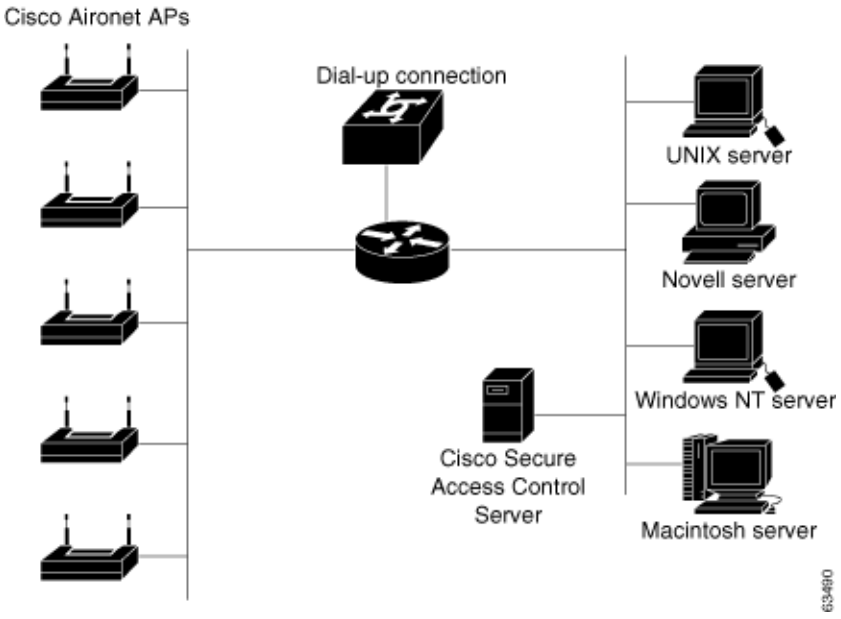
158308

fice

Campus WLAN

In a WLAN where a number of APs are deployed, as in a large building or a campus environment, your decisions on how to deploy ACS become more complex. Depending on the processing needs of the installation, all of the APs might be on the same LAN. Figure 2-5 shows all APs on the same LAN; however, the APs might also be distributed throughout the LAN, and connected via routers, switches, and so on.

Figure 2-5 Campus WLAN



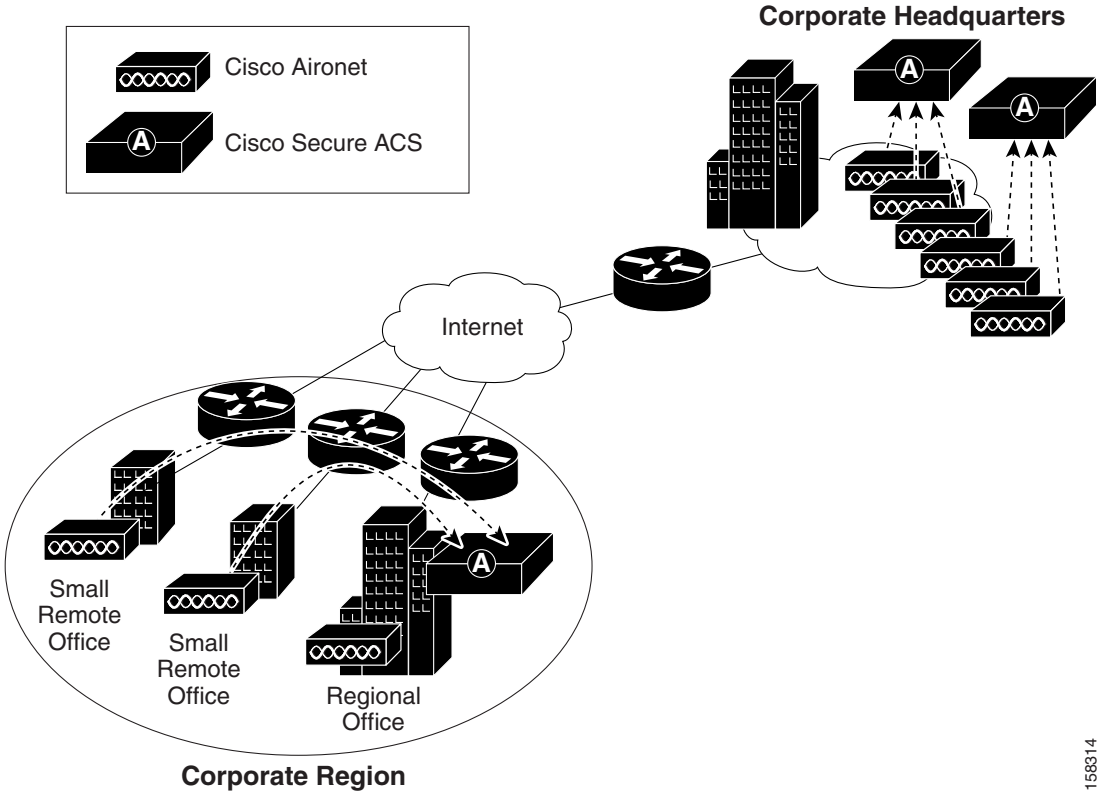
63490

Regional WLAN Setting

In a given geographical or organizational region, the total number of users might or might not reach a critical level for a single ACS. Small offices would not qualify for separate installations of ACSs and a regional office might have sufficient reserve capacity. In this case, the small offices can authenticate users across the WAN to the larger regional office. Once again, you should determine that this does not pose a risk to the users in the remote offices. Assess critical connectivity needs against the reliability and throughput to the central ACS.

Figure 2-6 shows a regional WLAN.

Figure 2-6 ACS in a Regional WLAN



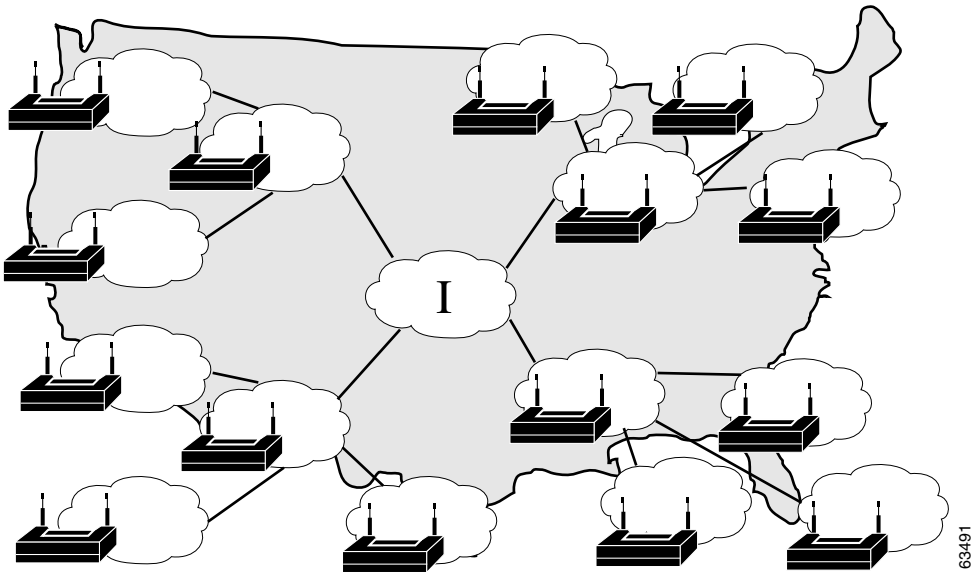
Large Enterprise WLAN Setting

In a very large geographically dispersed network (over 50,000 users), access servers might be located in different parts of a city, in different cities, or on different continents. If network latency is not an issue, a central ACS might work; but, connection reliability over long distances might cause problems. In this case, local ACSs may be preferable to a central ACS.

If the need for a globally coherent user database is most important, database replication or synchronization from a central ACS may be necessary. For information on database replication considerations, see Database Replication Considerations, page 2-12 and Database Synchronization Considerations, page 2-13. Authentication by using external databases, such as a Windows user database or the Lightweight Directory Access Protocol (LDAP), can further complicate the deployment of distributed, localized ACSs.

Figure 2-7 shows ACS installations in a geographically dispersed network that contains many WLANs.

Figure 2-7 ACS in a Geographically Dispersed WLAN



For the model in Figure 2-7, the location of ACS depends on whether all users need access on any AP, or require only regional or local network access. Along with database type, these factors control whether local or regional ACSs are required, and how database continuity is maintained. In this very large deployment model (over 50,000 users), security becomes a more complicated issue, too.

Additional Considerations for Deploying ACS in a WLAN Environment

You should also consider the following when deploying ACS in a WLAN environment, consider if:

- Wireless is secondary to wired access, using a remote ACS as a secondary system is acceptable.
- Wireless is the primary means of access, put a primary ACS in each LAN.
- The customer uses ACS for user configuration, data replication is critical.

Dial-up Access Topology

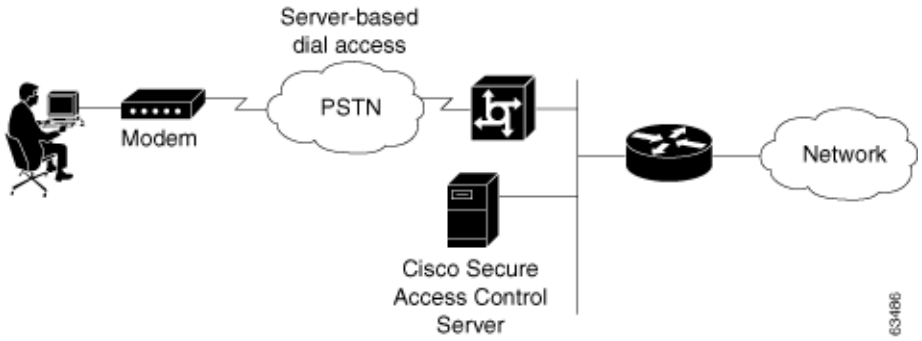
Until recently, dial-up access was the most prevalent method for providing remote access to network resources. However, DSL access and access through VPNs have largely replaced dial-up access through modems.

ACS is still used in some LAN environments to provide security for dial-up access. You can provide dial-up access for a small LAN or for a large dial-in LAN.

Small Dial-Up Network Access

In the small LAN environment, see Figure 2-8, network architects typically place a single ACS internal to the AAA client, which a firewall and the AAA client protect from outside access. In this environment, the user database is usually small; because, few devices require access to the ACS for authentication, authorization and accounting (AAA), and any database replication is limited to a secondary ACS as a backup.

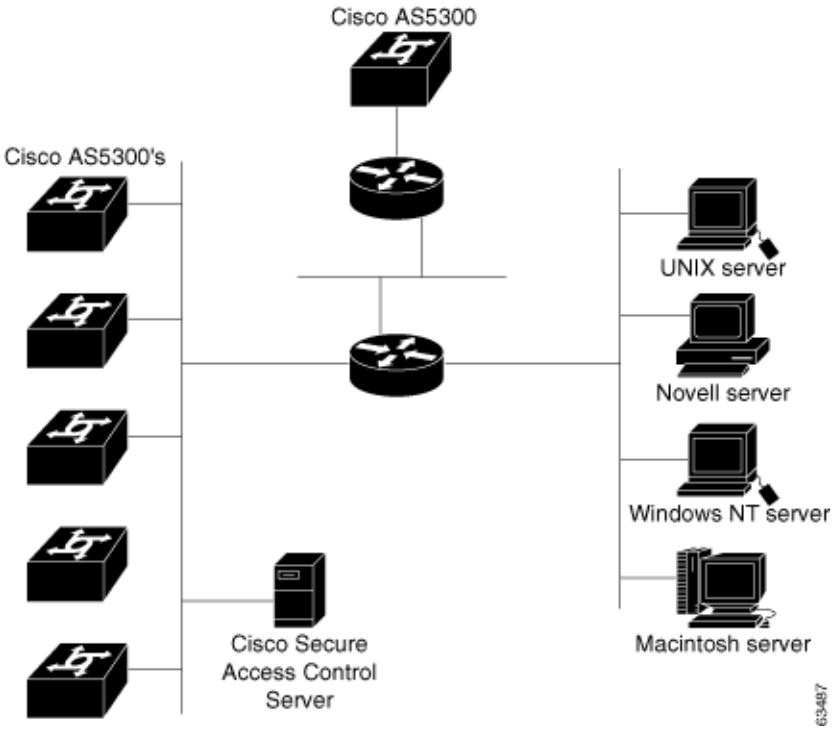
Figure 2-8 Small Dial-up Network



Large Dial-Up Network Access

In a larger dial-in environment, a single ACS with a backup may be suitable, too. The suitability of this configuration depends on network and server access latency. Figure 2-9 shows an example of a large dial-in network. In this scenario, the addition of a backup ACS is recommended.

Figure 2-9 Large Dial-up Network



Placement of the RADIUS Server

From a practical standpoint, the RADIUS server should be inside the general network, preferably within a secure subnet designated for servers, such as DHCP, Domain Name System (DNS), and so on. You should avoid requiring RADIUS requests to travel over WAN connections because of possible network delays and loss of connectivity. Due to various reasons, this type of configuration is not always possible; for example, with small remote subnets that require authentication support from the enterprise.

You must also consider backup authentication. You may use a system that is dedicated as the RADIUS secondary. Or, you may have two synchronized systems that each support a different network segment but provide mutual backup if one fails. Refer to the documentation for your RADIUS server for information on database replication and the use of external databases.

Determining How Many ACSs to Deploy (Scalability)

A number of factors affect the scalability of an ACS installation (that is, how effectively each ACS can process user access requests) and how many ACS servers you should deploy in the network.

For detailed information on scalability considerations, see the following white papers on ACS deployment, which are available on Cisco.com at:

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

- *Building a Scalable TACACS+ Device Management Framework*
- *Catalyst Switching and ACS Deployment Guide*
- *Deploying Cisco Secure ACS for Windows in Cisco Aironet Environment*
- *EAP-TLS Deployment Guide for Wireless LAN Networks*
- *Guidelines for Placing ACS in the Network*

This section contains:

Number of Users

In all topologies, the number of users is an important consideration. For example, assuming that an ACS can support 21,000 users, if an wireless access point can support 10 users, then a given ACS could support 2,100 wireless access points in a WLAN environment.

The size of the LAN or WLAN is determined by the number of users who use the LAN or WLAN:

Size	Users
small LAN	1 to 3,000
medium-sized LAN	3,000 to 25,000
large LAN	25,000 to 50,000
very large LAN or WLAN	over 50,000

For a detailed formula, see the white paper *Deploying Cisco Secure ACS for Windows in Cisco Aironet Environment*, which is available on Cisco.com at this location:

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

Number of Network Access Servers

An ACS can support up 5,000 discrete network access servers (NASs). You can use the multi-NAS capability of ACS to increase this number.

LAN Versus WAN Deployment (Number of LANs in the Network)

In general, you should provide one ACS server per LAN. If a backup ACS is required, the backup ACS may reside on the same LAN or can be an ACS on another LAN.

WAN Latency and Dependability

The distance between LANs in a large network (25,000 to 50,000 users) is also a consideration.

If the network is centralized, one primary ACS and one secondary ACS might be sufficient.

If the network is geographically dispersed, the number of ACS servers required varies with the needs of the regions. For example:

- Some regions may not need a dedicated ACS.
- Larger regions (regions with over 10,000 users), such as corporate headquarters, might need several ACSs.

The distance between subnets is also a consideration. If subnets are close together, the connections will be more reliable, and fewer ACS servers will be needed. Adjacent subnets could serve other buildings with reliable connections. If the subnets are farther apart, more ACS servers might be needed.

The number of subnets and the number of users on each subnet is also a factor. For example, in a WLAN, a building may have 400 potential users and the same subnet might comprise four buildings. One ACS assigned to this subnet will service 1,600 users (about one tenth of the number of current users). Other buildings could be on adjacent subnets with reliable WAN connections. ACSs on adjacent subnets could then be used as secondary systems for backup.

If the WAN connections between buildings in this subnet are short, reliable, and pose no issue of network latency, two ACSs can service all of these buildings and all the users. At 40-percent load, one ACS would take half of the access points as the primary server, and the other ACS would take the remaining APs. Each ACS would provide backup for the other. Again, at 40-percent load, a failure of one ACS would

only create an 80-percent load on the other ACS for the duration of the outage. If the WAN is not suitable for authentication connections, we recommend using two or more ACSs on the LAN in a primary or secondary mode or load balanced.

Determining How Many ACS Servers to Deploy in Wireless Networks

In planning how many ACS servers to deploy in a wireless network, consider:

- The location and number of access points. For example, with 4,200 APs:
  - One ACS could handle half of the APs as primary server.
  - Other ACSs could handle the remaining APs.
- The number of EAP-TLS clients together with EAP-TLS authentications per second
- The number of clients
- Scalability with different protocols

  For example, if you use EAP-TLS, you will need more ACS servers; but, if you use PEAP, you will need fewer. EAP-TLS is slower than PEAP due to public-key infrastructure (PKI) processing time.

For a detailed formula that you can be use to calculate the number of ACS servers required in a wireless network, see the white paper titled *Deploying Cisco Secure ACS for Windows in an Aironet Environment*, available on Cisco.com at:

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

Deploying ACS Servers to Support Server Failover

This section discusses deployment topologies for implementing server failover. This section contains:

- Load Balancing and Failover, page 2-12
- Database Replication Considerations, page 2-12
- Database Synchronization Considerations, page 2-13

Load Balancing and Failover

To implement load balancing, you can set up user groups and then assign groups to a specific RADIUS server (usually the nearest RADIUS server).

Database Replication Considerations

Database replication replicates selected database information, such as user and group information, from a primary ACS to one or more ACS backups or clients. The following aspects of replication are configurable with ACS:

- **Configuration components for replication**—What is replicated.
- **Replication scheduling**—When replication occurs.
- **Replication frequency**—How often systems are replicated.
- **Replication partners**—Which systems are replicated.

- **Client configuration**—How to configure the client.
- **Reports and event (error) handling**—What information to include in the logs.

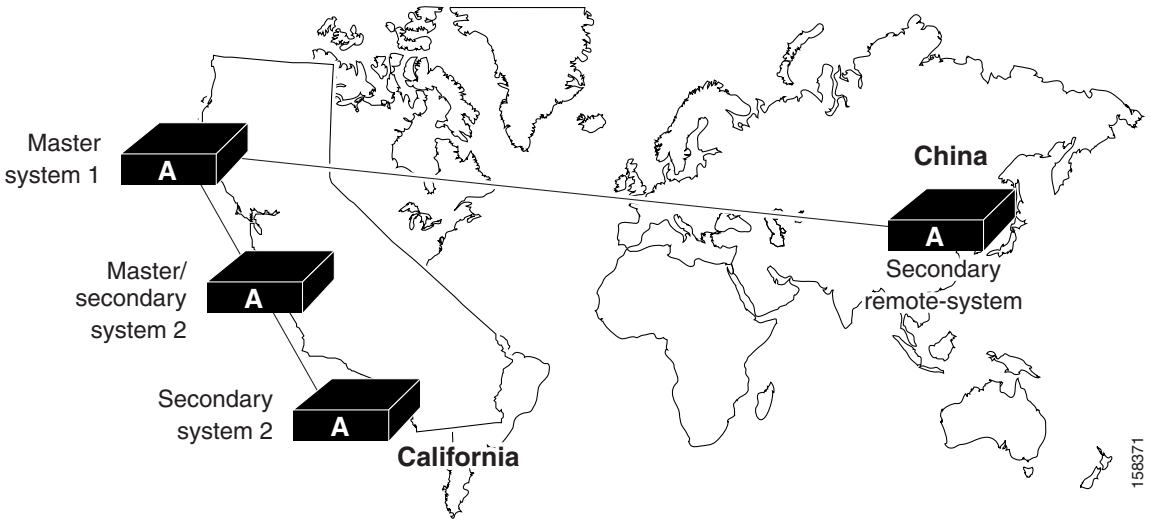
Replication Design

Because database replication in a ACS is a top-down approach, using the cascade method minimizes replication-induced downtime on the master server. If the primary server is not used for authentication services, but for database maintenance only, the cascade method may not be as critical.

However, when traveling across time zones, particularly international time zones, it may be necessary to use the cascade method going to remote secondaries. In this case, when you configure database replication on the Database replication setup page, click the **At specific times** radio button instead of the **Automatically triggered cascade** radio button.

Use the automatically triggered cascade method so that local replication occurs during a time that will minimize the impact on user authentication. During these long-distance replications, replicating to the backup or secondary server first also helps reduce this impact. Figure 2-10 shows a hypothetical deployment for replication where each region has a primary and a secondary ACS deployed. In this scenario, replication is made to the secondary servers to avoid replication downtime to the primary, but, may not be needed if the primary is used mainly for database maintenance but not for authentication.

Figure 2-10 ACS Database Replication Scenario



Database Synchronization Considerations

An alternative to database replication is the use of Relational Database Management System (RDBMS) synchronization. You use the RDBMS synchronization feature to update the ACS user database with information from an Open Database Connectivity (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. RDBMS synchronization supports addition, modification, and deletion for all data items it can access.

Additional Topics

This section discusses additional topics to consider when deploying AC. This section contains:

Remote Access Policy

Remote access is a broad concept. In general, it defines how the user can connect to the LAN, or from the LAN to outside resources (that is, the Internet). Connectivity is possible in many ways: dial-in, ISDN, wireless bridges, and secure Internet connections. Each method incurs its own advantages and disadvantages, and provides a unique challenge to providing AAA services. In addition to the method of access, other decisions can also affect how ACS is deployed; these include specific network routing (access lists), time-of-day access, individual restrictions on AAA client access, access control lists (ACLs), and so on.

You can implement remote-access policies for employees who telecommute, or mobile users who dial in over ISDN or a public switched telephone network (PSTN). Such policies are enforced at the corporate campus with ACS and the AAA client. Inside the enterprise network, remote-access policies can control wireless access by individual employees.

ACS remote-access policies provide control by using central authentication and authorization of remote users. The Cisco user database maintains all user IDs, passwords, and privileges. You can download ACS policies in the form of ACLs to network access servers such as the Cisco AS5300 Network Access Server, or by allowing access during specific periods, or on specific access servers.

Remote-access policies are part of the overall Cisco corporate security policy.

Security Policy

Every organization that maintains a network should develop a security policy for the organization. The sophistication, nature, and scope of your security policy directly affect how you deploy ACS.

For more information about developing and maintaining a comprehensive security policy, refer to these documents:

- Network Security Policy: Best Practices White Paper
- Delivering End-to-End Security in Policy-Based Networks
- Cisco IOS Security Configuration Guide

Administrative Access Policy

Managing a network is a matter of scale. Providing a policy for administrative access to network devices depends directly on the size of the network and the number of administrators required to maintain the network. A network device can be authenticated locally; but, this ability is not scalable. The use of

network management tools can help in large networks (25,000 to 50,000 users); but, if local authentication is used on each network device, the policy usually entails a single login on the network device. A single login on the network device does not provide adequate network device security.

ACS provides a centralized administrator database, and you can add or delete administrators at one location. TACACS+ is the recommended AAA protocol for controlling AAA client administrative access because of its ability to provide per-command control (command authorization) of AAA client administrator access to the device. RADIUS is not well suited for this purpose because of the one-time transfer of authorization information at the time of initial authentication.

The type of access is also an important consideration. In the case of different administrative access levels to the AAA clients, or if a subset of administrators is to be limited to certain systems, you can use ACS with command authorization per network device to restrict network administrators as necessary. Using local authentication restricts the administrative access policy to no login on a device or by using privilege levels to control access.

Controlling access by means of privilege levels is cumbersome and not very scalable. Such control requires altering the privilege levels of specific commands on the AAA client device and defining specific privilege levels for the user login. You can easily create more problems by editing command privilege levels. Using command authorization on ACS does not require that you alter the privilege level of controlled commands. The AAA client sends the command to ACS to be parsed and ACS determines whether the administrator has permission to use the command. The use of AAA allows authentication on any AAA client for any user on ACS and limits access to these devices on a per-AAA-client basis.

A small network with a small number of network devices may require only one or two individuals to administer it. Local authentication on the device is usually sufficient. If you require more granular control than what authentication can provide, some means of authorization is necessary. As discussed earlier, controlling access by using privilege levels can be cumbersome. ACS reduces this problem.

In large enterprise networks, with many devices to administer, the use of ACS practically becomes a necessity. Because administration of many devices requires a larger number of network administrators, with varying levels of access, the use of local control is simply not a viable way to track network-device configuration changes that are required when changing administrators or devices.

The use of network management tools, such as CiscoWorks, helps to ease this burden; but, maintaining security is still an issue. Because ACS can comfortably handle up to 300,000 users, the number of network administrators that ACS supports is rarely an issue. If a large remote-access population is using RADIUS for AAA support, the corporate IT team should consider separate TACACS+ authentication by using ACS for the administrative team. Separate TACACS+ authentication would isolate the general user population from the administrative team and reduce the likelihood of inadvertent access to network devices. If the use of TACACS+ is not a suitable solution, using TACACS+ for administrative (shell or exec) logins, and RADIUS for remote network access, provides sufficient security for the network devices.

Separation of Administrative and General Users

You should prevent the general network user from accessing network devices. Even though the general user may not intend to gain unauthorized access, inadvertent access could accidentally disrupt network access. AAA and ACS provide the means to separate the general user from the administrative user.

The easiest and recommended method to perform such separation is to use RADIUS for the general remote-access user and TACACS+ for the administrative user. One issue is that an administrator may also require remote network access, like the general user. If you use ACS, this issue poses no problem. The administrator can have RADIUS and TACACS+ configurations in ACS. By using authorization, RADIUS users can set PPP (or other network access protocols) as the permitted protocol. Under TACACS+, only the administrator would be configured to have shell (exec) access.

For example, if the administrator is dialing in to the network as a general user, a AAA client would use RADIUS as the authenticating and authorizing protocol, and the PPP protocol would be authorized. In turn, if the same administrator remotely connects to a AAA client to make configuration changes, the AAA client would use the TACACS+ protocol for authentication and authorization. Because this administrator is configured on ACS with permission for shell under TACACS+, the administrator would be authorized to log in to that device. This does require that the AAA client have two separate configurations on ACS, one for RADIUS and one for TACACS+.

An example of a AAA client configuration under IOS that effectively separates PPP and shell logins is:

```
aaa new-model
tacacs-server host  ip-address
tacacs-server key  secret-key
radius-server host  ip-address
radius-server key  secret-key
aaa authentication ppp default group radius
aaa authentication login default group tacacs+ local
aaa authentication login console none
aaa authorization network default group radius
aaa authorization exec default group tacacs+ none
aaa authorization command 15 default group tacacs+ none
username  user  password  password
line con 0
login authentication console
```

Conversely, if a general user attempts to use his or her remote access to log in to a network device, ACS checks and approves the username and password; but, the authorization process would fail because that user would not have credentials that allow shell or exec access to the device.

Database Considerations

Aside from topological considerations, the user database is one of the most influential factors in deployment decisions for ACS. The size of the user base, distribution of users throughout the network, access requirements, and type of user database are all factors to consider when you decide how to deploy ACS.

Number of Users

ACS is designed for the enterprise environment, and can handle 300,000 users. This capacity is usually more than adequate for a corporation. In an environment that exceeds these numbers, the user base would typically be geographically dispersed, which requires the use of more than one ACS configuration. A WAN failure could render a local network inaccessible because of the loss of the authentication server. In addition, reducing the number of users that a single ACS handles improves performance by lowering the number of logins occurring at any given time and reducing the load on the database.

Type of Database

ACS supports several database options, including the ACS internal database or using remote authentication with any of the external databases that are supported. For more information about database options, types, and features, see Table 1-2 ?????? where specifies non-EAP authentication protocol support., page 1-7, Chapter 13, “User Databases,” or Chapter 17, “ ????? where ??User Group Mapping and Specification.” Each database option has its own advantages and limitations in scalability and performance.

Network Latency and Reliability

Network latency and reliability are also important factors in how you deploy ACS. Delays in authentication can result in timeouts for the end-user client or the AAA client.

The general rule for large, extended networks, such as those in a globally dispersed corporation, is to have at least one ACS deployed in each region. This configuration may not be adequate without a reliable, high-speed connection between sites. Many corporations use secure VPN connections between sites so that the Internet provides the link. Although this option saves time and money, it does not provide the speed and reliability of a dedicated frame relay or T1 link. If a reliable authentication service is critical to business functionality, such as a WLAN of retail outlets with cash registers that are linked by a WLAN, the loss of WAN connection to a remote ACS could be catastrophic.

The same issue can be applied to an external database that ACS uses. You should deploy the database close enough to ACS to ensure reliable and timely access. Using a local ACS with a remote database can result in the same problems as using a remote ACS. Another possible problem in this scenario is that a user may experience timeout problems. The AAA client would be able to contact ACS; but, ACS would wait for a reply that might be delayed or never arrive from the external user database. If the ACS were remote, the AAA client would time out and try an alternate method to authenticate the user; but, in the latter case, it is likely the end-user client would time out first.

CHAPTER 3

Password Policy Configuration Scenario

Cisco Secure ACS 4.1, hereafter referred to as ACS, provides new password features to support corporate requirements mandated by the Sarbanes-Oxley Act of 2002. Sarbanes-Oxley (SOX) requires stricter enforcement of password restrictions.

ACS provides SOX support, which includes:

- Enforcement of password lifetime policy
- Enforcement of inactivity limits
- Improved password constraints

To enable password configuration that includes these new features, ACS 4.1 provides a new password policy page.

All administrator logins are subject to the policy that you configure for passwords and accounts, unless you check the **Account Never Expires** check box. For example, ACS provides configurable limits on password lifetime and 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.

Limitation on Ability of the Administrator to Change Passwords

With ACS 4.1, if an administrator is not granted full administrative access, the only action the administrator can take is to change his or her own password.

Summary of Configuration Steps

To configure password policy in ACS 4.1:

Step 1 Add a new administrator account.

Add a new administrator account, specify the administrator name and password, and grant access privileges. See Step 1: Add and Edit a New Administrator Account, page 3-2 for details.

Step 2 Configure password policy.

Configure restrictions on the admin user password. See Step 2: Configure Password Policy, page 3-4 for details.

Step 3 Configure session policy.

Configure restrictions on the admin user's session. See Step 3: Configure Session Policy, page 3-7 for details.

Step 4 Configure access policy.

Configure restrictions on admin access, such as the IP addresses from which administrators can log in. See Step 4: Configure Access Policy, page 3-9 for details.

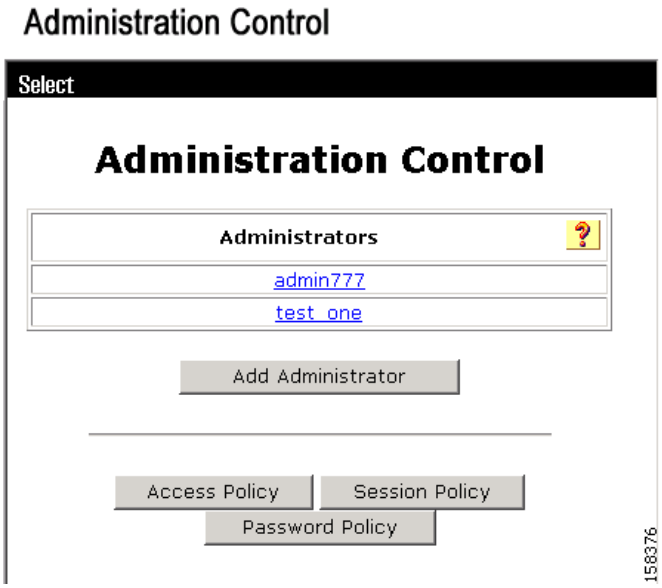
Step 1: Add and Edit a New Administrator Account

To add a new administrator account:

Step 1 In the navigation bar, click **Administration Control.**

The Administration Control page appears, as shown in Figure 3-1.

Figure 3-1 Administration Control Page



The Administration Control page initially lists no administrators. If administrators have been configured, the page lists the configured administrators.

Step 2 To add an administrator, click **Add Administrator.**

The Add Administrator page opens.

Step 3 In the Administrator Details area, enter:

Option	Description
Administrator Name	Enter 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.
Password	Enter the password for the administrator to access the ACS web interface. 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. Passwords must be at least 4 characters long and contain at least 1 numeric character. The password cannot include the username or the reverse username, must not match any of the previous 4 passwords. and must be in ASCII characters. For errors in passwords, ACS displays the password criteria. 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.
Confirm Password	Reenter the password that you entered in the password field.

Option	Description
Account Never Expires	If you want to override the lockout options set up on the Administrator Password Policy page (with the exception of manual lockout), check the check box next to Account Never Expires. If you check this option, the account never expires but password change policy remains in effect. The default value is unchecked (disabled).
Account Locked	If you want to lock out an administrator who is denied access due to the account policy options specified on the Password Policy page, check the check box for **Account Locked**. When unchecked (disabled), this option unlocks an administrator who was locked out. 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. 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. The reset of a locked account does not affect the configuration of the lockout and unlock mechanisms for failed attempts.

Step 4 Click **Grant All** or **Revoke All** to globally add or remove all privileges,

Step 5 If you want to grant specific privileges to the administrator, check the check boxes that correspond to the privileges that you want to grant.

Note For more information on administrative privileges, see the "Add Administrator and Edit Administrator Pages" section in Chapter 11 of the *User Guide for Cisco Secure Access Control Server 4.1*, "Administrators and Administrative Policy."

Step 6 Go to Step 2: Configure Password Policy, page 3-4 (the next section of this chapter) and follow the steps to specify password restrictions.

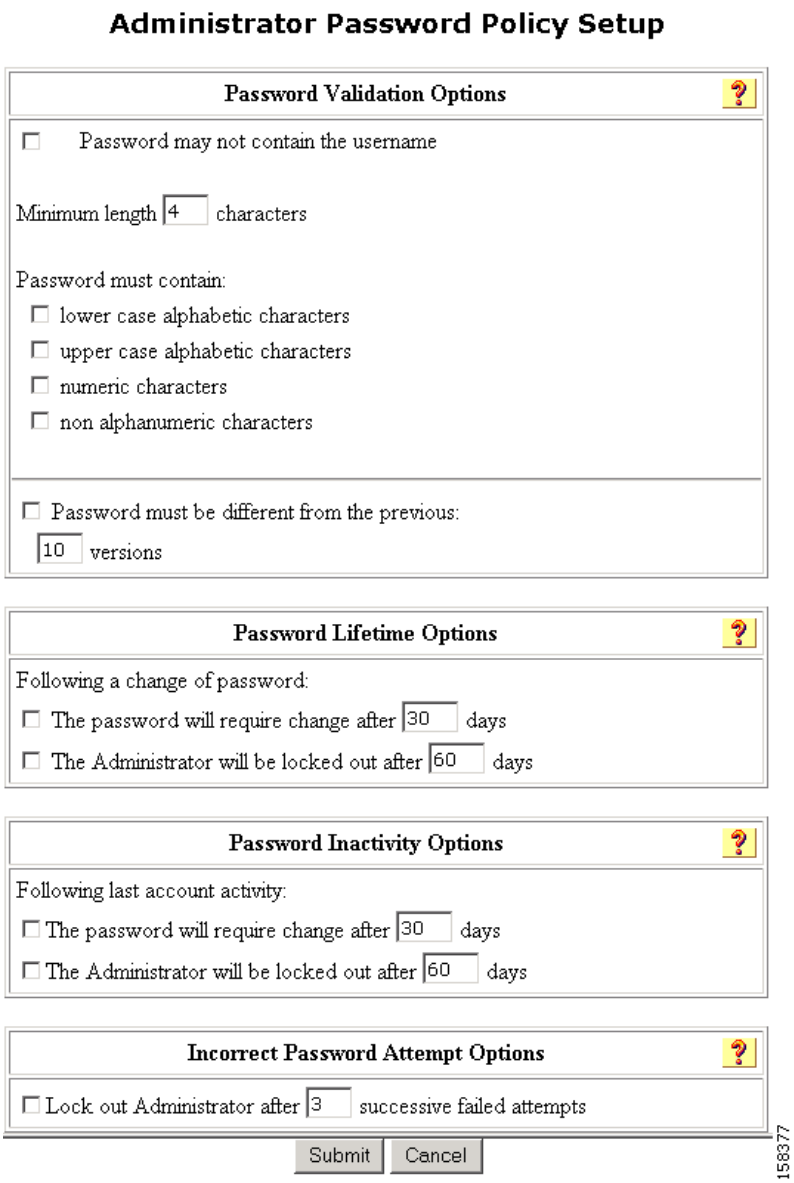
Step 2: Configure Password Policy

To configure password policy:

Step 1 On the Administration Control page, click **Password Policy**.

The Administrator Password Policy Setup page appears, shown in Figure 3-2.

Figure 3-2 The Administrator Password Policy Setup Page



Step 2 On the Password Policy Setup Page, specify:

- Password Validation Options

  See Specify Password Validation Options, page 3-6.
- Password Lifetime Options

  See Specify Password Lifetime Options, page 3-6.
- Password Inactivity Options

  See Specify Password Inactivity Options, page 3-7.
- Incorrect Password Attempt Option

  See Specify Incorrect Password Attempt Options, page 3-7.

Specify Password Validation Options

In the Password Validation Options section, configure:

- **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 (default = 4, range = 4 to 20).
- **Uppercase alphabetic characters**—If enabled, the password must contain uppercase alphabetic characters.
- **Lowercase 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, the at symbol (@).
- **Password must be different from the previous *n* versions**—If enabled, the password must be different from the previous *n* versions (default = 10, range = 0 to 99).

Specify Password Lifetime Options

In the Password Lifetime Options section, configure:

- **The password will require change after *n* days**—Following a change of password, if this option is enabled, *n* specifies the number of days before ACS requires a change of password due to password age (the default value is 30 days). 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 use the greater value of the two.
- **The Administrator will be locked out after *n* days**—Following a change of password, if this option is enabled, *n* specifies the number of days before ACS locks out the associated administrator account due to password age. The default value is 30 days; the range is1 to 365 days.

Specify Password Inactivity Options

In the Password Inactivity Options section, configure:

- **The password will require change after *n* days**—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 value is 30 days; the range is 1 to 365 days. When checked (enabled), the Administrator will be locked after *n* days option causes ACS to compare the two Password Inactivity Options and use the greater value of the two.

Note For additional security, ACS does not warn users who are approaching the limit for password inactivity.

- **The Administrator will be locked out after *n* days**—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 (default = 30, range = 1 to 365).

Note For additional security, ACS does not warn users who are approaching the limit for account inactivity.

Specify Incorrect Password Attempt Options

In the Incorrect Password Attempt Options section, configure:

Lock out Administrator after *n* successive failed attempts—If checked (enabled), *n* specifies the allowable number of incorrect password attempts. When checked, *n* cannot be set to zero (0). If not checked (disabled), ACS allows unlimited successive failed login attempts. The default value is 3 days; the range = 1 to 98 days.

Note For additional security, ACS does not warn users who are approaching the limit for failed attempts. If the **Account Never Expires** option is checked (enabled) for a specific administrator, this option is ignored.

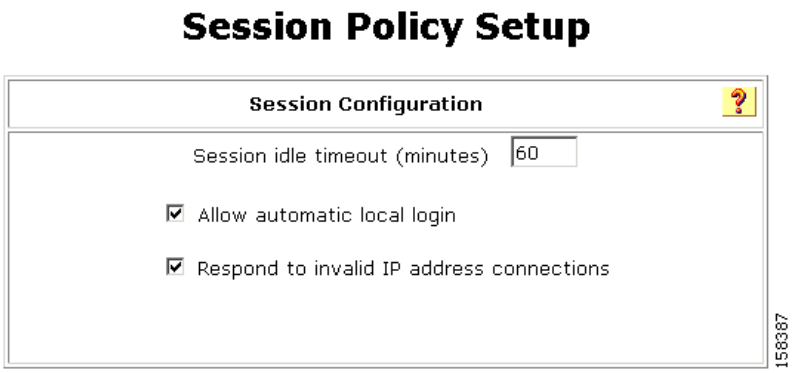
Step 3: Configure Session Policy

To configure session policy:

Step 1 On the Administration Control page, click **Session Policy**.

The Session Policy Setup page opens, as shown in Figure 3-3.

Figure 3-3 The Session Policy Setup Page



Step 2 On the Session Policy Setup page, set session options as required.

You can specify:

- **Session idle timeout (minutes)**—Specifies the time, in minutes, that an administrative session must remain idle before ACS terminates the connection (4-character maximum).

  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.

  This parameter only applies to the ACS administrative session in the browser. It does not apply to an administrative dial-up session.

- **Allow Automatic Local Login (ACS for Windows Only**—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 *local_login* to conduct these sessions.

  When unchecked (disabled), administrators must log in by using administrator names and passwords.

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.

  The local_login administrator account requires the Administration Control privilege. ACS records administrative sessions that use the local_login account in the Administrative Audit report under the local_login administrator name.

- **Respond to invalid IP address connections**—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 unchecked, ACS does not display an error message when a user makes an invalid remote connection attempt. This option is checked (enabled) by default.

  Disabling this option can help to prevent unauthorized users from discovering ACS.

Step 4: Configure Access Policy

This section describes how to configure administrative access policy.

Before You Begin

If you want to enable the SSL for administrator access, you must have completed the steps in Install the CA Certificate, page 5-4, and Add a Trusted Certificate, page 5-4. 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:

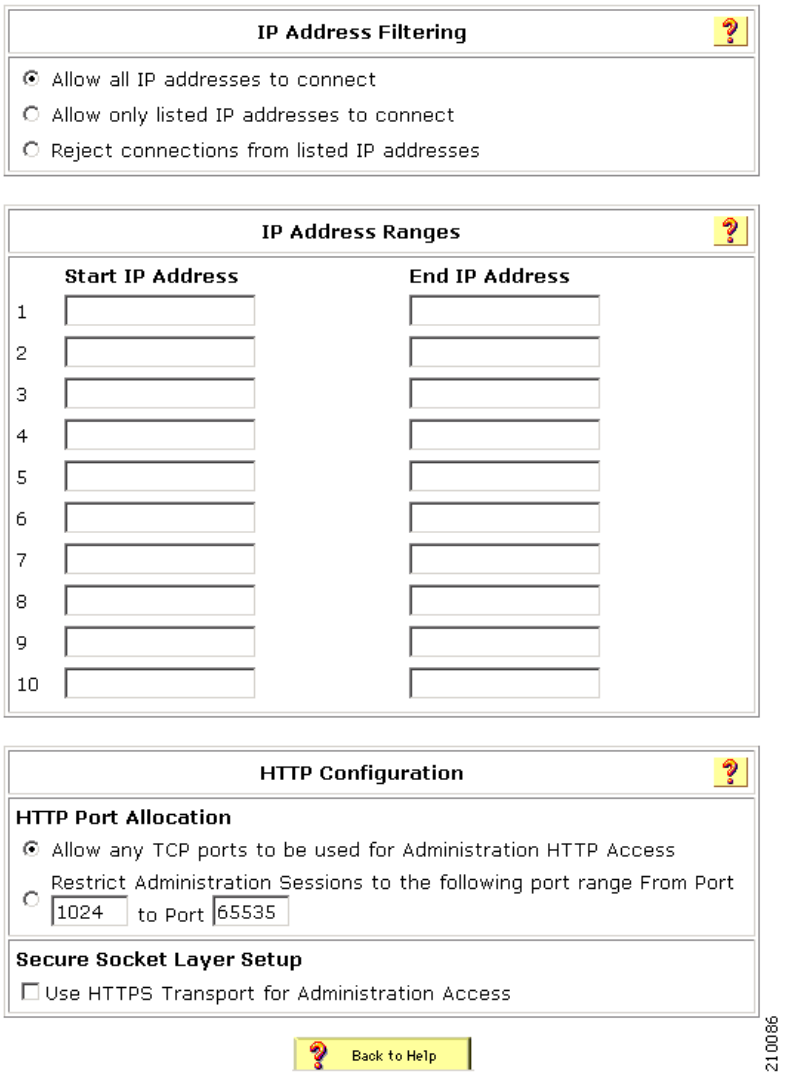
Step 1 In the navigation bar, click **Administration Control**.

ACS displays the Administration Control page.

Step 2 Click **Access Policy**.

The Access Policy Setup page appears, as shown in Figure 3-4.

Figure 3-4 Access Policy Setup Page



Step 3 Click the appropriate **IP Address Filtering** option

Table 3-1 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 3-1 Access Policy Options (continued)

Option	Description
Reject connections from listed IP addresses	Restricts remote access to the web interface to IP addresses outside of the specified IP Address Ranges. 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.
IP Address Ranges	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. Use dotted-decimal format. The IP addresses that define a range must differ only in the last octet (Class C format).
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 *n* to Port *n*	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. 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. 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. 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.

Table 3-1 Access Policy Options (continued)

Option	Description
Secure Socket Layer Setup	
Use HTTPS Transport for Administration Access	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. 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.

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.

Step 6 Check this option if you want ACS to use the SSL.

Step 7 Click **Submit**.

ACS saves and begins enforcing the access policy settings.

Viewing Administrator Entitlement Reports

To assist in SOX compliance, ACS 4.1 produces entitlement report, which contain data extracted from the ACS configuration and formatted into text based files.

ACS produces entitlement reports for administrators and users. The reports that you can generate are:

- **Privilege**—The privileges granted to a selected administrator.
- **Combined Privilege**—The privileges granted to all administrators.
- **Users to Groups Mapping**—The group membership of every user.

View Privilege Reports

To view privilege reports:

Step 1 In the navigation bar, click **Reports and Activity**.

The Reports page opens.

Step 2 Click **Entitlement Reports**.

A list of the available entitlement reports appears. Figure 3-5 shows an example list.

Figure 3-5 List of Entitlement Reports

Step 3 To view a report, click the report name.

Each report is downloaded to the local computer in the form of an Excel spreadsheet.

CHAPTER 4

Agentless Host Support Configuration Scenario

This chapter describes how to configure the agentless host feature in Cisco Secure Access Control Server 4.1, hereafter referred to as ACS.

Note The procedure in this chapter describes how to configure agentless host support by using ACS with a Lightweight Directory Access Protocol (LDAP) database. You can also configure agentless host support by using the ACS internal database: but, using an LDAP database is generally more efficient.

This chapter contains the following sections:

Overview of Agentless Host Support

Many hosts that ACS authenticates run agent software that requests access to network resources and receives authorization from ACS. However, some hosts do not run agent software. For example:

- Many 802.1x port security deployments authenticate hosts that do not have appropriate security agent software, such as Cisco Trust Agent.
- When an agentless host is connected to a Layer 2 device and an Extensible Authentication Protocol over User Datagram Protocol timeout (EoU timeout) occurs, in-band posture validation cannot occur.

ACS 4.1 solves this problem by using the MAC address of the host device to identify and authenticate the host. This technique is called MAC authentication bypass (MAB).

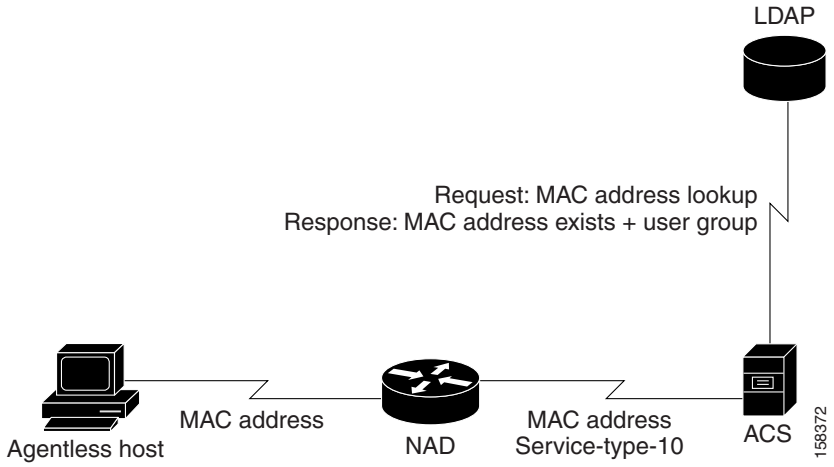
1. When an agentless host connects to a network access device (NAD), the NAD detects that the host does not have an appropriate software agent and uses the host's MAC address to identify it.
2. The NAD sends ACS a RADIUS authorization request with `servicetype=10` and the MAC address of the host contained in the `calling-station-id` attribute.
3. If you configure ACS for MAB, it searches the authentication database for the host's MAC address The database can be:
   - ACS internal

- LDAP (if you configure LDAP)

4. During the database lookup:
   - ACS looks up the MAC address in an identity store (the internal ACS database or an LDAP database).
   - ACS maps the MAC address to an ACS user group.
   - If ACS finds the MAC address, ACS associates the access request to an ACS user group.
   - If ACS does not find the MAC address, ACS assigns the access request to a default group that has been configured for failed MAB. At this stage, ACS proceeds with authorization as for all other access requests.
   - The expected value in the `calling-station-id attribute` is a MAC address; however, if the attribute contains a different value (IP address), ACS looks for the IP address in the access database
   - ACS applies authorization rules based on the user group and associated policies that a network access profile (NAP) contains.

Figure 4-1 shows the flow of MAB information.

Figure 4-1 MAB Flow



Using Audit Servers and GAME Group Feedback

You can configure ACS 4.1 to use audit servers. An audit server is a device that checks the information that the NAD provides against a list of predetermined device types.

With ACS 4.1, the audit server can categorize an end device and provide additional information to ACS. ACS can then make a group assignment decision based on the categorization of the device. For example, if the device is a printer, ACS can assign the device to a user group that includes printers.

In a Cisco Network Admission Control (NAC) environment, ACS 4.1 supports audit server authentication by enabling Generic Authorization Message Exchange (GAME) group feedback.

GAME group feedback provides an added security check for MAC address authentication by checking the device type categorization that ACS determines by associating a MAC address with a user group against information stored in a database on an audit server.

To use the GAME group feedback feature, you must add a NAC attribute-value pair to the ACS RADIUS dictionary before configuring a posture validation policy that uses GAME group feedback.

You then configure a posture validation policy in a NAP that requests device type authentication from the audit server. For details on configuring posture validation, see Enable Posture Validation, page 7-68.

The detailed steps for configuring GAME group feedback are described in Enable GAME Group Feedback, page 7-68 in Chapter 7, "NAC Configuration Scenario"

Summary of Configuration Steps

To configure agentless host support in ACS 4.1:

Step 1 Install ACS for Windows or ACS Solution Engine.

See Step 1Install ACS for Windows or ACS Solution Engine., page 4-3 for details.

Step 2 Configure a RADIUS AAA client.

See Step 2Configure a RADIUS AAA client., page 4-3 for details.

Configure restrictions on the admin user password.

Step 3 Install and set up an ACS security certificate:

Note This step is required to enable posture validation and network access profiles.

a. Obtain certificates and copy them to the ACS host.
b. Run the Windows certificate import wizard to install the certificate
c. Enable security certificates on the ACS installation.
d. Install the CA certificate.
e. Add a trusted certificate.

See Step 3Install and set up an ACS security certificate:, page 4-3 for details.

Step 4 Configure LDAP support for MAB:

a. Configure an external LDAP database for MAB support.
b. Create One or More LDAP Database Configurations in ACS.

See Step 4Configure LDAP support for MAB:, page 4-3 for details.

Step 5 Configure user groups for MAB segments.

See Step 5Configure user groups for MAB segments., page 4-3 for details.

Step 6 Enable agentless request processing:

a. Create a new network access profile (NAP).
b. Enable agentless host processing for the profile.
c. Configure MAB.

See Step 6Enable agentless request processing:, page 4-3 for details.

Step 7 Configure logging and reports.

Add the **Bypass Info** attribute to the Passed Authentications and Failed Attempts reports.
See Step 7Configure logging and reports., page 4-3.

Note If you are using ACS with NAC, configure audit server support and, optionally, configure GAME group feedback. See Configure GAME Group Feedback, page 4-23 for details.

Basic Configuration Steps for Agentless Host Support

This section describes the basic configuration steps for agentless host support.

Step 1: Install ACS

This section describes the installation process that you perform to run ACS, which runs on a Windows 2000 Server, a Windows 2003 system, or a Cisco Secure ACS solution Engine (ACS SE).

To install ACS:

Step 1 Start ACS installation.

For detailed information on ACS installation, refer to the:

- *Installation Guide for Cisco Secure ACS for Windows 4.1*
- *Installation Guide for Cisco Secure ACS Solution Engine 4.1*

During the installation process, you are prompted to enter a password for encrypting the internal database.

Step 2 Enter a password that is at least 8 characters long, and contains letters and numbers.

The ACS installation process for ACS for Windows automatically creates a shortcut to the ACS administrative GUI on your desktop.

Note If you are installing ACS on the ACS SE, you must manually create an administrative GUI user by using the use the **add-guiadmin** command to create a GUI account. For information on this command, see Appendix A of the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*, "Command Reference." You can then access the administrative GUI through a supported browser. For a list of supported browsers, see *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.1.*

Step 3 Double-click the ACS Admin icon to open a browser window to the ACS administrative GUI.

Step 4 If you do not see the ACS Admin icon on the desktop, open your browser from the machine on which you installed ACS and go to one of the following locations:

- http://*IP_address*:2002
- http://*hostname*:2002

where *IP_address* is the IP address of the host that is running ACS and hostname is the *hostname* of the host that is running ACS.

Step 2: Configure a RADIUS AAA Client

Before you can configure agentless host support, you must configure a RADIUS AAA client.

To configure a RADIUS AAA client:

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

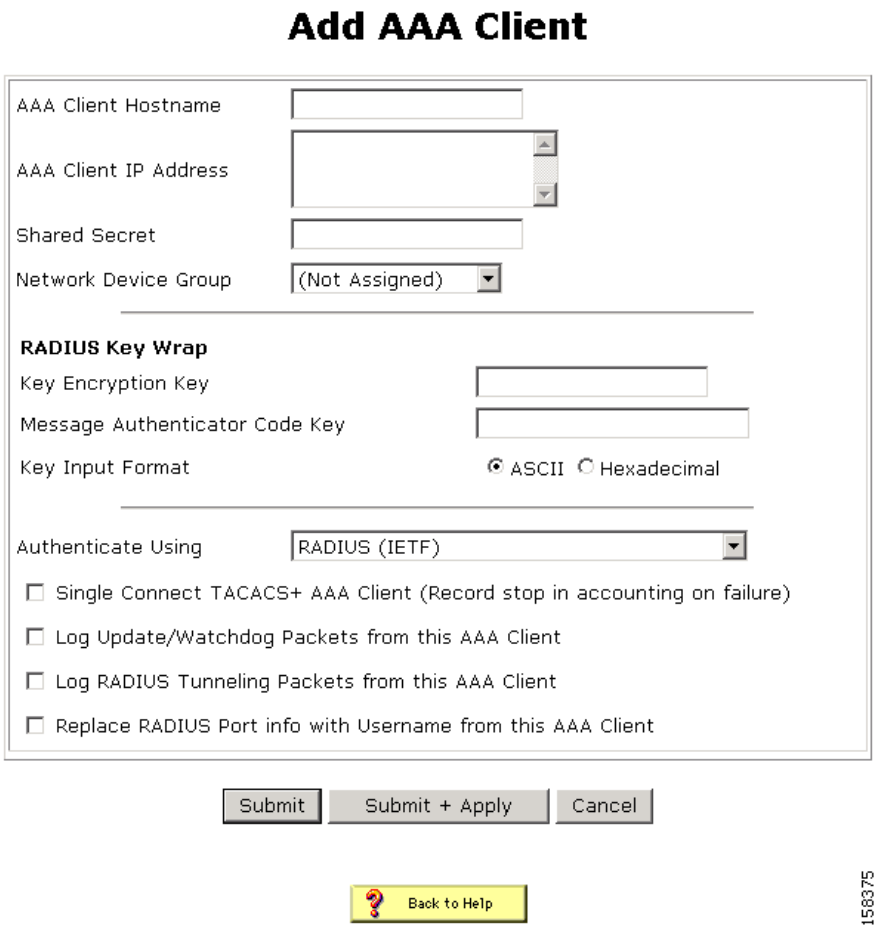
The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using Network Device Groups (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 opens, shown in Figure 4-2.

Figure 4-2 Add AAA Client Page



Step 3 In the AAA Client Hostname box, type the name assigned to this AAA client (up to 32 alphanumeric characters).

Step 4 In the AAA Client IP Address box, type the AAA client IP address or addresses.

Step 5 If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or select **Not Assigned** to set this AAA client to be independent of NDGs

Step 6 From the Authenticate Using list, select **RADIUS (IOS/PIX)**.

Step 7 Specify additional AAA client settings as required.

Step 8 Click **Submit + Apply**.

Step 3: Install and Set Up an ACS Security Certificate

This section describes a simplified procedure for the ACS for Windows platform. For detailed information on installing certificates, and also for information on how to install certificates on the Cisco Secure ACS Solution Engine platform, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.1*, "Advanced Configuration: Authentication and Certificates."

The steps in this section are required to enable posture validation, which is used in network access profiles (NAPs) that are used to

Obtain Certificates and Copy Them to the ACS Host

To copy a certificate to the ACS host:

Step 1 Obtain a security certificate.

Step 2 Create a *\Certs* directory on the ACS server.

a. Open a DOS command window.

b. To create a certificates directory, enter:

`mkdir <`*`selected_drive`***`>:\Certs`**

where *`selected_drive`* is the currently selected drive.

Step 3 Copy the following files to the *\Certs* directory:

- *server.cer* (server certificate)
- *server.pvk* (server certificate private key)
- *ca.cer* (CA certificate)

Run the Windows Certificate Import Wizard to Install the Certificate (ACS for Windows)

To run the Windows Certificate Import wizard to install the certificate on the server:

Step 1 Start Windows Explorer.

Step 2 Go to <*selected_drive*>:*Certs*.

where *`selected_drive`* is the currently selected drive.

Step 3 Double-click the *\Certs\ca.cer* file.

The Certificate dialog appears.

Step 4 Select **Install Certificate.**

The Windows Certificate Import wizard starts.

Step 5 To install the certificate, follow the instructions that the wizard displays.

Step 6 Accept the default options for the wizard.

Note Only perform this process once on a Windows 2000 Server.

Enable Security Certificates on the ACS Installation

To enable security certificates:

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

The System Configuration page opens.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

Step 4 The Install ACS Certificate page opens, shown in Figure 4-3.

Figure 4-3 Install ACS Certificate Page

Step 5 Ensure that you click the **Read certificate from file** radio button.

Step 6 In the Certificate file text box, enter the server certificate location (path and name); for example ***c:\Certs\server.cer***.

Step 7 In the Private Key File text box, type the server certificate private key location (path and name); for example: ***c:\Certs\server.pvk***.

Step 8 In the Private Key password text box, type **1111**.

Step 9 Click **Submit.**

Step 10 ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.

Step 11 Do not restart the services at this time.

Restart the services later, after you have completed the steps for adding a trusted certificate. See Add a Trusted Certificate, page 4-9.

Install the CA Certificate

To install the CA Certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

Step 2 The ACS Certification Authority Setup page appears, shown in Figure 4-4.

Figure 4-4 ACS Certification Authority Setup Page

Step 3 In the CA certificate file box, type the CA certificate location (path and name). For example: *c:\Certs\ca.cer.*

Step 4 Click **Submit**.

Add a Trusted Certificate

After you add a server certificate and set up the certificate authority, install a trusted certificate.

To add a trusted certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > Edit Certificate Trust List**.

The Edit Certificate Trust List appears.

Step 2 Locate the trusted certificate that you want to install and check the corresponding check box by the certificate name. For example, find the **Stress** certificate and check the corresponding check box.

Step 3 Click **Submit**.

Step 4 To restart ACS, choose **System Configuration > Service Control**, and then click **Restart**.

Step 4: Configure LDAP Support for MAB

You can configure the ACS internal database to manage MAB used with the agentless host feature; however, if you have a large number of MAC addresses to process (for example, several thousand), it is more efficient to use an external LDAP database than to configure the MAC address mappings manually through the ACS GUI.

To configure LDAP support for MAB:

Step 1 Configure an External LDAP database for MAB support.

See Configure an External LDAP Database for MAB Support, page 4-10 for details.

Step 2 Create one or more LDAP database configurations in ACS.

See Create One or More LDAP Database Configurations in ACS, page 4-13 for details.

Configure an External LDAP Database for MAB Support

Configure one or more external LDAP databases for MAB support. In each LDAP database, create:

- Device records that describe the agentless hosts that ACS will authenticate.
- LDAP groups that define an LDAP schema to enable MAB for agentless host support.

Example 4-1 shows portions of a sample Lightweight Directory Interchange Format (LDIF) file that defines an LDAP database for agentless host support.

Example 4-1 Sample LDAP Schema for MAB Support

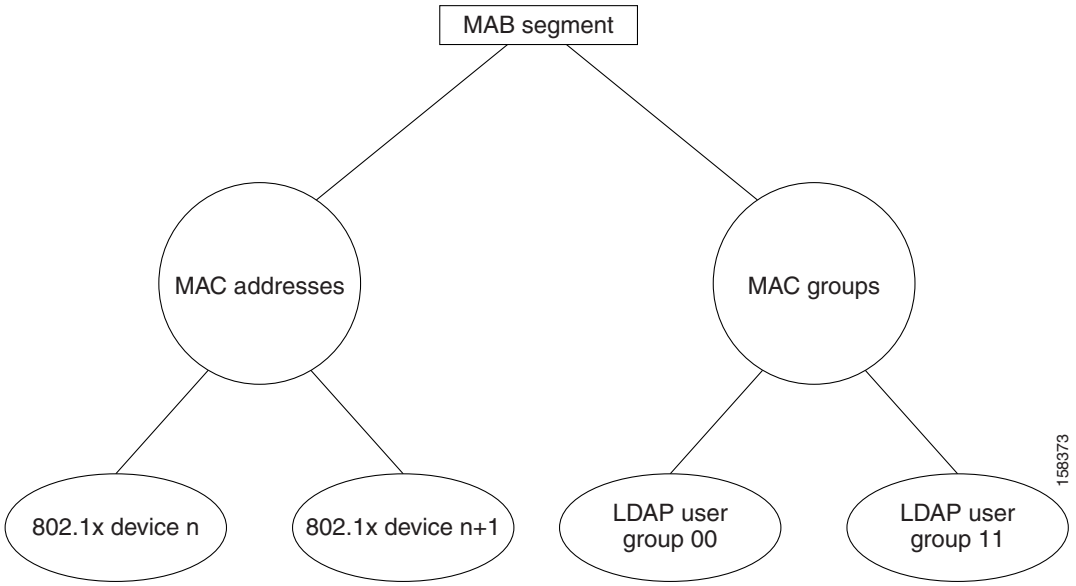
```
dn: ou=MAB Segment, o=mycorp
ou: MAB Segment
objectClass: top
objectClass: organizationalUnit
description: MAC Authentication Bypass Sub-Tree

dn: ou=MAC Addresses, ou=MAB Segment, o=mycorp
ou: MAC Addresses
objectClass: top
objectClass: organizationalUnit

dn: ou=MAC Groups, ou=MAB Segment, o=mycorp
ou: MAC Groups
objectClass: top
objectClass: organizationalUnit

dn: cn=user00-wxp.emea.mycorp.com,ou=MAC Addresses, ou=MAB Segment, o=mycorp
ipHostNumber: 10.56.60.100
objectClass: top
objectClass: ipHost
objectClass: ieee802Device
macAddress: 00:11:22:33:44:55
cn: user00-wxp.emea.mycorp.com

dn: cn=user11-wxp.emea.mycorp.com,ou=MAC Addresses, ou=MAB Segment, o=mycorp
ipHostNumber: 10.56.60.111
objectClass: top
objectClass: ipHost
objectClass: ieee802Device
macAddress: 11-22-33-44-55-66
cn: user11-wxp.emea.mycorp.com

dn: cn=Group_1_colon,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of delimited MAC Addresses
uniqueMember: cn=user00-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
uniqueMember: cn=user77a-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
 , o=mycorp
uniqueMember: cn=user88-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
cn: Group_1_colon

dn: cn=Group_2_dash,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of - delimited MAC Addresses
uniqueMember: cn=user11-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
```

```
uniqueMember: cn=user77b-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
 , o=mycorp
cn: Group_2_dash
```

Description of the Settings in the Sample LDAP Schema

Figure 4-5 shows the tree structure of the LDAP schema that is presented in Example 4-1.

Figure 4-5 Tree Structure for a MAB Support LDAP Schema



How the Subtrees Work

The sample LDAP schema in Example 4-1 contains code to define two subtrees:

```
dn: ou=MAC Addresses, ou=MAB Segment, o=mycorp
ou: MAC Addresses
objectClass: top
objectClass: organizationalUnit

dn: ou=MAC Groups, ou=MAB Segment, o=mycorp
ou: MAC Groups
objectClass: top
objectClass: organizationalUnit
```

The LDAP subtrees are:

- **MAC Addresses**—A user directory subtree that contains device records that specify MAC addresses for agentless hosts (IEEE 802.1x devices that require agentless host authentication by ACS).

  When you specify a user directory subtree during LDAP configuration in the ACS user interface, you enter the name assigned to the user directory subtree in your LDAP schema in the User Directory Subtree text box.

- **MAC Groups**—A group directory subtree that contains LDAP user groups of users who connect from specified MAC devices that are identified in the device records.

When you specify a group directory subtree during LDAP configuration in the ACS user interface, you enter the name assigned to the group directory subtree in your LDAP schema in the Group Directory Subtree text box.

How the LDAP User Groups Work

Each LDAP user group record sets up an LDAP user group that maps users connecting through one or more devices to the specified group.

For example, the LDAP user group identified as `cn=Group_1_colon` sets up an LDAP user group that will map users connecting from the host at 10.56.60.100 as well as from two other hosts:

```
dn: cn=Group_1_colon,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of delimited MAC Addresses
uniqueMember: cn=user00-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
uniqueMember: cn=user77a-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
 , o=mycorp
uniqueMember: cn=user88-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
cn: Group_1_colon
```

ACS queries the LDAP database to determine to which user groups to assign users who connect from a host with a specified MAC address. ACS then assign users in the LDAP user group to a specified ACS user group that you configure.

Table 4-1 describes the attributes of the sample LDAP groups.

Table 4-1 Attributes in LDAP User Groups for Agentless Host Support

Attribute Name	Description
objectClass	The value in the example indicates that this is a “group of unique names.” The value that you specify here must match the name that you specify in the Group Object Class text box when you specify the Common LDAP configuration during ACS LDAP configuration. For information on configuring LDAP, see Configure an External LDAP Database for MAB Support, page 4-10.
uniqueMember	The value in the example is uniqueMember. One or more uniqueMember entries are used to specify one or more device type records that have been set up in the LDAP schema to define agentless hosts with specified MAC addresses. The objectClass field in the LDAP user group shown in the previous code sample includes user00, user77a, and user88. The name that you give to this field in your LDAP schema must match the value that you enter in the Group Attribute Name text box when you specify the common LDAP configuration during ACS LD configuration. For information on configuring LDAP, see Configure an External LDAP Database for MAB Support, page 4-10.

Create One or More LDAP Database Configurations in ACS

After you have configured one or more LDAP databases to support MAB, configure ACS to query the LDAP databases.

The settings in the following procedure are based on the LDAP schema described in the previous section, Configure an External LDAP Database for MAB Support, page 4-10. For your ACS installation, configure ACS based on the schema that you set up for your network.

To create a LDAP configuration in ACS:

Step 1 In the navigation bar, click **External User Databases**.

The External User Databases page opens.

Step 2 Click **Database Configuration**.

The External User Database Configuration page opens.

Step 3 Click **Generic LDAP**.

The Database Configuration Creation table appears. If an LDAP configuration exists, the External User Database Configuration table also appears.

Step 4 Do one of the following. If:

- There are no existing LDAP database configurations, click **Create New Configuratio**n.
- The External User Database table appears, click **Configure**.

Step 5 If you are creating a new LDAP configuration, enter the name of the new configuration for generic LDAP and then click **Submit**.

Step 6 Click **Configure**.

The Generic LDAP Configuration page appears and contains four sections:

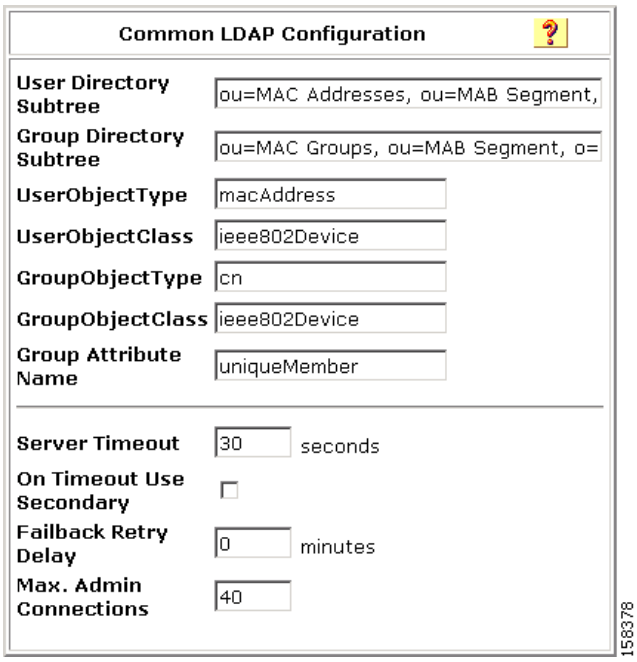
- **Domain Filtering**—Use to configure domain filtering, which is an optional configuration setting.
- **Common LDAP Configuration**—Configure the settings in this section to specify how ACS queries the LDAP database.
- **Primary LDAP Server**—Configure the settings in this section to specify the primary LDAP server.
- **Secondary LDAP Server**—Configure the settings in this section if you are setting up LDAP failback.

Step 7 If you want to set up Domain Filtering, refer to the "Configuring a Generic LDAP External User Database" section in Chapter 12 of the *User Guide for Cisco Secure Access Server 4.1*.

Step 8 Specify the common LDAP configuration

Figure 4-6 shows the Common LDAP Configuration section.

Figure 4-6 Common LDAP Configuration Section



You must specify:

- **User Directory Subtree**—Enter the distinguished name (DN) of the user directory subtree that contains all users. In MAB configuration, the users are, in effect, host devices.

  In the LDAP schema shown in Example 4-1, the DN of the User Directory Subtree is `ou=MAC Addresses, ou=MAB Segment, o=mycorp`.

- **Group Directory Subtree**—Enter the DN for the group directory subtree that contains all user groups as defined in your LDAP schema. In MAB configuration, the members of user groups are actually groups of MAC addresses.

  In the LDAP schema shown in Example 4-1, the DN of the group directory subtree is `ou=MAC Groups, ou=MAB Segment, o=cisco`.

- **UserObjectType**— Enter the name of the user object type that is defined in your LDAP schema. In the LDAP schema shown in Example 4-1, the user object type is specified as `macAddress`.

- **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. In the LDAP schema shown in Example 4-1, the user object class is specified as `ieee802Device`.

- **GroupObjectType**—The name of the attribute in the group record that contains the group name. In tIn the LDAP schema shown in Example 4-1, this is `cn`.

- **GroupObjectClass**—For MAB configuration, specify the name of a device record" that you have set up in your LDAP schema. For example, in Example 4-1, the group object class is `ieee802Device`.

- **GroupAttributeName**—For MAB configuration, specify the name of the LDAP attribute that specifies a LDAP user group. For example, in Example 4-1, each member of a LDAP user group is specified in a `uniqueMember` attribute.

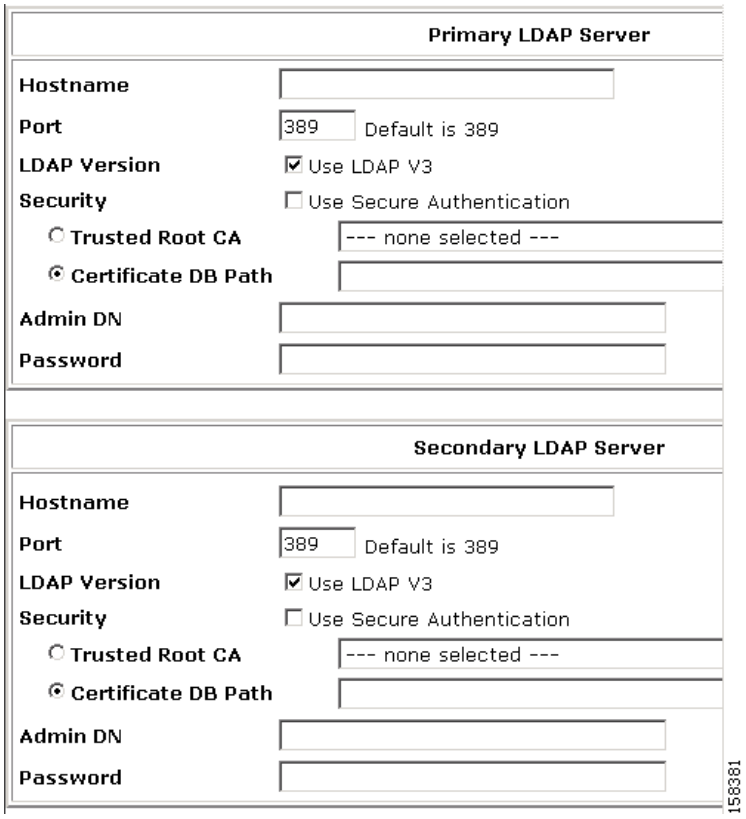
  – **Server Timeout**—The number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server failed.

- **On Timeout Use Secondary**—Determines whether ACS performs failover of LDAP authentication attempts.
- **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.

Specify LDAP server configuration information:

Figure 4-7 shows the Primary LDAP Server and Secondary LDAP Server configuration sections.

Figure 4-7 LDAP Server Configuration Sections



a. For the primary LDAP server specify:

- **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 the default.
- **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 unchecked, 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 ensure 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:** For ACS for Windows, this is the path to the Netscape *cert7.db* file For the ACS Solution Engine, this option provides a link to the Download Certificate Database page.

  For detailed information on this field, refer to the "LDAP Configuration Options" section in Chapter 12 of the *User Guide for Cisco Secure Access Control Server*, "User Databases."

- **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 whom LDAP authenticates.

- **Password**—The password for the administrator account that you specified in the Admin DN box. The LDAP server determines case sensitivity.

b. If you want to set up LDAP server failback, then in the Secondary LDAP server section, specify information to identify the failback LDAP server.

The options and text input boxes in the Secondary LDAP Server section are the same as the ones in the Primary LDAP Server section.

Step 9 Click **Submit**.

Step 5: Configure User Groups for MAB Segments

During configuration of network access profiles (NAPs) to enable agentless request processing, you will be required to map devices that have specified MAC addresses to one of the default user groups that ACS provides.

Before you assign the user groups, plan how to configure the user groups. For example, users associated with the user group can:

- Be denied access to the network
- Be limited by network access restrictions (NARs)
- Have specified password settings

For detailed information on how to set up user groups, refer to chapter 5 of the *User Guide for Cisco Secure ACS 4.1*, "User Group Management."

Step 6: Enable Agentless Request Processing

To enable agentless request processing, you must set up a network access profile (NAP) that enables the feature. To create a NAP to enable agentless request processing:

Step 1 Create a new NAP.

See Create a New NAP, page 4-17 for details.

Step 2 In the Protocols page, check the **Allow Agentless Request Processing** check box.

Step 3 In the Authentication section, configure MAB.

See Configure MAB, page 4-20 for details.

Step 4 If you are using agentless request processing in a NAC environment, configure posture validation for the NAP.

See Enable Agentless Request Processing for a NAP, page 4-19 for details.

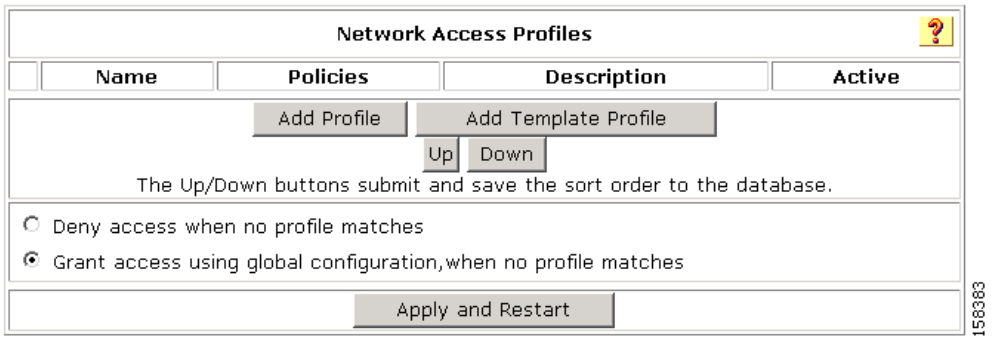
Create a New NAP

To create a new NAP:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens, as shown in Figure 4-8.

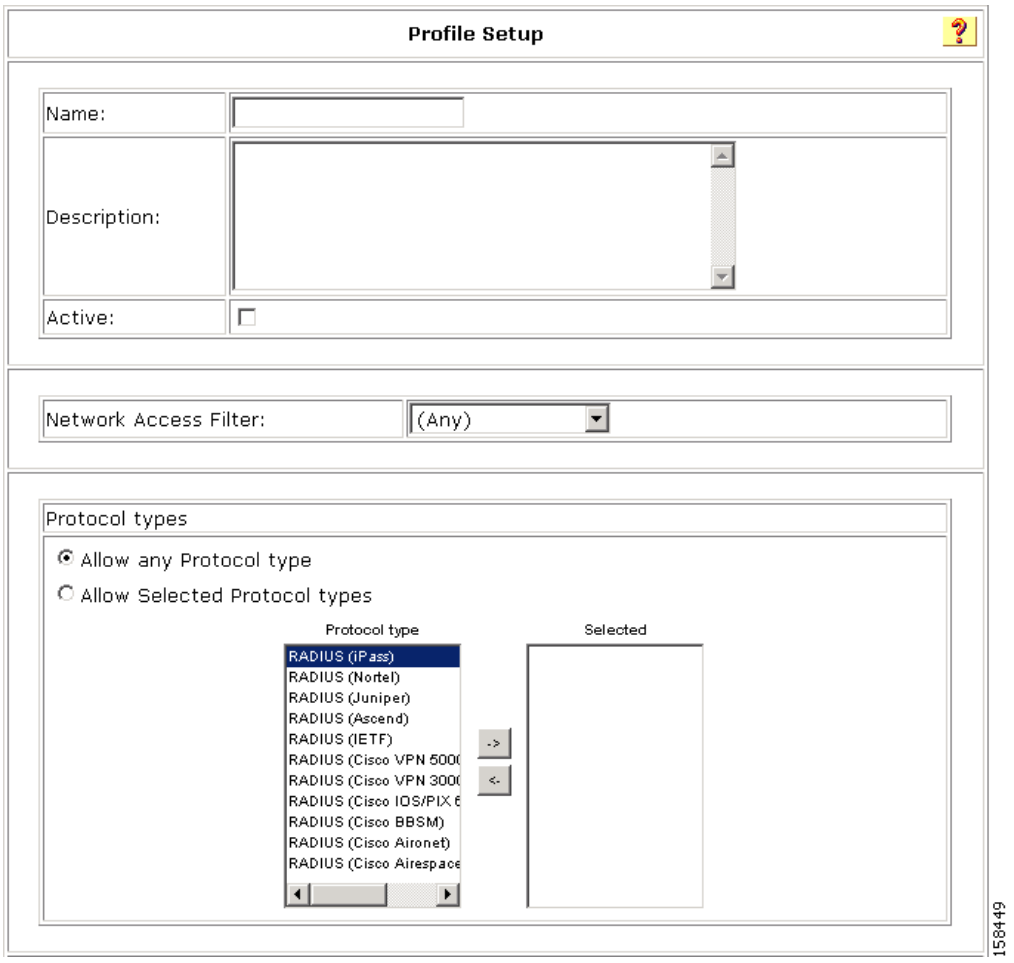
Figure 4-8 Network Access Profiles Page



Step 2 Click **Add Profile**,

The Profile Setup page opens, shown in Figure 4-9.

Figure 4-9 Profile Setup Page



Step 3 In the Name text box, enter the name of the NAP.

Step 4 If you have set up network access filters (NAFs) and want to apply one, then from the drop-down list of NAFs, choose the appropriate NAF.

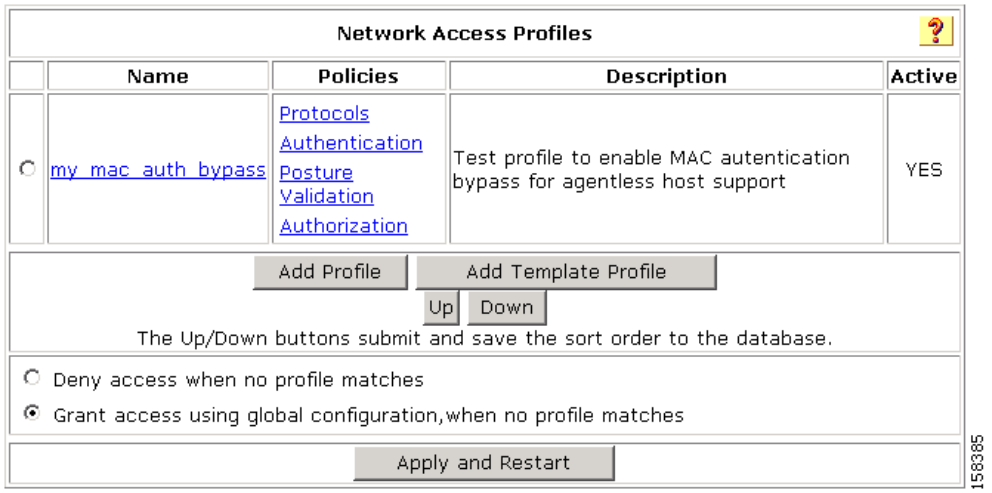
Step 5 In the Protocol types section, select at least one RADIUS protocol type.

Step 6 Configure additional NAP settings as required.

Step 7 Click **Submit**.

The Edit Network Access Protocols page for the new profile appears, as shown in Figure 4-10.

Figure 4-10 Edit Network Access Protocols Page



You are now ready to enable agentless request processing.

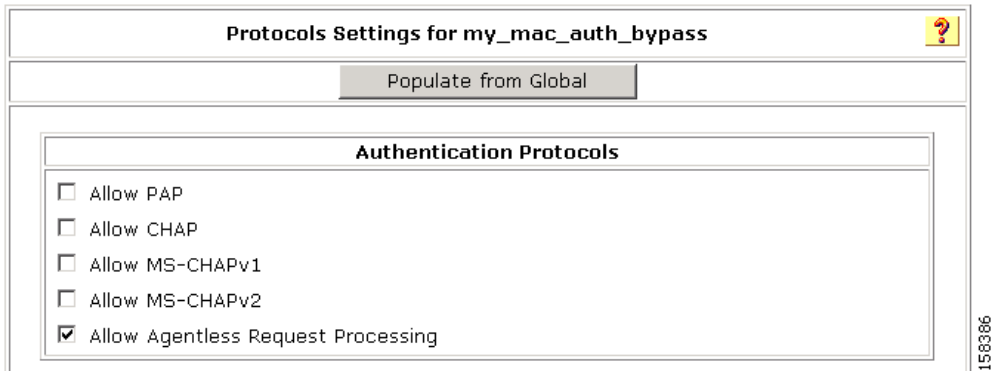
Enable Agentless Request Processing for a NAP

To enable agentless request processing for a NAP:

Step 1 In the Edit Network Access Profiles page, click **Protocols**.

The Protocols Settings page for the selected NAP opens. Figure 4-11 shows the top portion of the Protocols Settings page.

Figure 4-11 Protocols Settings Page



Step 2 Check the check box for A**llow Agentless Request Processing**.

Step 3 Configure additional protocol configuration options as required

Step 4 If you are using ACS in a NAC environment, check the **Allow Posture Validation** check box in the EAP Configuration area.

Step 5 Click **Submit**.

You are now ready to configure MAB settings.

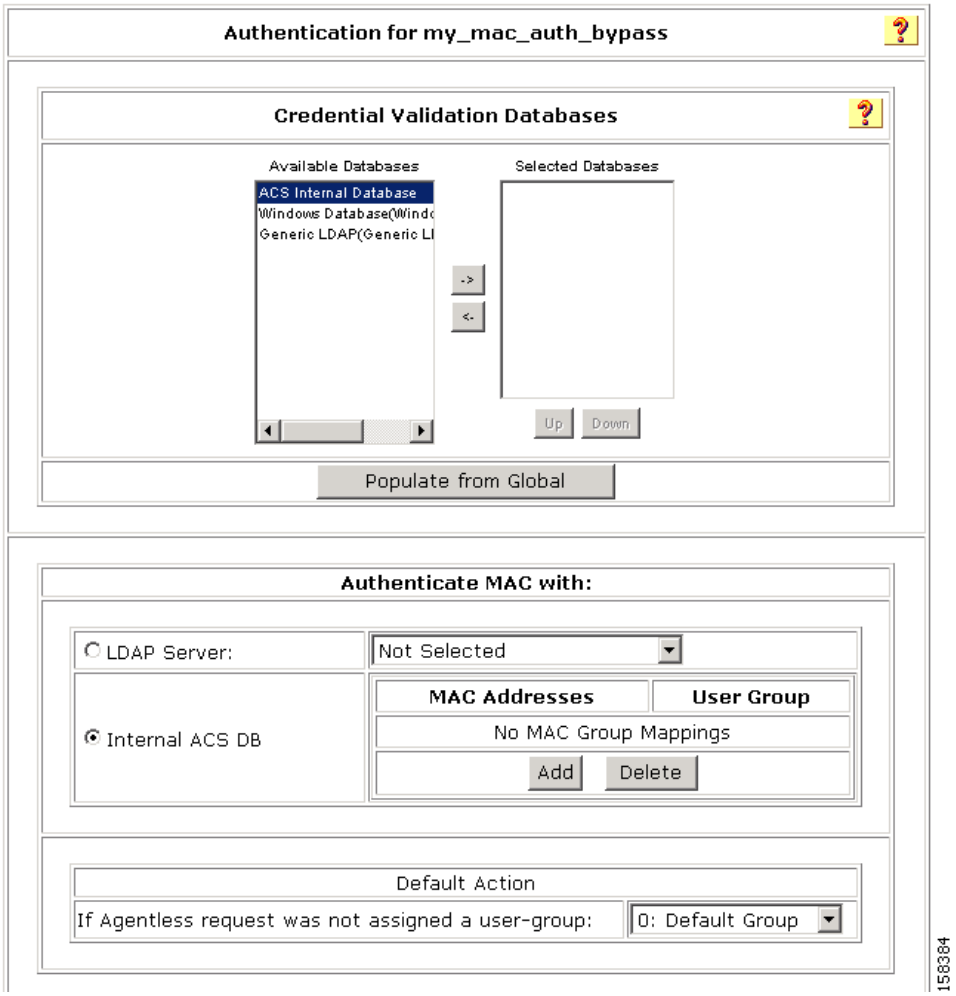
Configure MAB

To configure MAB:

Step 1 In the Edit Network Access Profiles page, click **Authentication**.

The Authentication page for the selected NAP opens. Figure 4-12 shows the Authentication Settings page.

Figure 4-12 Authentication Settings Page



Step 2 In the Credential Validation Databases section, choose the database(s) that ACS will use to authenticate agentless hosts.

Note If you clicked **Generic LDAP** or another LDAP database, choose **External User Databases** > **External User Database Configuration** and configure an LDAP database.

Step 3 If you specified an LDAP database in the Credential Validation Databases section, click **LDAP Server** and then select a LDAP database that you configured on the **External User Databases > External User Database Configuration** page.

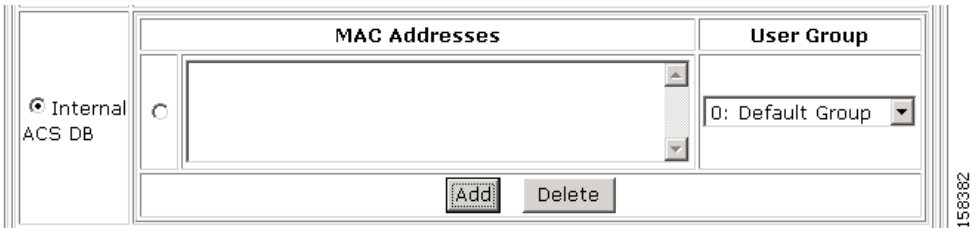
Step 4 If you will validate MAC addresses by using the ACS internal database:

a. Click **Internal ACS DB**.

b. Click **Add**.

A text box for entering MAC addresses and associated user group mappings appears, as shown in Figure 4-13.

Figure 4-13 MAC Address Input Area



c. In the MAC addresses input area, enter one or more MAC addresses to use in authenticating agentless hosts.

You can enter the MAC address in the following 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*.

d. From the drop-down list of user groups in the User Group area, choose a user group to which devices having one of the specified MAC address are mapped.

e. To add additional groups of MAC addresses, click **Add** and enter additional groups and associated user groups as required.

Step 5 In the Default Action (If Agentless request was not assigned to a user group) area, from the drop-down list of user groups, choose a group to which to assign the MAC addresses if the MAC addresses are not found in the LDAP Server or the ACS Internal Database; or, if the LDAP Server is not reachable.

Step 6 If you enabled the EAP protocol and posture validation, set up posture validation rules in the Posture Validation section.

Step 7 As required, specify additional authorization rules in the Authorization section.

Step 8 Click **Submit**.

Step 7: Configure Logging and Reports

By default, the following information about MAB processing is logged to the *CSAuth* log file:

- The start of MAB request handling and what trigger is used to initiate MAB.

  The format of this message is:

  `Performing Mac Authentication Bypass on <MAC_address>`

  where *MAC_address* is the MAC address that triggered the processing.

- User group mapping actions that indicate which MAC address in the authentication database was mapped to what user group. The format of this message is:

  `<MAC_address> was (not) found in <DB_name> and mapped to <user_group> user-group`

  where *MAC_address* is the MAC address that was mapped, *DB_name* is the name of the database that was used to match the MAC_address, and *user_group* is the name of the user group to which the MAC address was mapped.

Note Because the results of MAC address lookup can influence the response that ACS returns to the NAD, the success or failure of the MAC address lookup has an effect on the user group that is mapped to an access request. Therefore, the MAC address lookup result might be listed in the Passed Authentications or Failed attempts report.

Configuring Reports for MAB Processing

When you configure reports, you can add a new attribute called `Bypass info` to the Passed Authentications and Failed Attempts reports.

To add this attribute:

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

The System Configuration page opens.

Step 2 Click **Logging**.

The Logging Configuration page opens.

The Logging Configuration page shows three columns of ACS reports: CSV, ODBC, and Syslog.

Step 3 To add the Bypass attribute to a specified report:

a. Click **Configure** under the report type for one of the reports that you want to modify; for example, click the CSV report for the Passed Authentications report.

The Enable Logging page for the specified report opens.

b. Check the check box in the Enable Logging section.

c. In the Attributes column of the Select Columns to Log section, select the **Bypass Info** attribute.

d. Click the right arrow icon to move this attributed to the Logged Attributes column.

e. Select any other attributes that you want to log.

f. Set the other values on the Logging Configuration page as required.

g. Click **Submit**.

Step 4 Repeat Step 3 for additional report types as required.

Step 5 Repeat Steps 3 and 4 for the Failed Attempts report.

Configuration Steps for Audit Server Support

If you are using ACS with the NAC solution or with other applications that support the use of audit servers, you can set up agentless host support that uses an audit server.

An audit server runs a database that can enable further authentication of the information that is used to assign agentless host devices to user groups. For example, the categorization of devices in the LDAP schema might set up device categories such as *printer*, *PC*, or *FAX machine*. The database on the audit server can check whether a device with a specified MAC address or IP address is the type of device associated in the database with the specified MAC address or IP address. If it is not the correct device type, a specified authentication policy can be executed.

The mechanism that ACS 4.1 uses to communicate with audit servers in a NAC environment is called GAME group feedback. The GAME protocol defines the GAME groups. When you configure GAME group feedback for an audit server that is used in a NAP, you can enable the Request Device Type from Audit Server feature. If this feature is 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.

Configure GAME Group Feedback

To configure GAME group feedback:

Step 1 Import an audit vendor file by using **CSUtil**.

Step 2 Import a device-type attribute file by using **CSUtil**.

Step 3 Import NAC attribute-value pairs.

Step 4 Enable Posture Validation.

Step 5 In the External Posture Validation Audit Server Setup page, configure an external audit server.

Step 6 Enable GAME group feedback.

Step 7 In the external audit server posture validation setup section, configure:

- Which hosts are audited section.
- GAME group feedback.
- Device-type retrieval and mapping for vendors who have a device attribute in the RADIUS dictionary.

Step 8 Set up a device group policy.

The detailed steps for configuring GAME group feedback are described in Enable GAME Group Feedback, page 7-68 in Chapter 7, “NAC Configuration Scenario”

CHAPTER 5

PEAP/EAP-TLS Configuration Scenario

You can now select EAP-TLS as an inner method that is used within the tunnel that ACS establishes for PEAP authentication. If you select EAP-TLS, ACS can use it not only to encrypt the initial data sent through the PEAP protocol; but, once a secure tunnel is established between ACS and the NAD, to encrypt (for a second time) the data that is transmitted within the secure tunnel.

This enhanced encryption method greatly enhances the security of communications between ACS and the NAD.

Most customers who will use this feature are customers who use Microsoft supplicants.

Summary of Configuration Steps

To configure PEAP-TLS:

Step 1 Configure security certificates.

See Step 1: Configure Security Certificates, page 5-1 for details.

Step 2 Configure global authentication settings.

See Step 2: Configure Global Authentication Settings, page 5-5 for details.

Step 3 Specify EAP-TLS options.

See Step 3: Specify EAP-TLS Options, page 5-6 for details.

The following sections provide more details about the previous steps.

Step 1: Configure Security Certificates

This section describes a simplified procedure for the ACS for Windows platform. For detailed information on installing certificates and for information on how to install certificates on the Cisco Secure ACS Solution Engine platform, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.1*, "Advanced Configuration: Authentication and Certificates."

Obtain Certificates and Copy Them to the ACS Host

To use EAP-TLS, you must obtain and install security certificates.

To copy a certificate to the ACS host:

Step 1 Obtain a security certificate.

Step 2 Create a *\Certs* directory on the ACS server.

a. Open a DOS command window.

b. To create a certificates directory, enter:

`mkdir <`*`selected_drive`***`>:\Certs`**

where *`selected_drive`* is the currently selected drive.

Step 3 Copy the following files to the *\Certs* directory:

- *server.cer* (server certificate)
- *server.pvk* (server certificate private key)
- *ca.cer* (CA certificate)

Run the Windows Certificate Import Wizard to Install the Certificate

To run the Windows Certificate Import wizard to install the certificate on the server:

Step 1 Start Windows Explorer.

Step 2 Go to <*selected_drive*>:*Certs*.

where *`selected_drive`* is the currently selected drive.

Step 3 Double-click the *\Certs\ca.cer* file.

The Certificate dialog appears.

Step 4 Select **Install Certificate.**

The Windows Certificate Import wizard starts.

Step 5 To install the certificate, follow the instructions that the wizard displays.

Step 6 Accept the default options for the wizard.

Note Only perform this process once on a Windows 2000 Server.

Enable Security Certificates on the ACS Installation

To enable security certificates:

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

The System Configuration page opens.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

Step 4 The Install ACS Certificate page opens, shown in Figure 5-1.

Figure 5-1 Install ACS Certificate Page

Step 5 Ensure that you click the **Read certificate from file** radio button.

Step 6 In the Certificate file text box, enter the server certificate location (path and name); for example ***c:\Certs\server.cer***.

Step 7 In the Private Key File text box, type the server certificate private key location (path and name); for example: ***c:\Certs\server.pvk***.

Step 8 In the Private Key password text box, type **1111**.

Step 9 Click **Submit.**

Step 10 ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.

Step 11 Do not restart the services at this time.

Restart the services later, after you have completed the steps for adding a trusted certificate. See Add a Trusted Certificate, page 5-4.

Install the CA Certificate

To install the CA Certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

Step 2 The ACS Certification Authority Setup page appears, shown in Figure 5-2.

Figure 5-2 ACS Certification Authority Setup Page

Step 3 In the CA certificate file box, type the CA certificate location (path and name). For example: *c:\Certs\ca.cer*.

Step 4 Click **Submit**.

Add a Trusted Certificate

After you add a server certificate and set up the certificate authority, install a trusted certificate.

To add a trusted certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > Edit Certificate Trust List**.

The Edit Certificate Trust List appears.

Step 2 Locate the trusted certificate that you want to install and check the check box next to the certificate name.

For example, find the **Stress** certificate and check the check box next to it.

Step 3 Click **Submit**.

Step 4 To restart ACS, choose **System Configuration > Service Control**, and then click and then click **Restart**.

Step 2: Configure Global Authentication Settings

To configure global authentication settings:

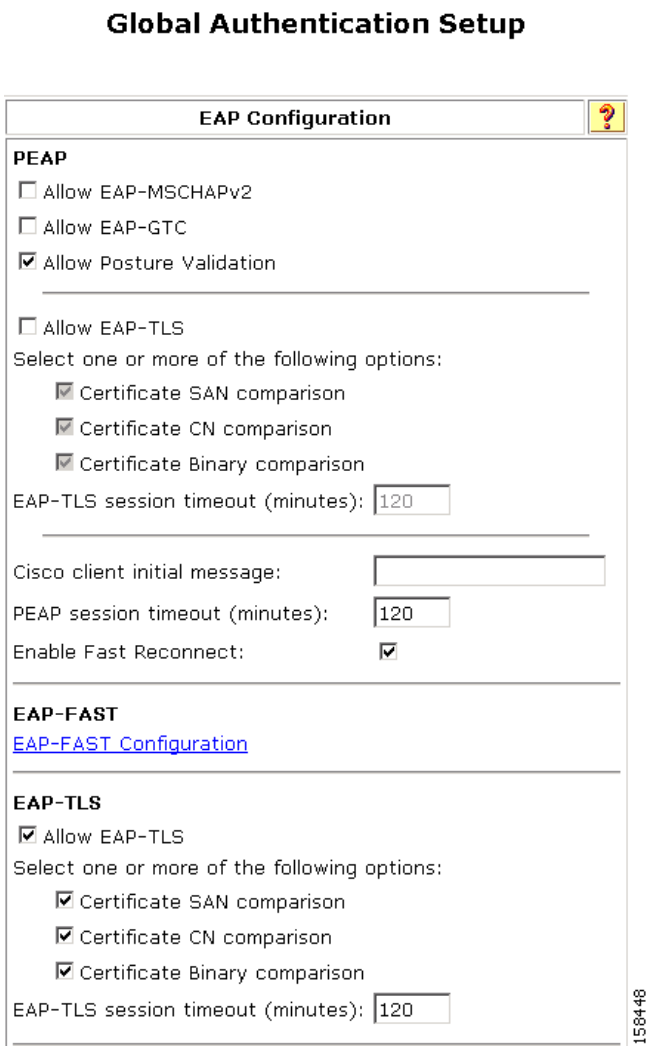
Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Global Authentication Setup**.

The Global Authentication Setup page opens, as shown in Figure 5-3.

Figure 5-3 Global Authentication Setup Page



Step 3 Specify the protocols to use with the PEAP protocol. They are:

- EAP_MSCHAP2
- EAP-GTC

Step 4 If you want to enable posture validation on this ACS installation, check the **Enable Posture Validation** check box.

Step 3: Specify EAP-TLS Options

Specify one or more of the certificate comparison options for EAP-TLS:

- **Certificate SAN Comparison**—Based on the name in the Subject Alternative Name (SAN) field in the user certificate.
- **Certificate CN Comparison**—Based on the name in the Subject Common Name (CN) 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. You cannot use this comparison method to authenticate users in an ODBC external user database.

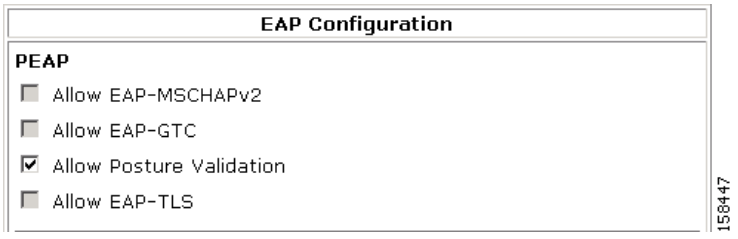
Step 4: (Optional) Configure Authentication Policy

The authentication policy that is available with PEAP has changed slightly with ACS 4.1.

You can now enable EAP-TLS when you set up an authentication policy in the protocols section of network access profile configuration.

Figure 5-4 shows the modified EAP configuration section on the NAP Protocols page.

Figure 5-4 EAP Configuration Section of NAP Protocols Page



CHAPTER 6

Syslog Logging Configuration Scenario

Overview

ACS 4.1 provides a new system logging (syslog) feature. With the addition of this feature, all AAA reports and audit report messages can be sent to up to two syslog servers.

Configuring Syslog Logging

To configure ACS to generate syslog messages:

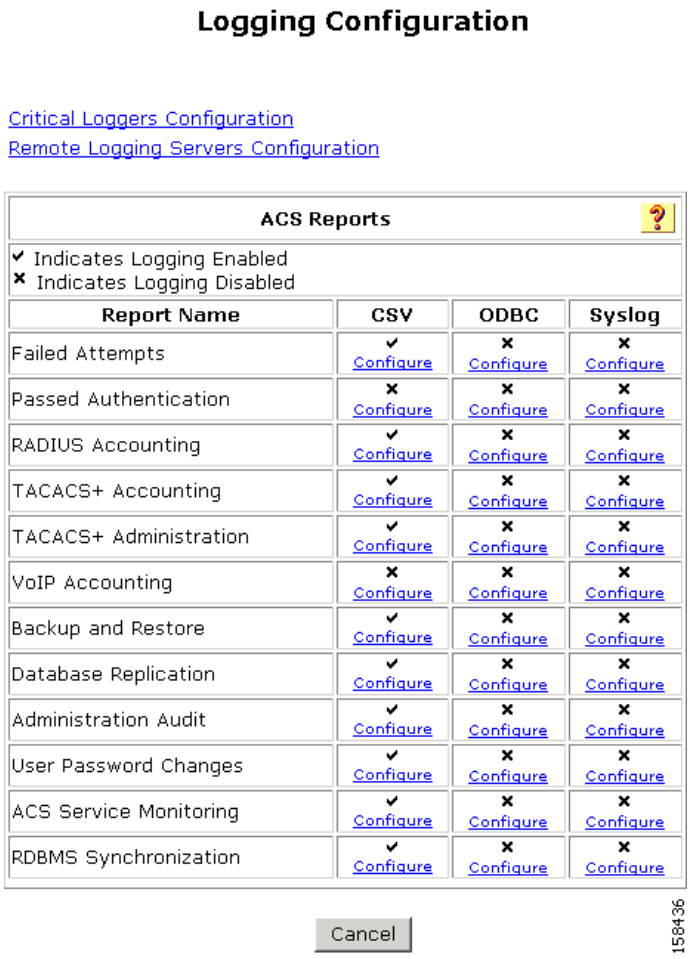
Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Logging.**

The Logging page opens, shown in Figure 6-1.

Figure 6-1 Logging Configuration Page



Logging Configuration

Critical Loggers Configuration
Remote Logging Servers Configuration

ACS Reports

✔ Indicates Logging Enabled
✖ Indicates Logging Disabled

Report Name	CSV	ODBC	Syslog
Failed Attempts	✔ Configure	✖ Configure	✖ Configure
Passed Authentication	✖ Configure	✖ Configure	✖ Configure
RADIUS Accounting	✔ Configure	✖ Configure	✖ Configure
TACACS+ Accounting	✔ Configure	✖ Configure	✖ Configure
TACACS+ Administration	✔ Configure	✖ Configure	✖ Configure
VoIP Accounting	✖ Configure	✖ Configure	✖ Configure
Backup and Restore	✔ Configure	✖ Configure	✖ Configure
Database Replication	✔ Configure	✖ Configure	✖ Configure
Administration Audit	✔ Configure	✖ Configure	✖ Configure
User Password Changes	✔ Configure	✖ Configure	✖ Configure
ACS Service Monitoring	✔ Configure	✖ Configure	✖ Configure
RDBMS Synchronization	✔ Configure	✖ Configure	✖ Configure

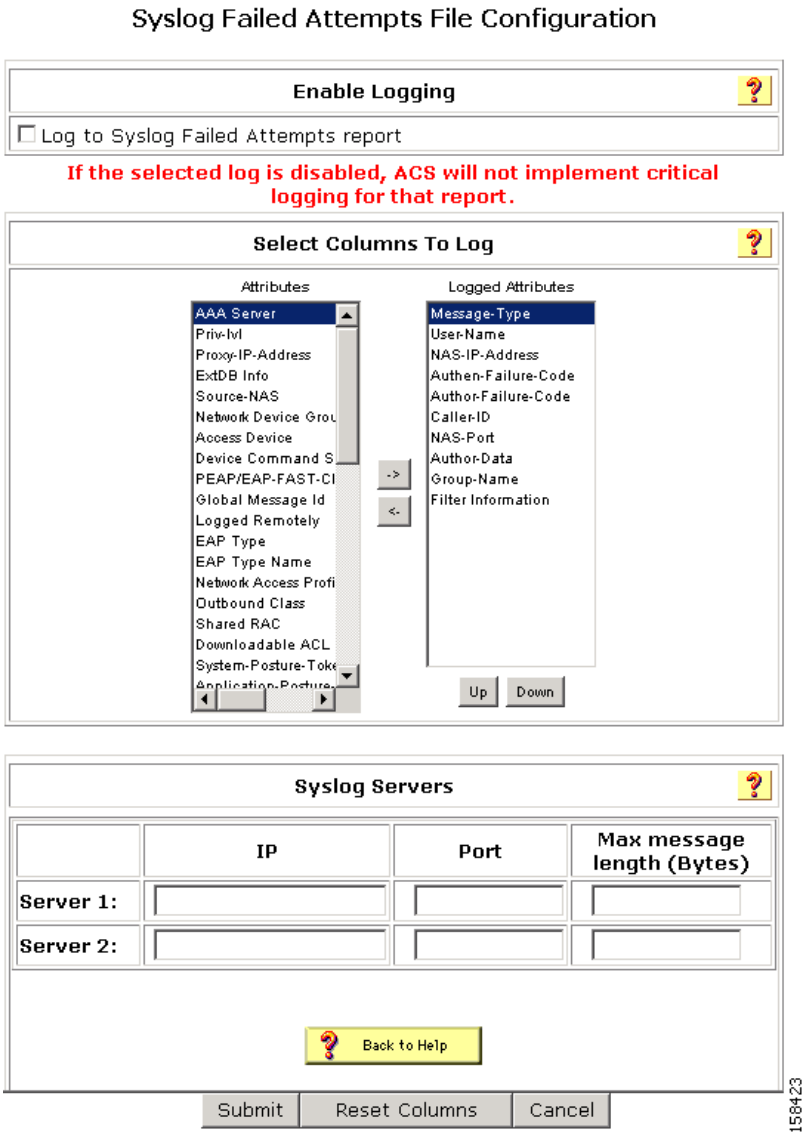
Cancel

158436

Step 3 To enable a syslog report, on the Logging Configuration page, click the **Configure** link in the Syslog column, in the row for each report that you want to generate.

The Enable Login window for the specified report opens, as shown in Figure 6-2.

Figure 6-2 Enable Logging Page



Step 4 Check the check box for logging the specified information to syslog.

For example, in Figure 6-2, check the **Log to Syslog Failed Attempts Report** check box.

In the Select Columns to Log section, a list of the fields available for the specified syslog report appears.

Step 5 To move an attribute to the list of the attributes shown in the report, select the field in the Available column and then click the right arrow icon to move it to the Logged Attributes column.

In the Syslog Servers section, specify the following information for the syslog servers to which ACS will send logging information:

- **IP**—Enter the IP address of the syslog server.
- **Port**—Enter the syslog port number on the specified server.
- **Max message length (Bytes)**—Enter the maximum syslog message length that ACS will accept.

  You can enter information for up to two syslog servers.

Step 6 Click **Submit**.

Step 7 Repeat the process for any additional reports for which you want to enable syslog reporting.

Format of Syslog Messages in ACS Reports

Syslog messages included in ACS reports have the following format:

```
<n> mmm dd hh:mm:ss XX:XX:XX:XX TAG  msg_id total_seg seg# A1=V1
```

The elements of the message are:

- *n*—The Priority value of the message; it is a combination of facility and severity of the syslog message, which is calculated according to RFC 3164, by first multiplying the *facility* value by 8 and then adding the *severity* value.
- *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*—One of the following values, depending on the application 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—ACS backup and restore log messages.
  - CisACS_12_Replication—ACS database replication log messages.
  - CisACS_13_AdminAudit—ACS administration audit log messages.
  - CisACS_14_PassChanges—ACS user password changes log messages.
  - CisACS_15_ServiceMon—ACS service monitoring log messages.
  - CisACS_16_RDBMSSync—ACS RDBMS Synchronization Audit log messages.
  - CisACS_17_ApplAdmin—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.
- *seg#* -Segment sequence number within this message segmentation.
- *A1*=*V1*—Attribute-value pairs delimited by a comma (,) for Cisco ACS log messages and the message itself.

Facility Codes

ACS syslog messages use the following facility values:

- **4**—Security and authorization messages. This value is used for all AAA related messages (failed attempts, passed attempts, accounting, and so on).

- **13**—Log audit. This value is used for all other ACS report messages.

All ACS syslog messages use a severity value of 6 (informational).

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.

The following sample syslog message shows how the facility code and other information might look in an ACS-generated syslog message:

```
<110> Oct 16 08:58:07 64.103.114.149 CisACS_13_AdminAudit  18729fp11 1 0 AAA
Server=tfurman-w2k,admin-username=local_login,browser-ip=127.0.0.1,text-message=Administra
tion session finished,
```

In this example, <110 >represents the calculated value when the facility code is 13 (the log audit facility code).

Message Length Restrictions

When an ACS message exceeds the syslog standard length limitation or target length limitation, the message content is split into several segments:

- If all attribute-value elements fit into one segment then no segmentation is performed.
- If the message does not fit into one segment, the message is split between attribute-value pairs, keeping an attribute-value pair complete within the segment. That is, the first segment ends with a semicolon (;), while the next segment's content starts with the next attribute-value pair.
- In rare cases when one attribute-value pair is too long to fit in one segment all by itself, the value is segmented between sequenced segments of the message. Such segmentation might happen if attribute value contains several hundreds of characters. In general, ACS attribute values are designed to avoid such length.

All segments of one message have exactly the same header. The **<**msg_id**>** and **<**total_seg**>** values are shared between all segments. The **<**seg**#>** is set according to number of segments and the relative part of the content follows.

Use the following message length restrictions:

- For sending messages to a standard syslog server, the maximum message length should be 1024 bytes.
- For sending messages to Cisco Security Monitoring, Analysis and Response System (MARS), the maximum message length should be 500 bytes.
- Message segmentation should be used when the original message, including header and data, exceeds length limitations.

CHAPTER 7

NAC Configuration Scenario

This chapter describes how to set up Cisco Secure Access Control Server 4.1, hereafter referred to as ACS, to work in a Cisco Network Admission Control (NAC) environment. This chapter contains the following sections:

Step 1: Install ACS

This section describes the installation process that you perform to run ACS, which runs on a Windows 2000 Server, Windows 2003, or on a Cisco Secure ACS Solution Engine (ACS SE).

For detailed information on ACS installation, refer to the:

- *Installation Guide for Cisco Secure ACS for Windows Release 4.1*
- *Installation Guide for Cisco Secure ACS Solution Engine Release 4.1*

To install ACS:

Step 1 Start the ACS installation.

During the installation process, you are prompted to enter a password for encrypting the internal database.

Step 2 Enter a password that is at least 8 characters long, and contains letters and numbers.

The ACS installation process for ACS for Windows automatically creates a shortcut to the ACS administrative GUI on your desktop.

Note If you are installing ACS on the ACS SE, you must manually create an administrative GUI user by using the **add-guiadmin** command from the CLI to create a GUI account. For information on this command, see Appendix A of the *Installation Guide for Cisco Secure ACS Solution Engine 4.1*, "Command Reference." You can then access the administrative GUI through a supported browser. For a list of supported browsers, see *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Release 4.1*, which is available at:

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

Step 3 Double-click the icon to open a browser window to the ACS administrative GUI.

Step 4 If you do not see the icon on the desktop, open your browser from the machine on which you installed ACS and go to one of these addresses:

- http://*IP_address*:2002
- http://*hostname*:2002

where *IP_address* is the IP address of the host that is running ACS and hostname is the *hostname* of the host that is running ACS.

Step 2: Configure a RADIUS AAA Client

Before you can configure agentless host support, you must configure a RADIUS AAA client.

To configure a RADIUS AAA client:

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

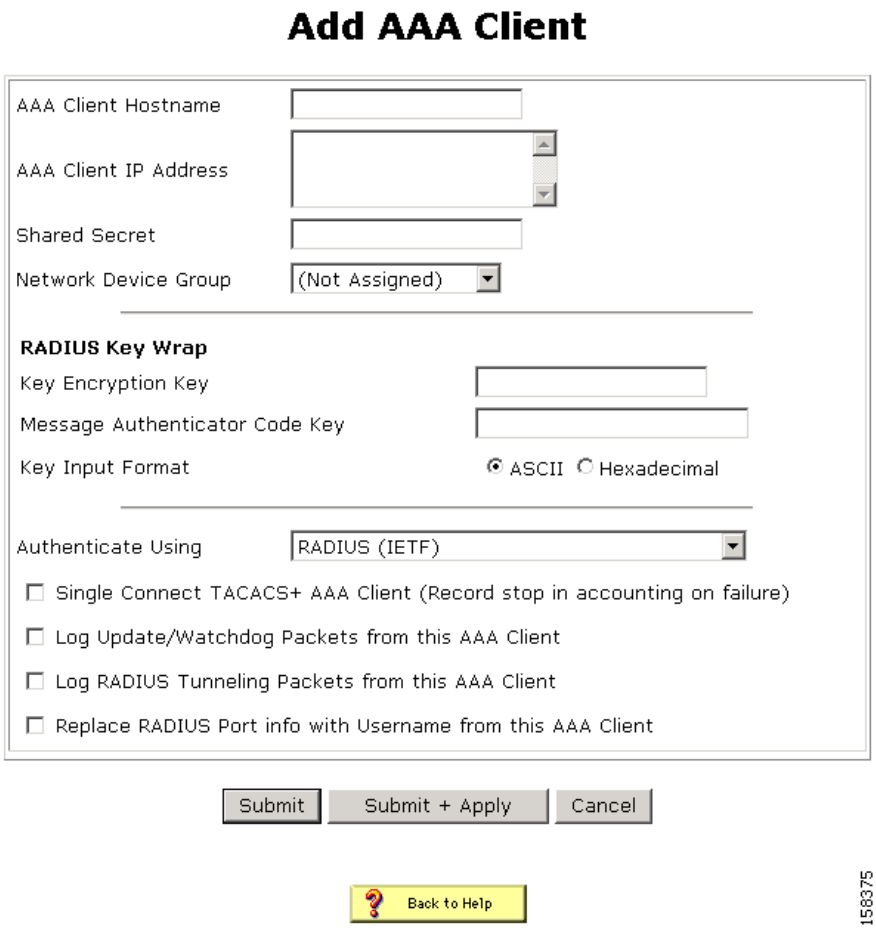
The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using Network Device Groups (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 opens, shown in Figure 7-1.

Figure 7-1 Add AAA Client Page



Step 3 In the AAA Client Hostname box, type the name assigned to this AAA client (up to 32 alphanumeric characters).

Step 4 In the AAA Client IP Address box, type the AAA client IP address or addresses.

Step 5 In the Shared Secret box, type the shared secret key for the AAA client. The shared secret must be identical on the AAA client and ACS. Keys are case sensitive. If the shared secrets do not match, ACS discards all packets from the network device.

Step 6 If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or, select **Not Assigned** to set this AAA client to be independent of NDGs.

Step 7 Type the shared secret keys for RADIUS Key Wrap in EAP-TLS authentications.

Each key must be unique, and must also be distinct from the RADIUS shared key. You can configure these shared keys 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, ACS uses the AAA client key. You must enable the Key Wrap feature in the NAP Authentication Settings page to implement these shared keys in EAP-TLS authentication:

a. Key Encryption Key (KEK)—Used for encryption of the Pairwise Master Key (PMK). The maximum length is 20 characters.

b. Message Authenticator Code Key (MACK)—Used for the keyed hashed message authentication code (HMAC) calculation over the RADIUS message. The maximum length is 16 characters.

c. Key Input Format—Click the format of the key, ASCII or hexadecimal strings (the default is ASCII).

Step 8 From the Authenticate Using list, select **RADIUS (IOS/PIX)**.

Step 9 Specify additional AAA client settings as required.

Step 10 Click **Submit + Apply**.

Step 3: Configure the Logging Level

To set ACS to full logging capabilities:

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

The System Configuration page opens.

Step 2 Click **Service Control.**

Step 3 Under **Level of Detail,** click the **Full** radio button.

Step 4 Check the **Manage Directory** check box and choose how many days of logging to keep. (Select the number of days based on how much space you have on your hard drive: We recommend that you specify seven days.)

Step 5 Click **Restart** to restart ACS. (Wait until the browser's progress bar shows that the page has reloaded completely.)

Step 4: Install and Set Up an ACS Security Certificate

This section describes a simplified procedure for the ACS for Windows platform. For detailed information on installing certificates and for information on how to install certificates on the Cisco Secure ACS Solution Engine platform, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.1*, "Advanced Configuration: Authentication and Certificates."

Obtain Certificates and Copy Them to the ACS Host

To copy a certificate to the ACS host:

Step 1 Obtain a security certificate.

Step 2 Create a *\Certs* directory on the ACS server.

a. Open a DOS command window.

b. To create a certificates directory, enter:

```
mkdir <selected_drive>:\Certs
```

where *selected_drive* is the currently selected drive.

Step 3 Copy the following files to the *\Certs* directory:

- *server.cer* (server certificate)
- *server.pvk* (server certificate private key)
- *ca.cer* (CA certificate)

Run the Windows Certificate Import Wizard to Install the Certificate (ACS for Windows)

To run the Windows Certificate Import wizard to install the certificate on the server:

Step 1 Open Windows Explorer.

Step 2 Go to <*selected_drive*>:*Certs*.

Step 3 Double-click the *\Certs\ca.cer* file.

The Certificate dialog appears.

Step 4 Select **Install Certificate.**

The Windows Certificate Import wizard starts.

Step 5 To install the certificate, follow the instructions that the wizard displays.

Step 6 Accept the default options for the wizard.

Note Only perform this process once on a Windows 2000 Server.

Enable Security Certificates on the ACS Installation

To enable security certificates on the ACS installation:

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

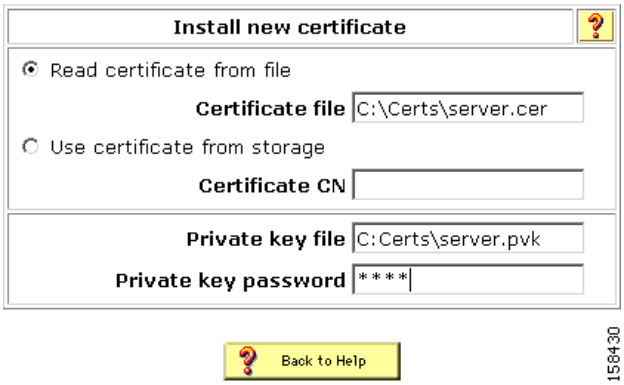
The System Configuration page opens.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

Step 4 The Install ACS Certificate page opens, as shown in Figure 7-2.

Figure 7-2 Install ACS Certificate Page



Step 5 Click the **Read certificate from file** radio button.

Step 6 In the Certificate file text box, enter the server certificate location (path and name); for example: `c:\Certs\server.cer`.

Step 7 In the Private key file text box, type the server certificate private key location (path and name); for example: *c:\Certs\server.pvk*.

Step 8 In the Private Key password text box, type **1111.**

Step 9 Click **Submit.**

Step 10 ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.

Step 11 Do not restart the services at this time.

Restart the services later, after you have completed the steps for adding a trusted certificate. See Add a Trusted Certificate, page 7-7.

Install the CA Certificate

To install the CA Certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

Step 2 The ACS Certification Authority Setup page appears, shown in Figure 7-3.

Figure 7-3 ACS Certification Authority Setup Page

Step 3 In the CA certificate file box, type the CA certificate location (path and name); for example: *c:\Certs\ca.cer*.

Step 4 Click **Submit**.

Add a Trusted Certificate

To add a trusted certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > Edit Certificate Trust List**.

The Edit Certificate Trust List appears.

Step 2 Locate the trusted certificate that you want to install and check the corresponding check box by the certificate name. For example, find the **Stress** certificate and check the corresponding check box.

Step 3 Click **Submit**.

Step 4 To restart ACS, choose **System Configuration > Service Control**, and then click **Restart**.

Step 5: Configure Remote Web Access

To prepare ACS for remote administration:

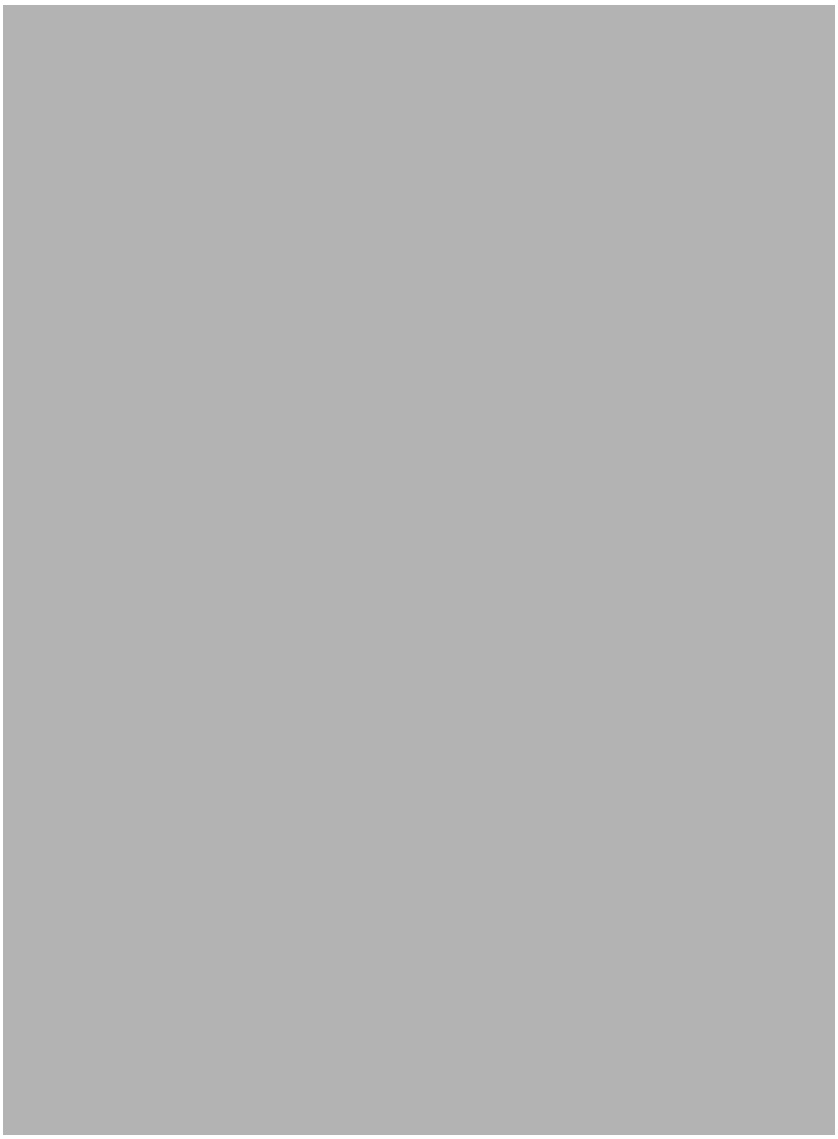
Step 1 In the navigation bar, click **Administration Control**.

The System Configuration page opens.

Step 2 Click **Add Administrator**.

The Administration Control page opens, as shown in Figure 7-4.

Figure 7-4 Administration Control Page



Step 3 To add an administrator, click **Add Administrator.**

The Add Administrator page opens.

Step 4 In the Administrator Details area:

Option	Description
Administrator Name	Enter the login name for the ACS administrator account. Administrator names can contain 1 to 32 characters, but cannot contain the left angle bracket (<), the right angle bracket (>), and the backslash (\). An ACS administrator name does not have to match a network user name.
Password	Enter the password for the administrator to access the ACS web interface. 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. Passwords must be at least 4 characters long and contain at least 1 numeric character. The password cannot include the username or the reverse username, must not match any of the previous 4 passwords, and must be in ASCII characters. If you make a password error, ACS displays the password criteria. 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.
Confirm Password	Reenter the password that you entered in the password field.
Account Never Expires	If you want to override the lockout options set up on the Administrator Password Policy page (with the exception of manual lockout), check the check box next to Account Never Expires. If you check this option, the account never expires, but the password change policy remains in effect. The default value is unchecked (disabled).
Account Locked	If you want to lock out an administrator who is denied access due to the account policy options specified on the Password Policy page, check the **Account Locked** check box. When unchecked (disabled), this option unlocks an administrator who was locked out. 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. 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. The reset of a locked account does not affect the configuration of the lockout and unlock mechanisms for failed attempts.

Step 5 Click **Grant All**.

This grants all privileges to the new administrator; or, specifies to which groups or actions this administrator is granted access.

Note For more information on administrative privileges, see the "Add Administrator and Edit Administrator Pages" section in Chapter 11 of the *User Guide for Cisco Secure Access Control Server 4.1*, "Administrators and Administrative Policy."

Step 6 Click **Submit**.

After performing these steps, from a remote host, you can open a browser in which to administer ACS.

The URLs for remote access are:

- http://*IP_address*:2002
- http://*hostname*:2002

Step 6: Enable Downloadable ACLs and Network Access Filters

To enable downloadable access control lists (dACLs) and Network Access Filters (NAFs), which are required to create Network Access Profiles (NAPs):

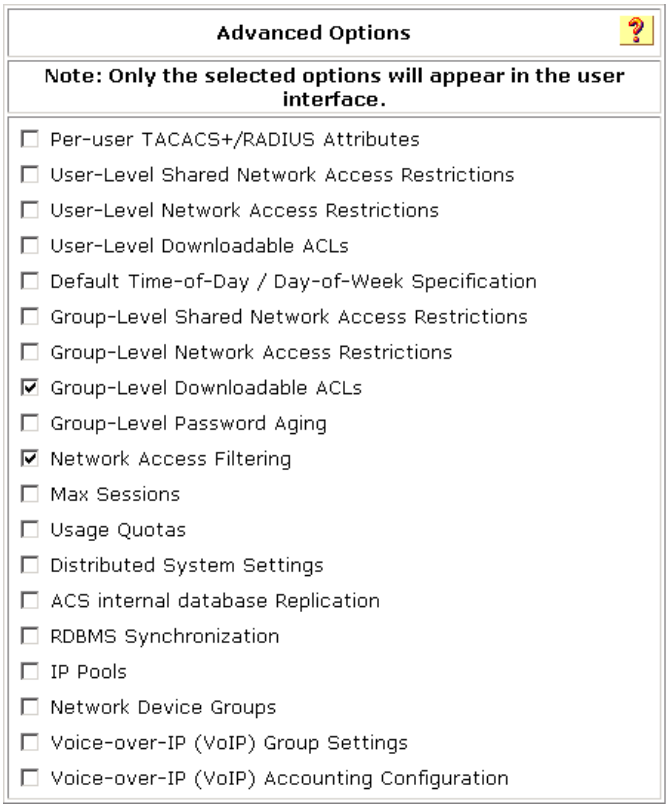
Step 1 In the navigation bar, click **Interface Configuration**.

The Interface Configuration page opens.

Step 2 Click **ACS Certificate Setup**.

The Advanced Options page appears, shown in Figure 7-5.

Figure 7-5 Advanced Options Required to Enable Network Access Profiles



Step 3 Check the check boxes for:

- **Group-Level Downloadable ACLs**
- **Network Access Filtering**

Step 4 Click **Submit**.

Step 7: Configure ACS for PEAP

To configure ACS so that PEAP will work properly with NAC posture validation:

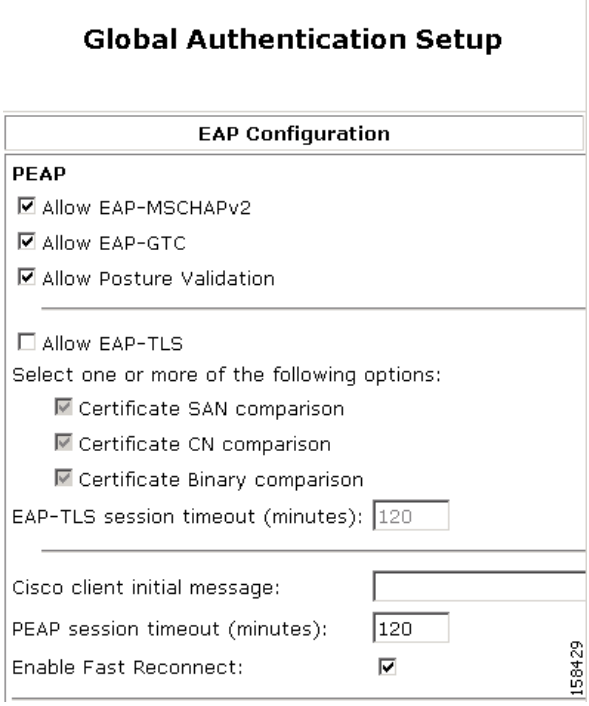
Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Global Authentication Setup**.

The Global Authentication Setup Page appears, as shown in Figure 7-6.

Figure 7-6 Global Authentication Setup Page



Step 3 Check the check box for **Allow EAP-MSCHAPv2** or **Allow EAP-GTC**; or, check both check boxes.

Step 4 In the PEAP section, check the **Allow Posture Validation** check box.

Step 5 Click **Submit + Restart**.

Step 8: Configure ACS for EAP-FAST

To configure ACS to work with NAC and use EAP-FAST will with posture validation:

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

The System Configuration page opens.

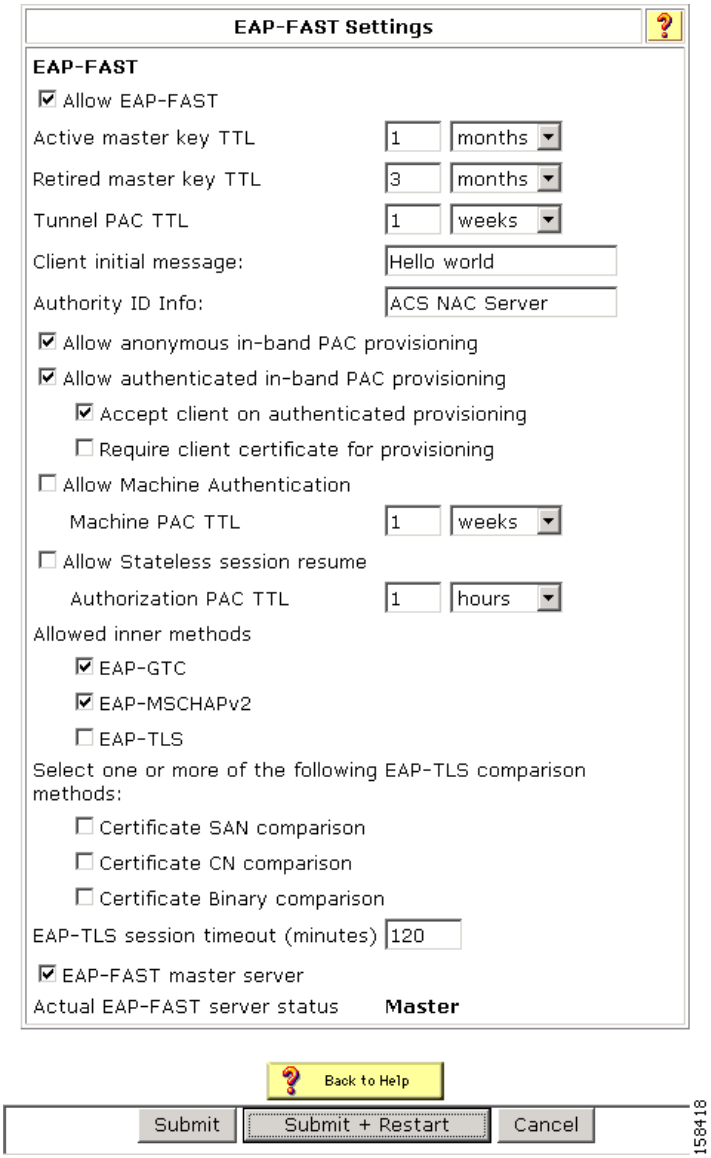
Step 2 Click **Global Authentication Setup**.

The Global Authentication Setup Page appears, as shown in Figure 7-6.

Step 3 Click **EAP-FAST Configuration**.

The EAP FAST Configuration page appears, as shown in Figure 7-7.

Figure 7-7 EAP-FAST Configuration Page



Step 4 Check the **Allow EAP-FAST** check box.

Step 5 In the Client Initial Message text box, enter a message, for example, *Welcome*.

Step 6 In the Authority ID Info field, enter *ACS NAC Server.*

Step 7 Check the **Allow authenticated in-band PAC provisioning** check box.

Step 8 Check the **Accept client on authenticated provisioning** check box.

Step 9 Check the check boxes for the **EAP-GTC** and **EAP-MSCHAPv2** inner methods.

The **EAP-FAST Master Server** check box is automatically checked (enabled).

Step 10 Click **Submit + Restart**.

Step 9: Configure Network Access Filtering

To use ACS in a NAC environment, configure network access filtering (NAF).

NAF is an ACS feature that groups several devices into one group. The devices can be ACS clients, ACS servers, ACS network device groups (NDGs), or a specific IP address. NAFs are particularly useful for defining Network Access Profiles (NAPs).

To configure ACS to use NAFs:

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

The Interface Configuration page opens.

Step 2 Click **Advanced Options**.

Step 3 Check the **Network Access Filtering** check box.

Click **Submit**.

Step 4 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page opens.

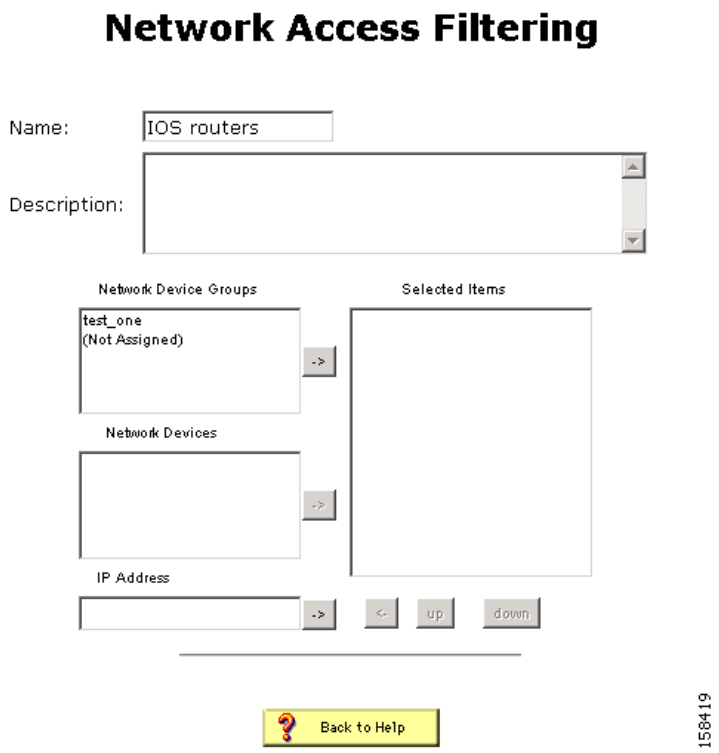
Step 5 Click **Network Access Filtering**.

The Network Access Filtering table appears. Initially, this table does not contain shared profile components.

Step 6 Click **Add**.

The Edit Network Access Filtering page opens, as shown in Figure 7-8.

Figure 7-8 Edit Network Access Filtering Page



Step 7 In the Name text box, enter a name for the network access filter.

Step 8 Move any devices or device groups to the Selected Items list.

To move a device or device group, select the item to move and then click the right arrow button to move it to the Selected Items list.

Step 9 Click **Submit**.

Step 10: Configure Logs and Reports

ACS logs records of users who gain network access or are refused network access. The ACS reports summarize these logs, and provide useful information for debugging and tracking problems.

The Passed Authentications report is particularly useful in NAC-enabled networks; because, it shows the group mapping for each posture validation request. By default, the Passed Authentication report is unchecked (disabled).

To enable the Passed Authentication report:

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

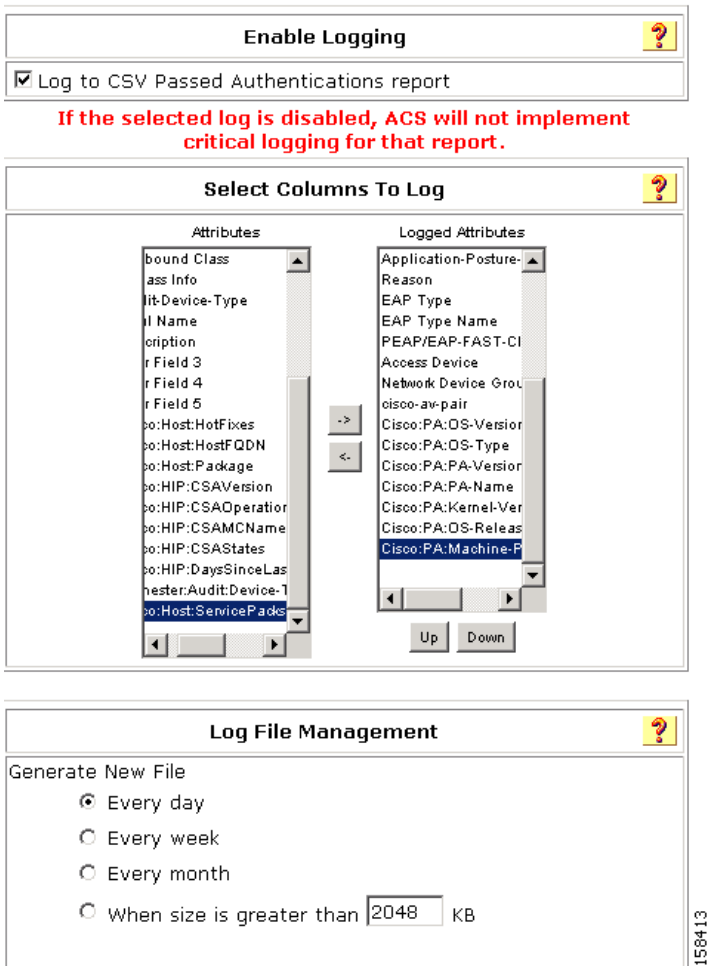
The System Configuration page opens.

Step 2 Click **Logging**.

The Logging Configuration page opens.

Step 3 In the ACS Reports table, click the **Configure** link for the CSV Passed Authentications report. The CSV Passed Authentications File Configuration page opens, as shown in Figure 7-9.

Figure 7-9 CSV Passed Authentications File Configuration Page



Step 4 Check the **Log to CSV Passed Authentications Report** check box.

Step 5 Move the attributes that you want to log from the **Attributes** list to **Logged Attributes** list.

Some useful attributes to log are:

- cisco-av-pair attributes starting with `PA` and `A`
- Profile Name
- Reason
- System-posture-token
- Application-posture-token

Step 6 Click **Submit.**

Step 11: Set Up Network Access Profiles

A NAP, also known as a *profile*, is a way to classify access requests according to the AAA clients' IP addresses, membership in a network device group, protocol types, or other specific RADIUS attribute values sent by the network device through which the user connects.

If you configure NAPs, ACS traverses the ordered list of active profiles, and maps a RADIUS transaction to a profile by using a first-match strategy on the first access-request of the transaction.

After you set up a profile, you associate a set of rules or policies with it, to reflect your organization's security policies. These associations are called profile-based policies. Configuring a profile-based policy includes creating rules for:

- Protocols
- Authentication
- Posture validation
- Authorization

A profile is a classification of network access requests for applying a common policy.

You can create a profile in two ways:

- Manually, by selecting options in the NAP configuration pages.
- By using the sample NAC templates provided with ACS 4.1 to start a profile and then editing the profile as required for your installation.

When you set up a NAP, you can configure:

- Profile name
- Description
- The Active flag, which determines whether this profile is active or inactive
- Classification by NAF selection
- Classification by protocol selection
- Classification by advanced filtering (Boolean expression that comprises RADIUS attributes and values)

ACS uses three conditions to determine how an access request is classified and mapped to a profile. ACS selects the profile when all three conditions match. For each condition, you can substitute the value *Any* to always match the condition.

You can classify (filter) a user request by choosing a NAF from the list of existing NAFs. You configure NAF objects in the Shared Profile Components pages.

You can use protocol types to choose one or more protocol types as a filter. The protocol types are a subset of the vendor-specific attributes (VSAs) that a network access server supports. ACS 4.1 does not support the TACACS+ protocol for NAPs.

You can use Advanced Filtering to create a specific rule that contains one or more RADIUS attributes and values. The Advanced Filtering rules are based on a Boolean AND expression that uses RADIUS attributes to examine the request packet.

Each NAP contains a name, description, active flag and a set of classifications that you use to rank an access request based on different parameters.

Create a NAP

To create a NAP:

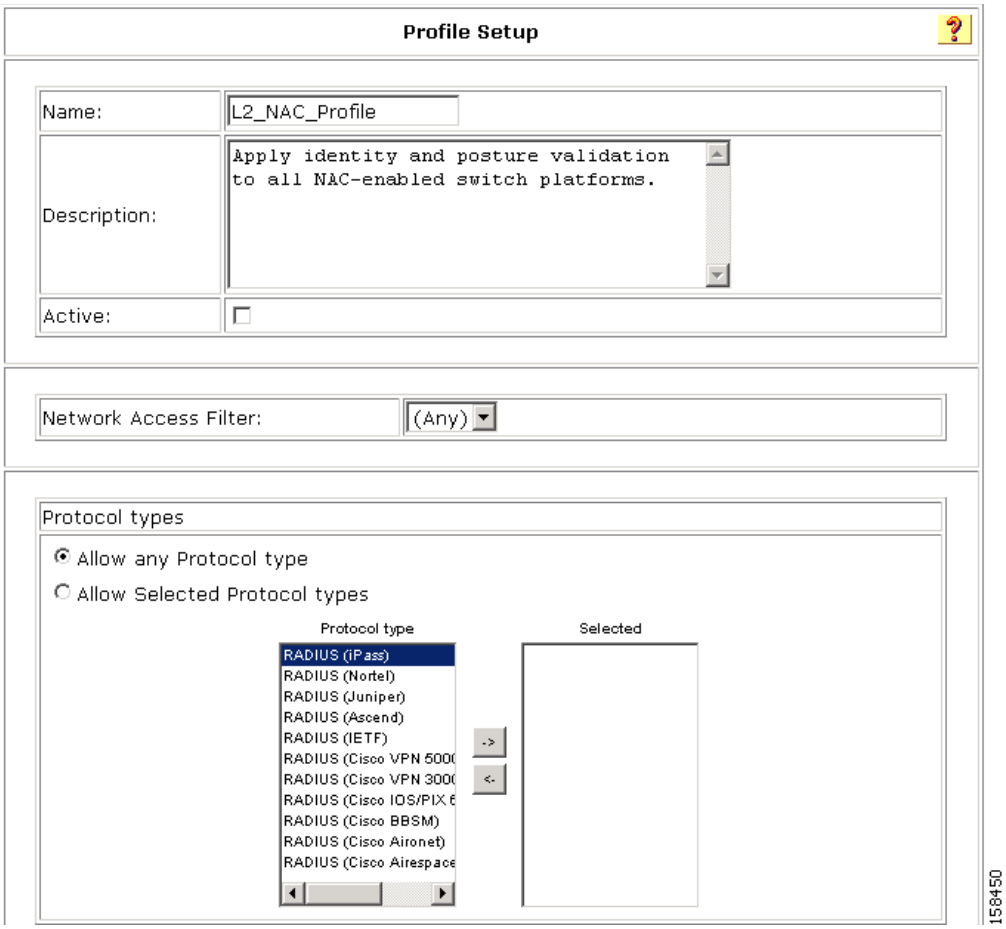
Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens. Initially, the list of Network Access Profiles is empty.

Step 2 Click **Add.**

The Profile Setup page opens, as shown in Figure 7-10.

Figure 7-10 Profile Setup Page



Step 3 Enter a name for the profile.

Step 4 If you want to activate the profile now, check the **Active** check box.

Step 5 To select the protocols that the profile will be used with, click the **Allow Selected Protocol** types radio button, and then move one or more protocols to the Selected area.

Step 6 Click **Submit**.

Step 12: Configure Profile-Based Policies

After you create a profile, configure the policies to associate with that profile. The available policies are:

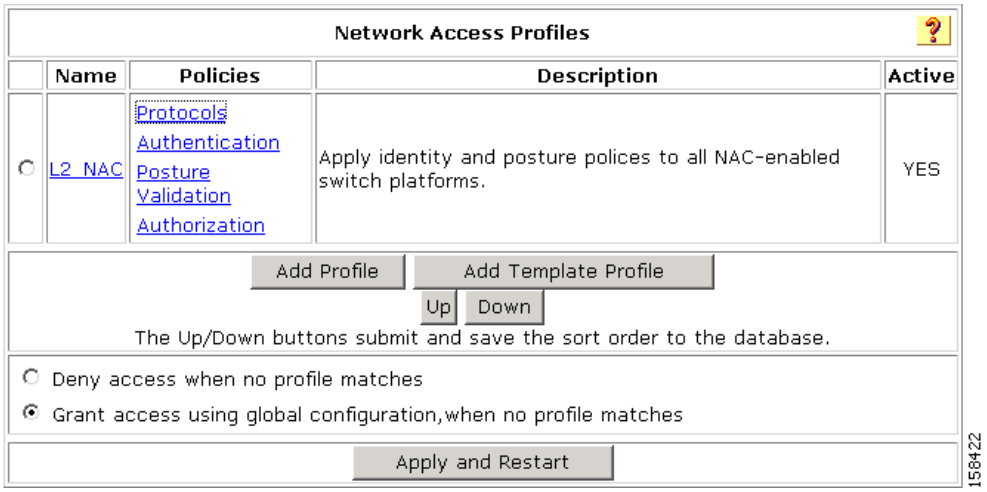
- **Protocols**—The protocols with which the selected profile is used.
- **Authentication**—The set of configuration policies that are related to authentication mechanisms.
- **Posture Validation** —Settings that define how posture validation will be performed.
- **Authorization** —An optional set of authorization rules. If you do not specify authorization policies, ACS defaults to the global configuration setting of authorizing by user-groups.

To configure profile-based policies:

Step 1 In the navigation bar, click **Network Access Profiles.**

The Edit Network Access Profiles page opens, as shown in Figure 7-11.

Figure 7-11 Edit Network Access Profiles Page



Step 2 Click a a profile option to configure.

- **Protocols**—To configure protocol settings, see Configure Protocol Settings, page 7-19.
- **Authentication**—To configure authentication settings, see Configure Authentication, page 7-19.
- **Posture Validation**—To configure posture validation, see Configure Posture Validation, page 7-21.
- **Authorization**—To configure authorization, see Configure Authorization, page 7-22.

Configure Protocol Settings

To configure protocol settings:

Step 1 On the Network Access Profiles page, click **Protocols**.

The Protocols Settings page for the selected profile opens.

Step 2 In the EAP section, check the **Allow Posture Validation** check box.

Step 3 Check the **Enable EAP-FAST** check box.

Step 4 If you are using agentless host processing, check the **Allow Agentless Host Processing** check box.

Step 5 Click **Submit**.

Configure Authentication

The Authentication page for a specified profile controls how a profile authenticates matched requests and which user-validation databases ACS uses for authentication.

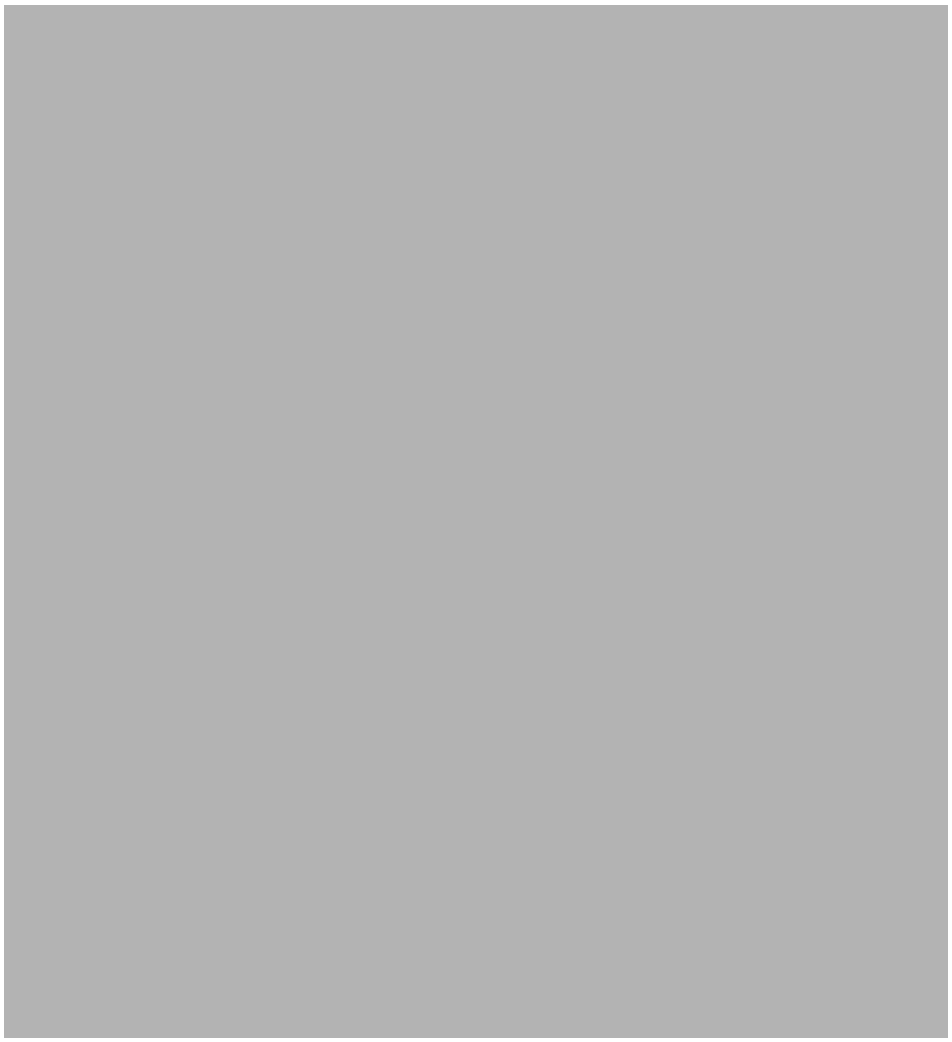
The Authentication page list the databases that were configured in the External User Databases section. These databases are mapped to ACS user groups based on the mapping rules defined in **External User Databases > Databases Group Mapping.**

To configure profile authentication settings:

Step 1 In the Edit Network Access Profiles page for the profile that you want to edit, click **Authentication**.

The Edit Authentication page for the selected profile opens. Figure 7-12 shows an example.

Figure 7-12 Edit Authentication Page for a Selected Profile



Step 2 Select one or more databases from the list of Available Databases and click the right arrow button to move them to the list of Selected databases.

Step 3 If you are configuring a MAC authentication bypass (MAB), see Configure MAB, page 4-20 for instructions on configuring MAB.

Configure Posture Validation

Posture validation rules define how ACS performs posture validation. Each posture validation rule specifies a condition and associated actions. The condition contains a set of required credential types, and the action contains a list of external posture validation servers (optional) and internal posture validation polices.

Posture Validation rules also contain:

- The name for the rule.
- A mandatory credential that defines the mandatory credential types that activate this rule.
- Local policies.
- A list of external servers that ACS queries for information that it uses to calculate a posture token.
- Posture Agent (PA) messages that return the client for each token.
- URL redirect information that is sent to the network access device for each token.

ACS evaluates posture rules by using a first-match strategy. ACS calculates the “worst” token that is returned based on the selected internal policies and information that the external posture servers send.

If the client is a nonresponsive host (NRH), ACS uses a specified audit server to audit the client.

Audit Servers are 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 called agentless hosts. The Cisco PA is called the Cisco Trust Agent. ACS uses audit servers to assess posture validation based on an organization’s security policy.

Configure Authorization

A profile-based authorization policy is a set of conditions that ACS uses to authenticate users to the network. ACS associates the conditions that you specify in the authorization policy with actions that determine which RAC and downloadable ACLs are returned to the network device.

When you configure an authorization policy, you can also specify whether access to the network is denied for a specific user group; or, in a NAC network, denied based on a returned posture token. Authorization policies are tied not only to the user identity, but also to the profile type to which a user is mapped and the posture of the machine used to access the network.

Note In a non-NAC network, leave the assessment result simply as *Any* (the default).

An authorization rule has this form:

If (user-group = selected-user-group and posture-token = selected-posture-token),

then provision (selected-RAC and selected-dACL)

You can also use the authorization rules to explicitly deny (send an access-reject) as an action. If you check the **Include RADIUS attributes from user-group/user** check box, ACS merges the RADIUS attributes defined in the user configuration, user-groups, and RAC. This process is:

1. ACS adds all nonconflicting attributes from all sources.
2. If a conflict occurs between the RADIUS attributes, ACS uses the attribute from the highest priority sources, where priority is assigned (from high to low):
   a. User
   b. RAC
   c. User-group

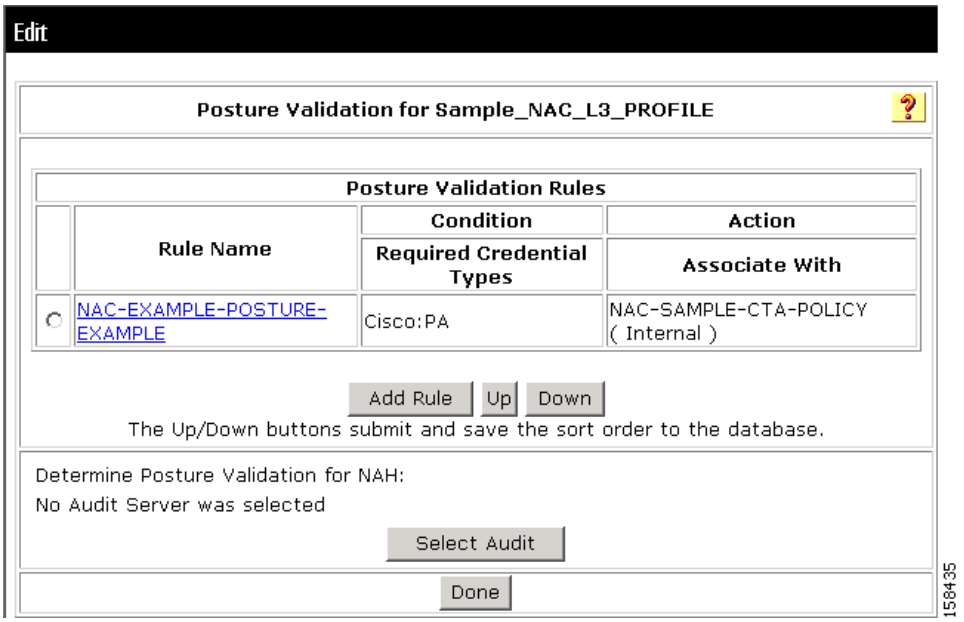
Create an Authorization Policy

To create an authorization policy for a profile:

Step 1 On the Network Access Profiles page, click **Authorization**.

The Edit Authorization Rules page for the selected profile opens. Figure 7-13 shows an example.

Figure 7-13 Edit Authorization Policy Page



Step 2 Click **Add Rule** to add a line.

Step 3 Choose a User Group, System Posture Token, Shared RAC, and Downloadable ACL.

Note You must edit the default authorization rule if you do not check the **Include RADIUS attributes from user's group** and **Include RADIUS attributes from user record** check boxes.

Step 4 Add additional authorization rules as required.

Step 5 Click **Submit**.

Step 6 Click **Apply and Restart**.

Define ACLs

In ACS 4.1, you can download access lists to specific devices or device groups.

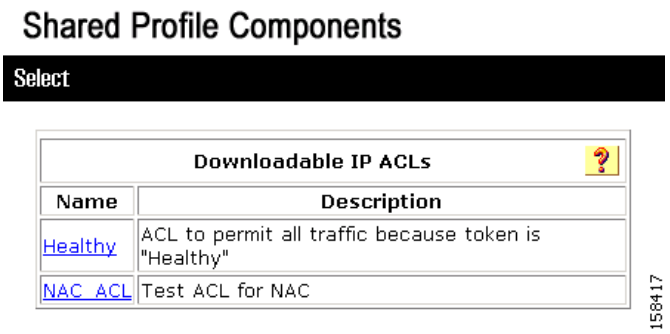
You can define an access list that contains one or more ACLs and later download the list to network devices, based on their assignments to user groups. Before you define ACLS, enable downloadable ACLs.

To define an ACL:

Step 1 Choose **Shared Profile Components > Downloadable IP ACLs**.

A list of downloadable IP ACLs appears, as shown in Figure 7-14:

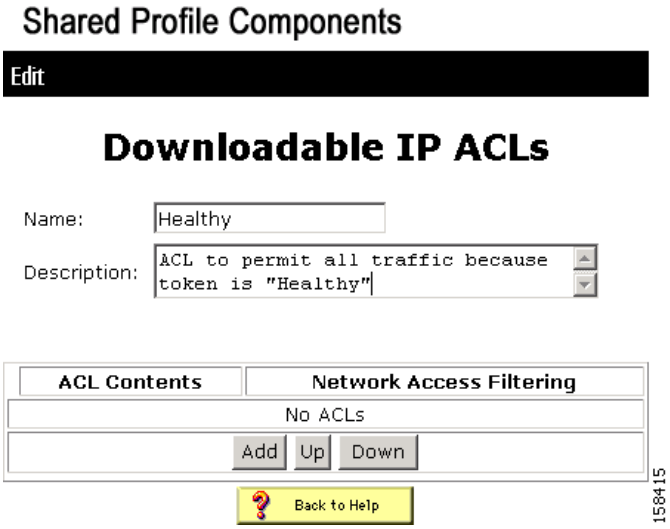
Figure 7-14 Downloadable IP ACL List



Step 2 Click **Add**.

The Edit Downloadable IP ACLs page opens, as shown in Figure 7-15.

Figure 7-15 Downloadable IP ACLs Page



Each Assessment Result (system posture token), according to its definition, should have its own ACL, which contains one or more Access Control Entries (ACEs) that will instruct the NAC network device (router) to block packets from going to a specific destination or allow packets to reach a specific destination.

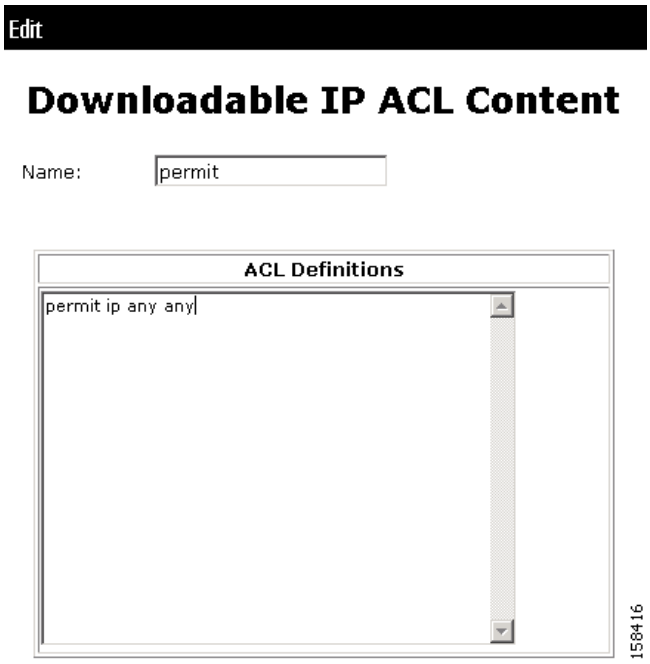
Step 3 On the Downloadable IP ACLs page, enter a Name and optional Description for the ACL.

Note Do not use spaces in the name of the ACL. IOS does not accept ACL names that include spaces.

Step 4 Click **Add** (below the ACL table of contents) to add a new Access Control Entry (ACE) to the ACL and assign it to a NAF.

The Downloadable IP ACL Content page opens, as shown in Figure 7-16.

Figure 7-16 Downloadable IP ACL Content Page



Step 5 In the Name text box, type the ACL name.

Step 6 In the ACL Definitions input box, type definitions for the ACL.

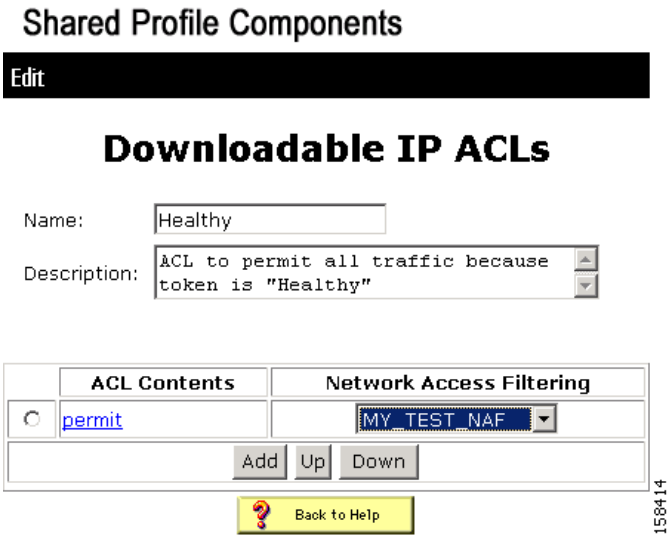
ACL definitions consist of a series of **permit** and **deny** statements that permit or deny access for specified hosts. For information on the syntax for ACL definitions, see the "Downloadable ACLs" section of Chapter 4 of the *User Guide for Cisco Secure Access Control Server 4.1*, "Shared Profile Components."

Step 7 Click **Submit**.

Note Before configuring the ACL on ACS, you should test the syntax on the device to ensure that each ACE is valid.

The Downloadable ACL page appears with the new ACL in the ACL Contents list, as shown in Figure 7-17.

Figure 7-17 Downloadable ACL Contents List with New Content



Step 8 From the drop-down list in the Network Access Filtering column of the ACL Contents table, choose the correct NAF for this ACL.

You perform this action to enable the downloading of different ACEs for different devices or a group of devices. For example, the syntax of an ACE on routers differs from the syntax on a Project Information Exchange (PIX) firewall. By using a NAF, you can assign the same ACL to a PIX and a router, even though the actual ACE that is downloaded is different.

Step 9 Click **Submit**.

The new ACL appears on the list of downloadable ACLs.

Create a RAC

Shared RADIUS Authorization Components (RACs) contain groups of RADIUS attributes that you can dynamically assign to user sessions based on a policy. For example, you can create a RAC that gathers RADIUS attributes to define a VLAN. By using NAP configuration, you can define a policy that ACS uses to apply conditions specified in Network Access Filters (grouped NDGs), and in posture assessment rules to the shared RAC.

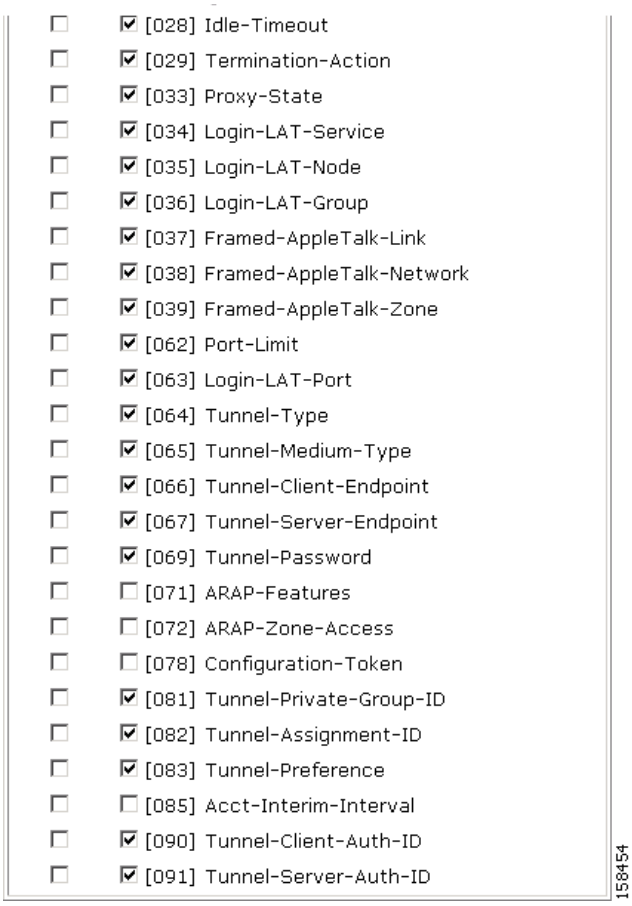
To define RACs:

Step 1 Select the appropriate Tunneling RADIUS attributes in the Advanced Options page:

a. Choose **Interface Configuration > RADIUS (IETF)**.

b. Choose the Tunnel attributes as shown in Figure 7-19.

Figure 7-18 Tunnel Attributes for RACs Used in NAC Configuration:



c. Click **Submit**.

d. Restart ACS to enable the new settings.

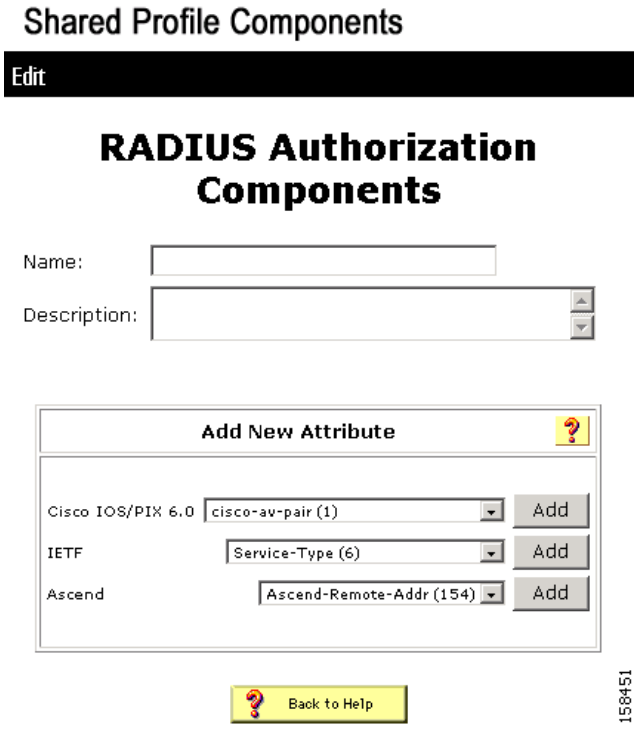
To restart the system, choose **System Configuration > Service Control** and then click **Restart**.

Step 2 To add a RAC:

a. Choose **Shared Profile Components > RADIUS Authorization Components**.

The RADIUS Authorization Components page for Tunnel type (64) opens, as shown in Figure 7-19.

Figure 7-19 RADIUS Authorization Components Page

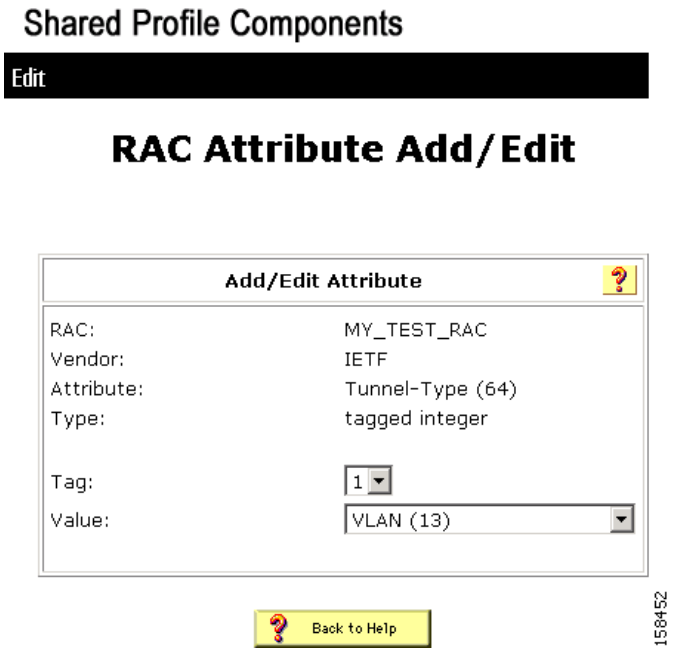


b. Enter a Name and Description in the RADIUS Authorization Components page.

c. From the IETF lists, select **Tunnel type (64)** and click **Add**.

The RAC Attribute Add/Edit page opens, as shown in Figure 7-20.

Figure 7-20 RAC Attribute Add/Edit Page



d. Click **Submit**.

Step 3 Add **Tunnel-Medium-Type = 802(6)**, **Tunnel-Prate-Group-ID = <vlan name>**, or any other attribute that is required to define a VLAN.

Step 4 Click **Submit**.

Step 13: Configure Posture Validation for NAC

This section describes how to set up simple posture validation for a NAC-enabled network. You can create internal policies that ACS uses to validate the posture data or you can configure ACS to send the posture data to an external posture validation server.

Configure Internal Posture Validation Policies

An *internal posture validation policy* is an internal attribute policy that you can use in more then one profile. The result of an internal posture validation policy returns a Posture Assessment (*token*) according to rules that you set.

To create an internal posture validation policy:

Step 1 In the navigation bar, click **Posture Validation**.

The Posture Validation Components Setup page opens.

Step 2 Click **Internal Posture Validation Setup**.

The Posture Validation page opens, which lists any existing posture validation policies.

Step 3 Choose **Add Policy**.

The Edit Posture Validation page opens.

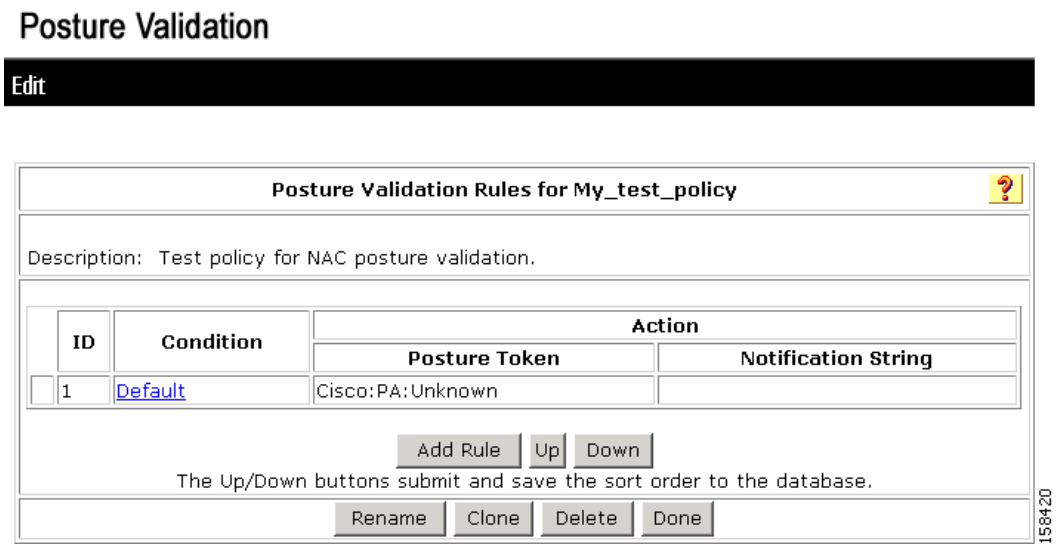
Step 4 Enter a name for the policy.

Step 5 Enter a Description (optional).

Step 6 Click **Submit**.

A new internal policy is created with a default rule. Figure 7-21 shows an example policy.

Figure 7-21 Creating a New Posture Validation Policy



Step 7 To edit the default rule:

a. Click on the **Default** link.

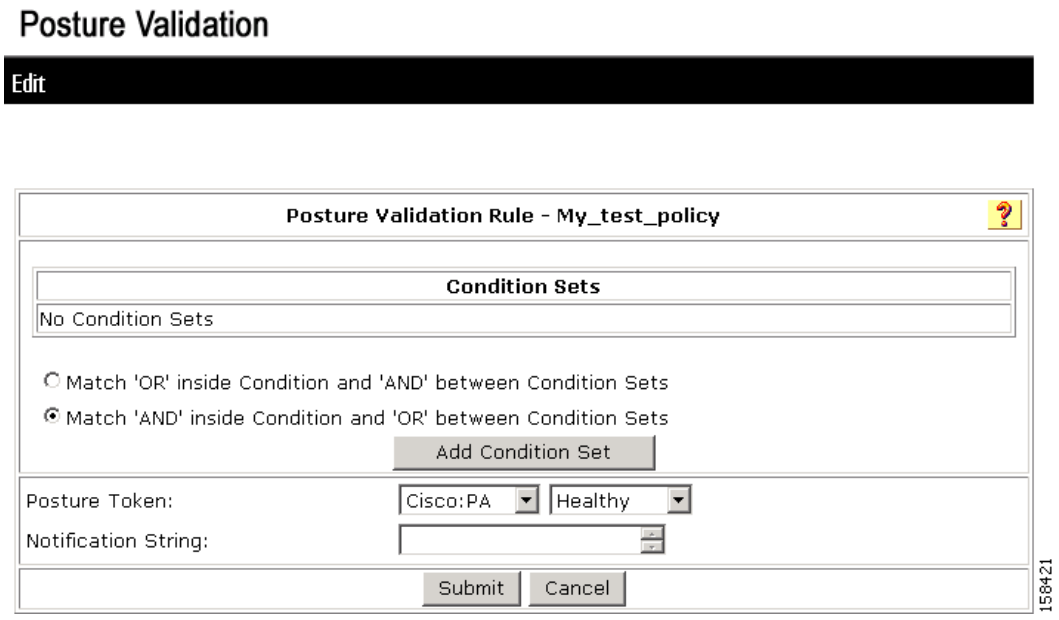
b. Choose a new Posture Assessment and Notification String for the default rule.

Step 8 To add a new rule:

a. Click **Add Rule**.

The Edit Posture Rule page appears, as shown in Figure 7-22. Initially no conditions are available for the rule.

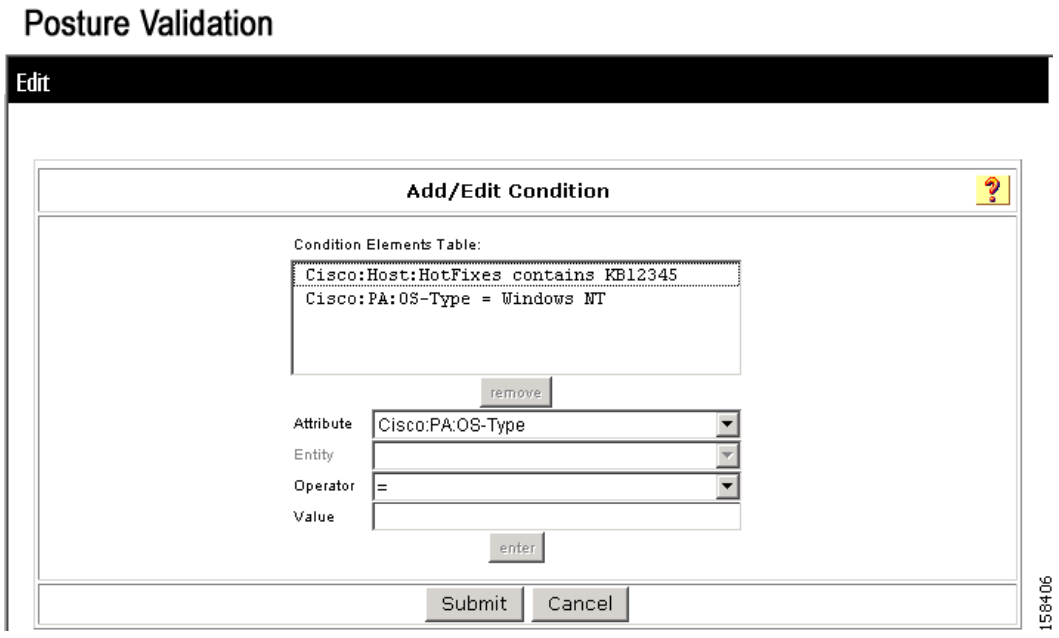
Figure 7-22 Edit Posture Validation Rule Page



b. Click **Add Condition Set**.

c. The Add/Edit Condition page appears, as shown in Figure 7-23.

Figure 7-23 Add/Edit Condition Page



d. From the **Attribute** drop-down list, choose an Attribute value.

e. From the Operator drop-down list, choose a condition.

f. In the Value text box, enter a value for the condition.

g. Click **Enter**.

The specified rule appears in Add/Edit Condition page appears, as shown in Figure 7-23.

h. Enter additional conditions as required.

i. Click **Submit**.

j. Click **Apply and Restart** to apply the new posture validation rule(s).

For information on creating advanced rules, see Configure Posture Validation, page 7-21.

Configure External Posture Validation Policies

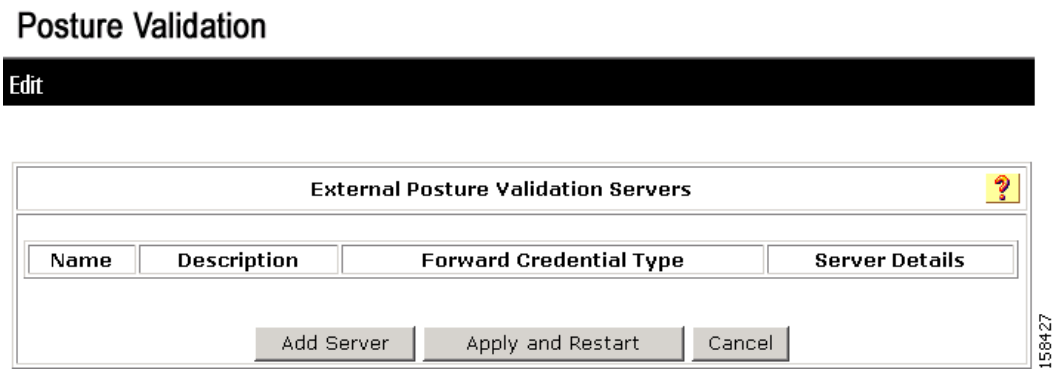
An external posture validation policy uses an external server that returns a posture assessment (token) to ACS according to data that the ACS forwards to this server.

To set up an external posture validation server:

Step 1 In the Posture Validation Components Setup page, click **External Posture Validation Setup**.

Step 2 The Edit External Posture Validation Servers page opens, as shown in Figure 7-24.

Figure 7-24 Edit External Posture Validation Servers Page

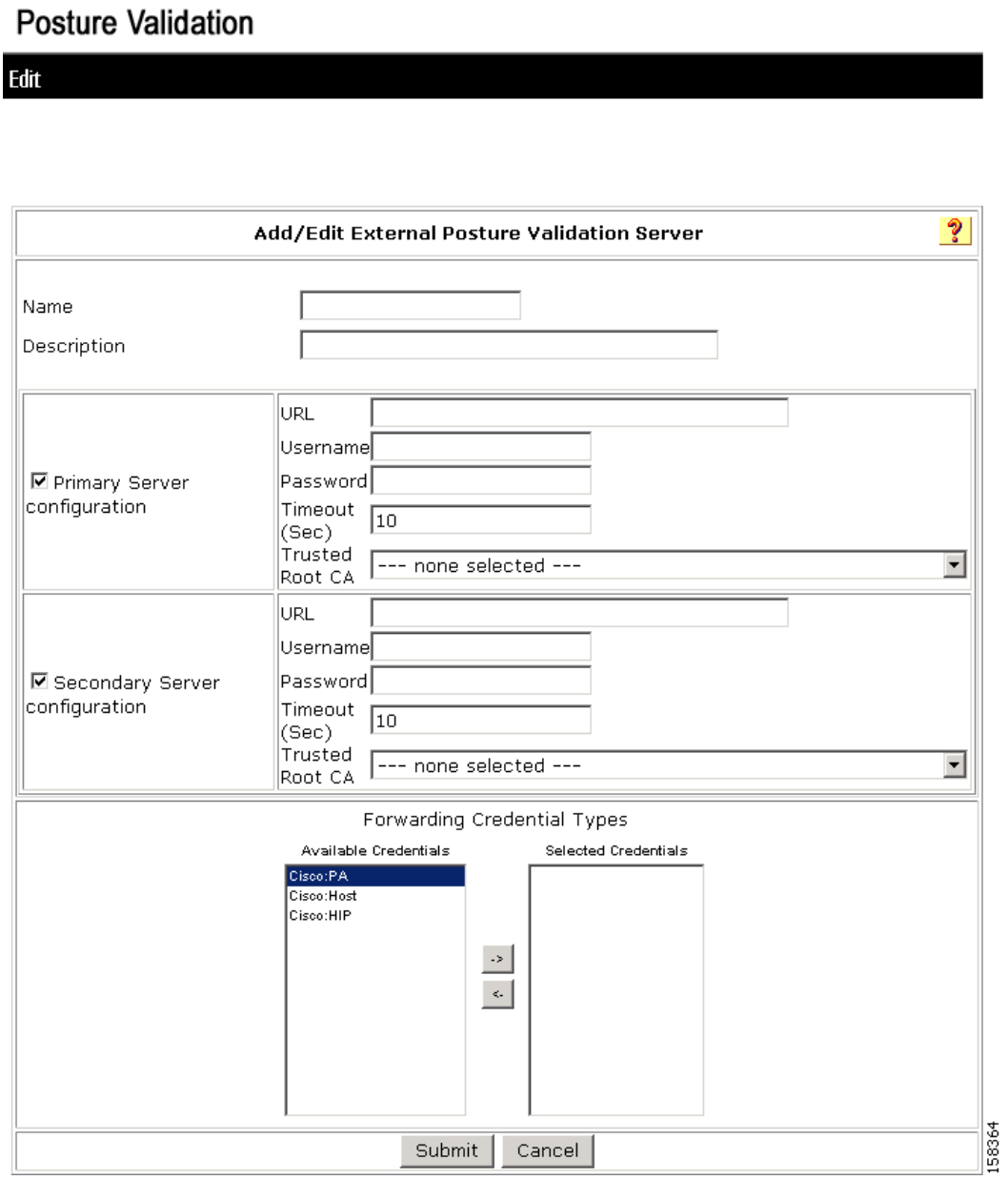


Initially, the list of external posture validation servers is empty.

Step 3 Click **Add Server**.

The Add/Edit External Posture Validation Server page appears, as shown in Figure 7-25.

Figure 7-25 Add/Edit External Posture Validation Server Page



Step 4 Enter a Name and Description (optional).

Step 5 Enter the server details, URL, User, Password, Timeout, and certificate (if required by the antivirus server).

Step 6 Click **Submit**.

Configure an External Posture Validation Audit Server

A NAC-enabled network might include agentless hosts that do not have the NAC client software. ACS can defer the posture validation of the agentless hosts to an audit server. The audit server determines the posture credentials of a host without relying on the presence of a PA.

Configuring an external audit server involves two stages:

- Adding the posture attribute to the ACS internal dictionary.
- Configuring an external posture validation server (audit server).

Add the Posture Attribute to the ACS Dictionary

Before you can create an external posture validation server, you must add one or more vendor attributes to the ACS internal data dictionary. To do this, you use the **bin\CSUtil** tool, which is located in the ACS installation directory.

To add the posture attributes:

Step 1 Create a text file in the *Utils* directory with the following format:

```
[attr#0]
vendor-id=[your vendor id]
vendor-name=[The name of you company]
application-id=6
application-name=Audit
attribute-id=00003
attribute-name=Dummy-attr
attribute-profile=out
attribute-type=unsigned integer
```

Your vendor ID should be the Internet Assigned Numbers Authority (IANA)-assigned number that is the first section of the posture token attribute name, [vendor]:6:

Step 2 To install the attributes specified in the text file:

a. Open a DOS command window.

b. Enter the following command:

\<*ACS_Install_Dir*>\bin\CSUtil –addAVP [*file_name*]

where *ACS_Install_Dir* is the name of the ACS installation directory and *file_name* is the name of the text file that contains vendor attributes.

Step 3 Restart the **CSAdmin**, **CSLog**, and **CSAuth** services.

Configure the External Posture Validation Audit Server

You can configure an audit server once, and then use it for other profiles.

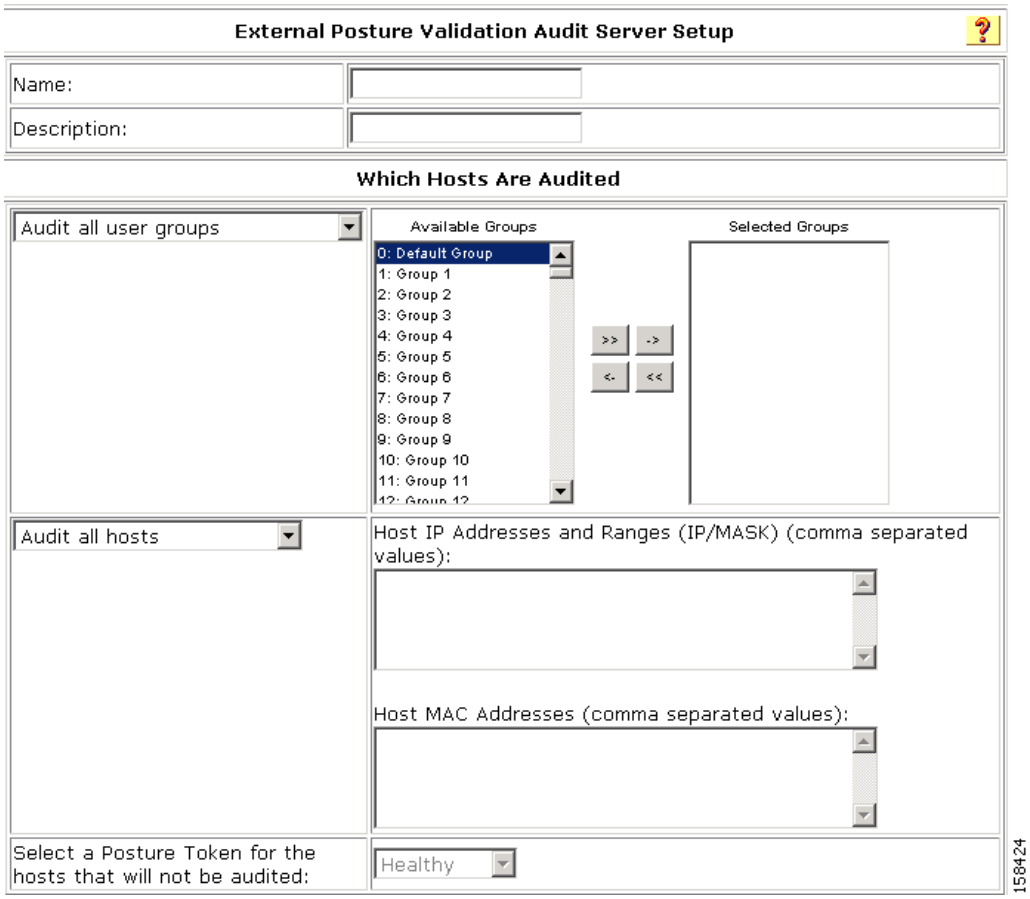
To configure an audit server:

Step 1 In the Posture Validation Components Setup page, click **External Posture Validation Audit Setup**.

Step 2 Click **Add Server**.

The External Posture Validation Audit Server Setup page appears, as shown in Figure 7-26.

Figure 7-26 External Posture Validation Audit Server Setup Page



Step 3 To configure the audit server:

a. Enter a Name and Description (optional).

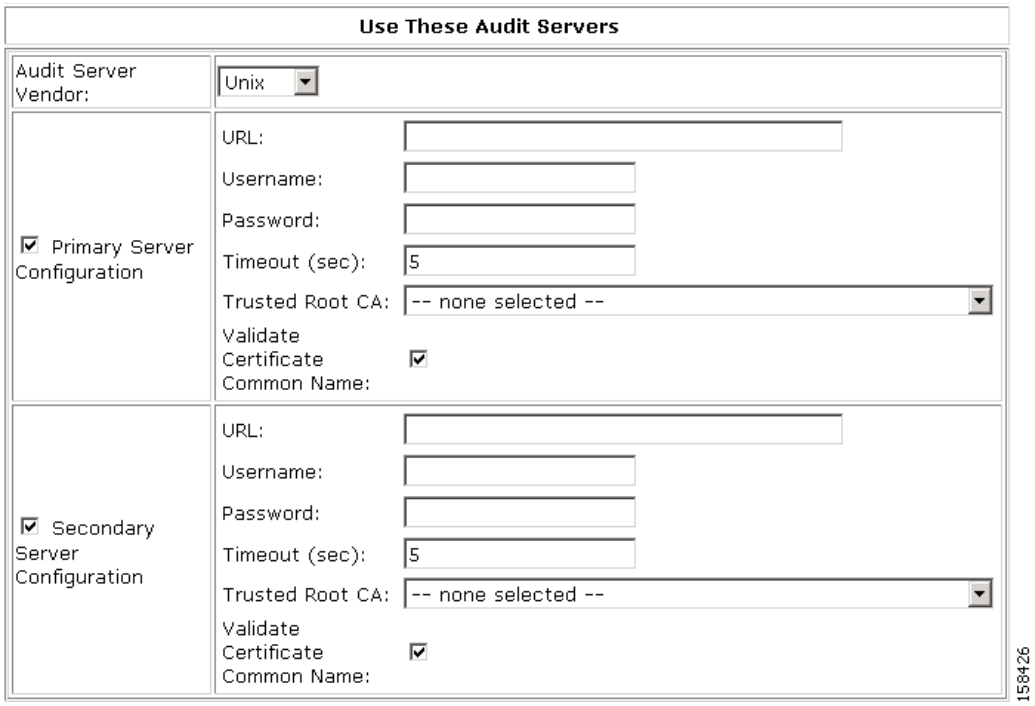
b. In the Which Hosts Are Audited section, choose what hosts you want to audit. You can enter the host IP or MAC addresses for the hosts that you want to audit or for a host that you do not want to audit.

c. For the hosts that will not be audited, choose a posture token from the drop-down list.

d. Scroll down to the Use These Audit Servers section.

Figure 7-27 shows the Use These Audit Servers section of the External Posture Validation Server Setup page.

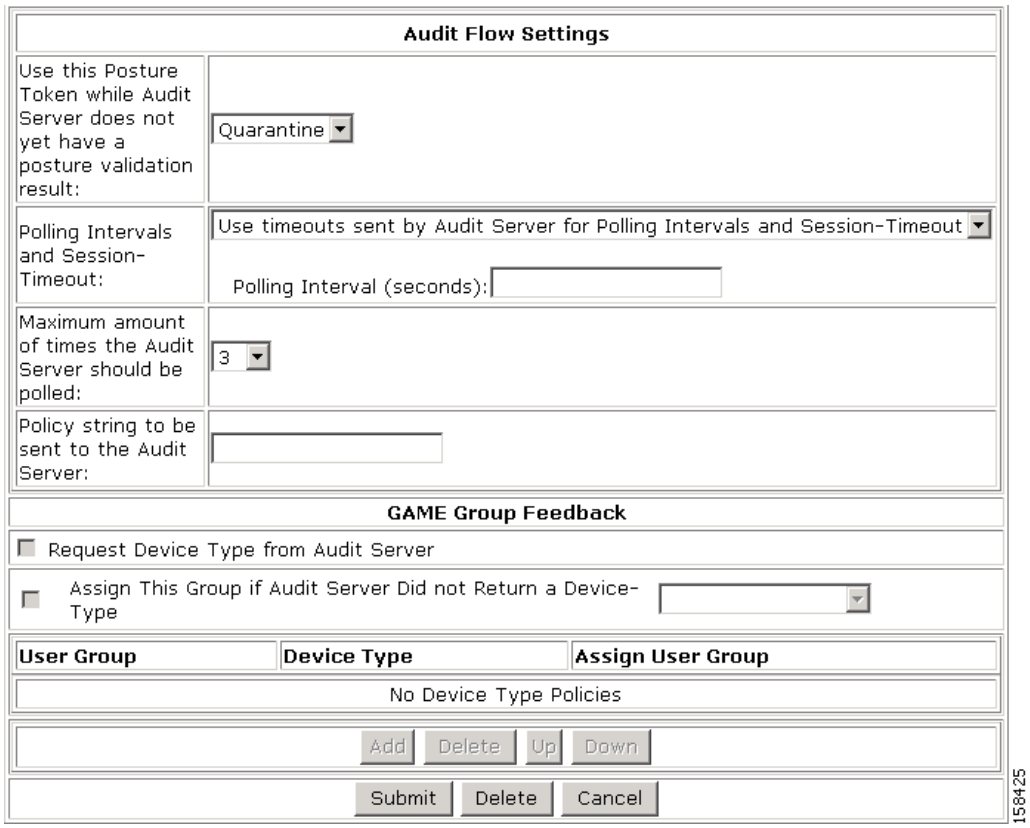
Figure 7-27 Use These Audit Servers Section



e. In the Use These Audit Servers section, enter the Audit Validation Server information, Audit Server vendor, URL, and password.

Figure 7-28 shows the Audit Flow Settings and the GAME Group Feedback section.

Figure 7-28 Audit Flow Settings and GAME Group Feedback Sections



f. If required, in the Audit Flow Setting section, set the audit-flow parameters.

g. If you are configuring GAME group feedback to support agentless host configuration in the NAC environment, configure the settings in the GAME Group Feedback section.

For information on configuring GAME Group Feedback settings, see Enable GAME Group Feedback, page 7-68.

h. Click **Submit**.

Authorization Policy and NAC Audit

Audit servers define two types of posture assessments (tokens). A:

- Temporary posture assessment is used as the *in progress* assessment. ACS grants the in progress posture assessment to the agentless host while the audit server is processing the auditing on the host and does not have a final result.
- *Final* posture assessment is the posture assessment that the audit server returns after it completes the auditing process.

Note To configure the authorization policy to work with the audit server, at least two RACs or downloadable ACLs are required: one for the in progress posture assessment and one for the final posture assessment. You should use a separate RAC or downloadable ACL for each token.

Step 14: Set Up Templates to Create NAPs

ACS 4.1 provides several profile templates that you can use to configure common usable profiles. In NAC-enabled networks, you can use these predefined profile templates to configure commonly used profiles. This section describes the templates provided in ACS 4.1.

Sample NAC Profile Templates

ACS 4.1 provides the following sample profile templates for NAC. A:

- NAC Layer 3 profile template (NAC L3 IP)
- NAC Layer 2 profile template (NAC L2 IP)
- NAC Layer 2 802.1x template (NAC L2 802.1x)
- Wireless (NAC L2 802.1x) template

In addition to these templates, ACS 4.1 provides two templates for agentless host processing that you can use in NAC installations:

- Agentless Host for Layer 3 profile template
- Agentless Host for Layer 2 (802.1x) profile template

Sample NAC Layer 3 Profile Template

This template creates a profile for Layer 3 NAC requests. Before you use this template, you should choose **System Configuration > Global Authentication Setup** and check the **Enable Posture Validation** check box**.**

To create a Layer 3 NAC profile template:

Step 1 Check the check boxes for the following options in the Global Authentication Setup page:

- Allow Posture Validation
- EAP-FAST
- EAP-FAST MS-CHAPv2
- EAP-FAST GTC

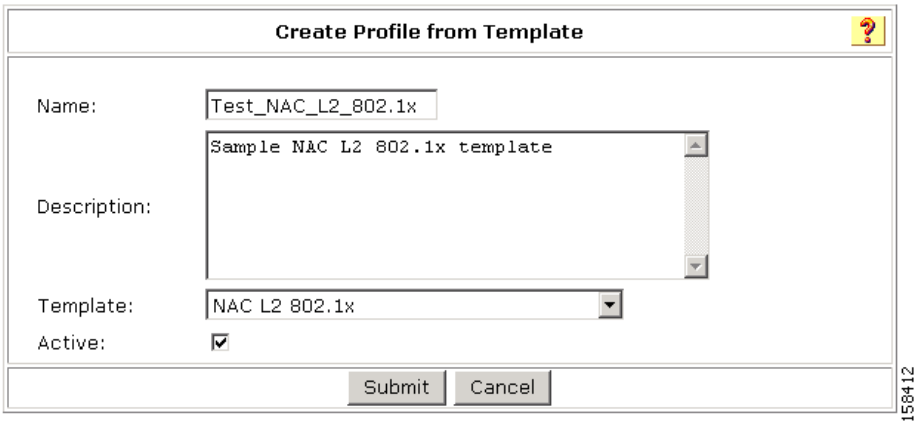
Step 2 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 3 Click **Add Template Profile**.

The Create Profile from Template page opens, as shown in Figure 7-29.

Figure 7-29 Create Profile From Template Page



Step 4 Enter a Name and Description (optional).

Step 5 From the **Template** drop-down list, choose **NAC L3 IP**.

Step 6 Check the **Active** check box.

Step 7 Click **Submit**.

If no error appears, then you have created a profile that can authenticate Layer 3 NAC hosts.

The Edit Network Access Profile page opens, and the new profile appears in the Name column.

The predefined values for the Layer 3 NAC template include:

- Profile Setup options
- Protocols
- A sample posture validation policy
- Authentication policy

Step 8 To select a predefined set of values, click on one of the configuration options:

- The profile name (to select the profile setup page for the profile)
- Protocols
- Authentication Policy
- Sample Posture Validation Rules

Profile Setup

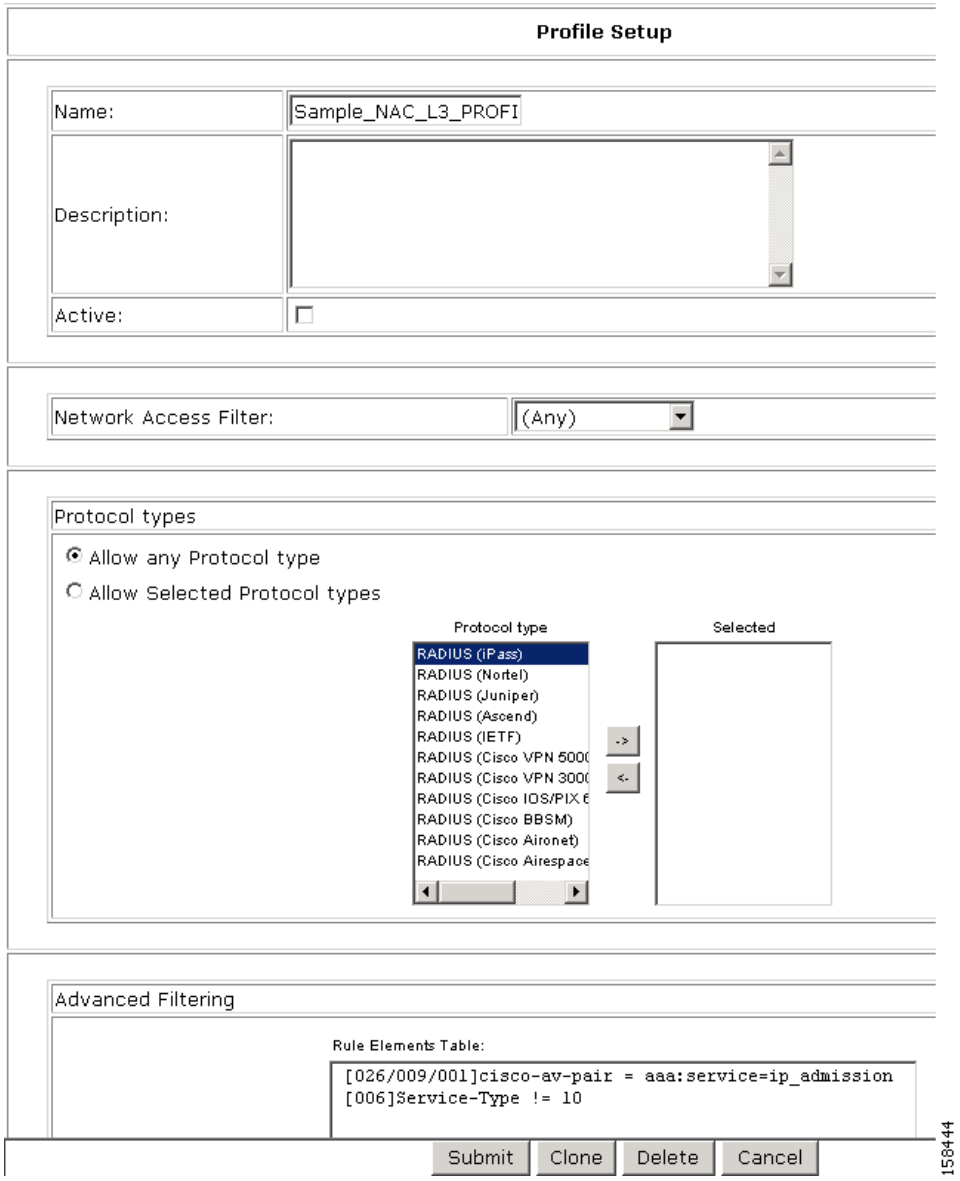
To use the Profile Setup settings from the template:

Step 1 In the navigation bar, click **Network Access Profiles**.

Step 2 Choose the profile that you created.

Step 3 The Profile Setup page appears, as shown in Figure 7-30.

Figure 7-30 Profile Setup Page for Layer 3 NAC Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- In the Protocol types list, **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can click the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

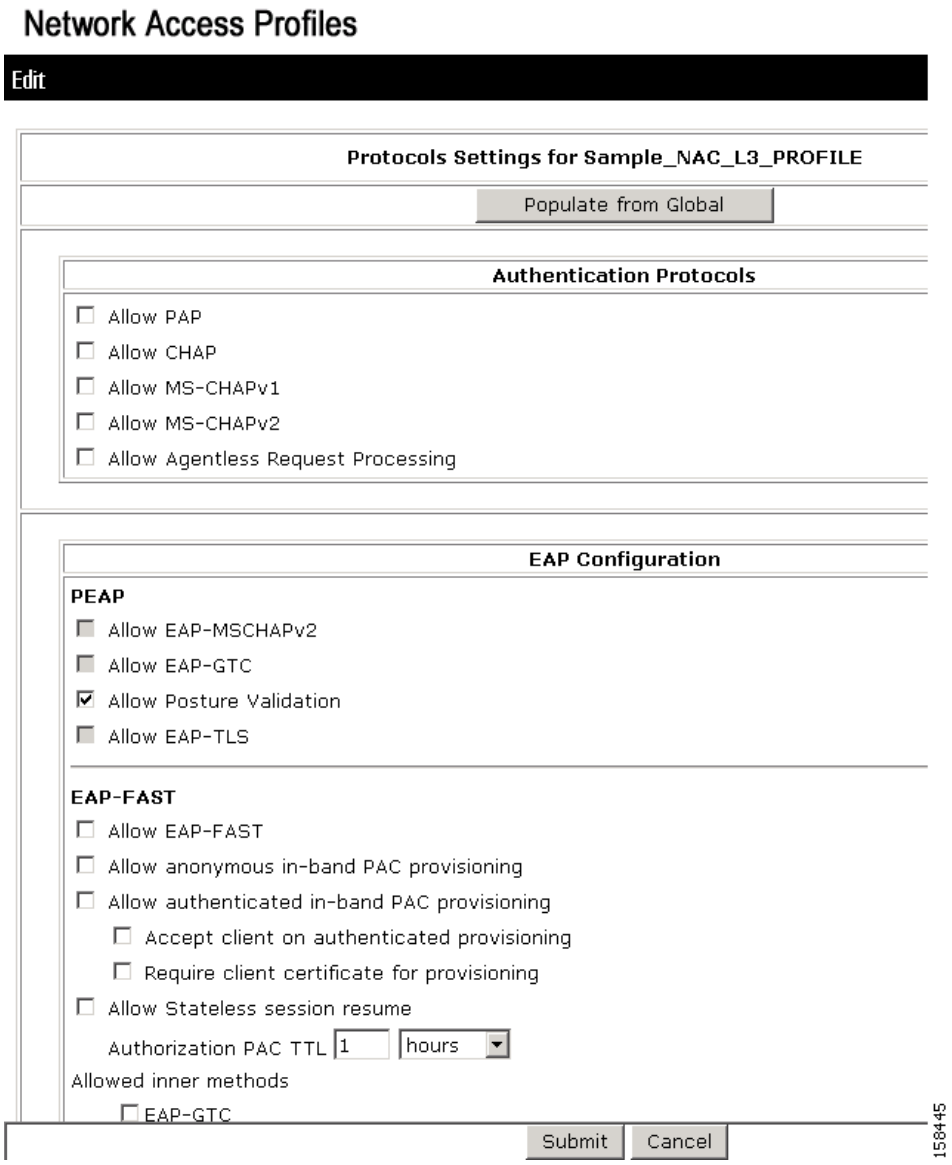
```
[026/009/001]Cisco-av-pair = aaa:service=ip admission
[006]Service-Type != 10
```

These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

Protocols Policy for the NAC Layer 3 Template

Figure 7-31 shows the Protocols settings for the NAC Layer 3 template.

Figure 7-31 Protocols Setting for NAC Layer 3 Template



In the EAP Configuration section, Posture Validation is enabled.

Authentication Policy

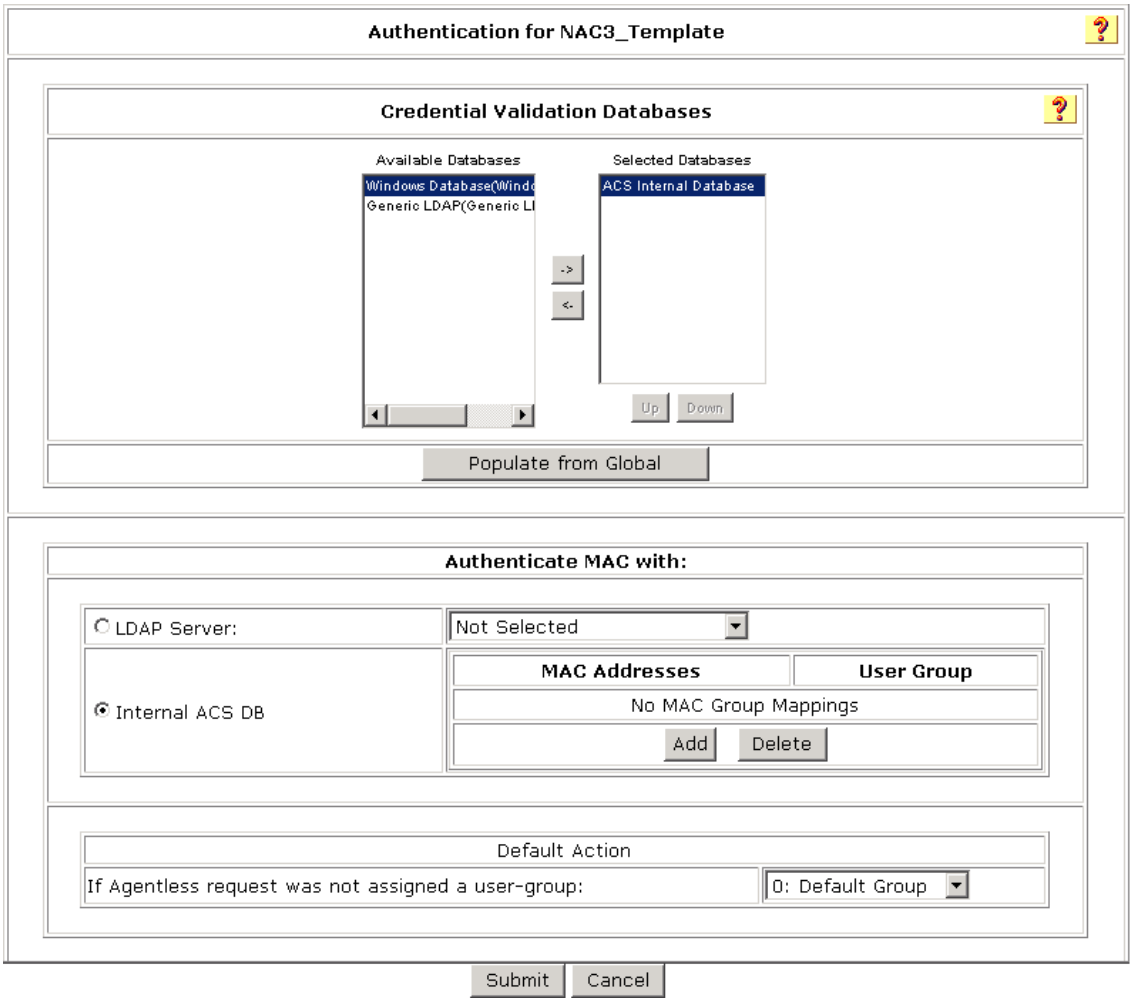
To configure authentication policy:

Step 1 In the navigation bar, select **Network Access Profiles**.

Step 2 Choose the **Authentication** link from the Policies column.

The Authentication page for the profile opens, as shown in Figure 7-32.

Figure 7-32 Authentication Page for Layer 3 NAC Profile Template



On this page, you can see the Layer 3 NAC template configuration for authentication:

Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

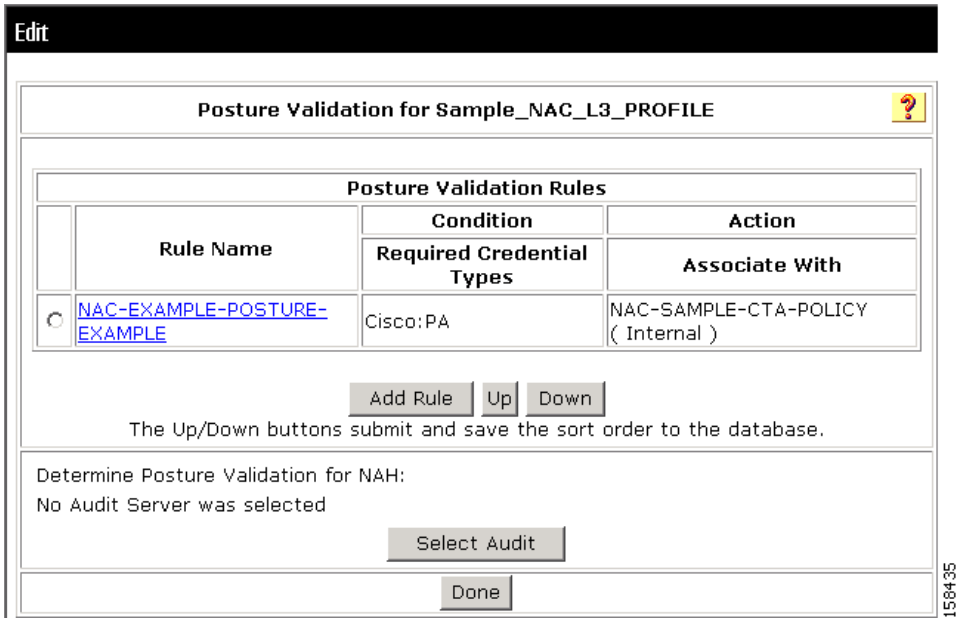
b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Sample Posture Validation Rule

Figure 7-33 shows the sample posture validation policy provided with the NAC Layer 3 template.

Figure 7-33 Sample Posture Validation Policy for NAC Layer 3 Template



Sample NAC Layer 2 Template

This template creates a profile for Layer 2 NAC requests.

Before you use the Layer 2 NAC profile template:

1. Select **EAP-FAST Configuration** in **Global Authentication Settings**.
2. Check (enable) the **Allow authenticated in-band PAC provisioning**.
3. Check (enable) **EAP-GTC** and **EAP-MSCHAPv2**.

To create a Layer 2 NAC profile template:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 2 Click **Add Template Profile**.

Step 3 Enter a Name and Description (optional).

Step 4 From the **Template** drop-down list, choose **NAC L2 IP**.

Step 5 Check the **Active** check box.

Step 6 Click **Submit**.

If no error appears, then you have created a Profile that can authenticate Layer 2 NAC hosts and the Profile Setup page for the NAC Layer 2 template appears.

The predefined values for the Layer 2 NAC template include:

- Profile Setup
- Protocols settings
- Authentication policy
- A sample posture validation rule

  The name of this policy is NAC-EXAMPLE-POSTURE-EXAMPLE.

Step 7 To select a configuration option, click the option name.

Profile Setup

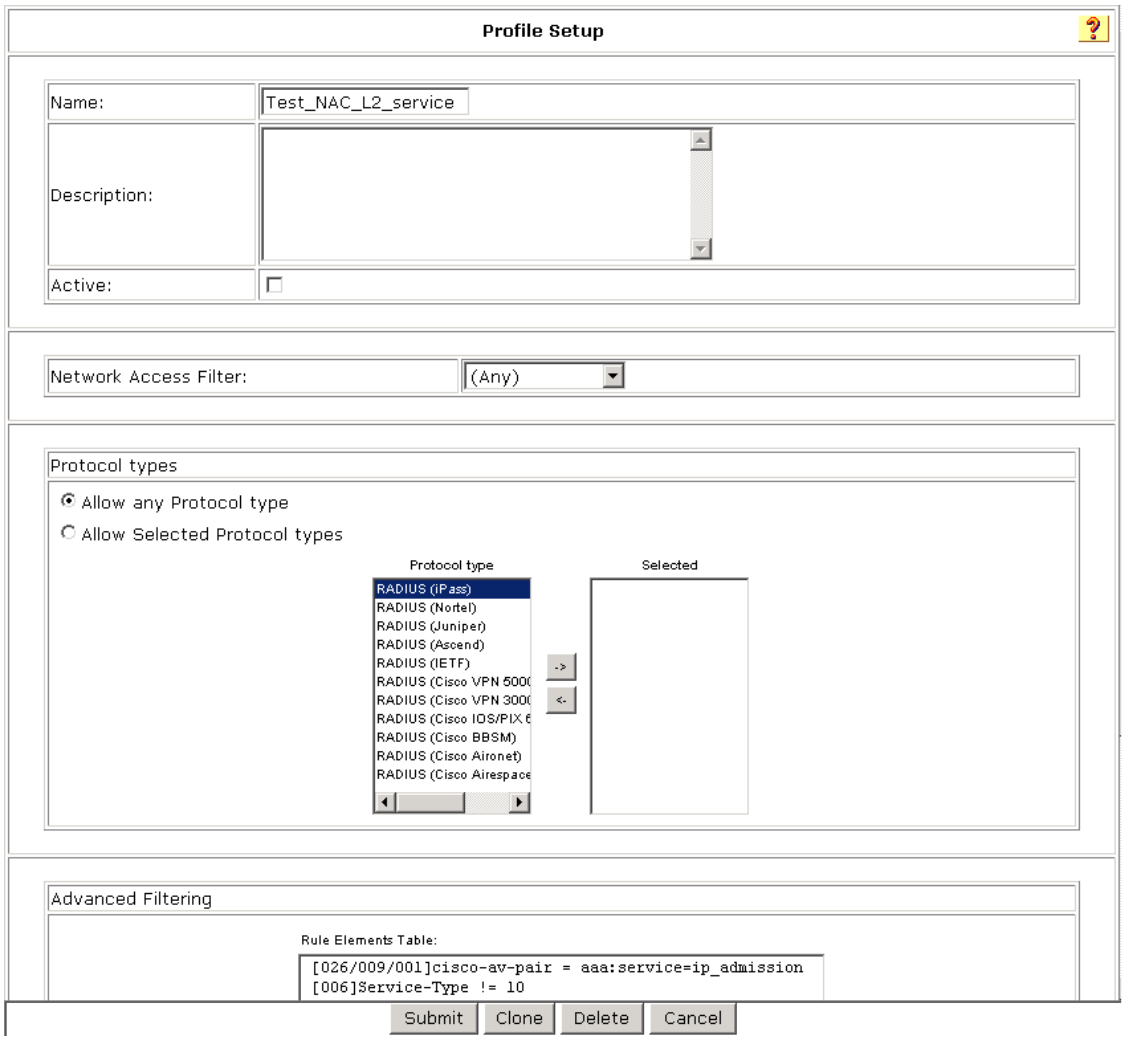
To enable the profile setup:

Step 1 Go to **Network Access Profiles**.

Step 2 Choose the Profile that you created.

The Profile Setup page appears, as shown in Figure 7-34.

Figure 7-34 Profile Setup Page for NAC Layer 2 Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can select the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

  ```
  [026/009/001]Cisco-av-pair = aaa:service=ip admission
  [006]Service-Type != 10
  ```

  These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

This template automatically sets Advanced Filtering and Authentication properties with NAC Layer 2 IP Configuration.

ACS and Attribute-Value 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 from 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.

  ACS uses the Auth-Proxy posture code to check if the switch has downloaded access-control entries (ACEs) for the specified downloadable ACL. If the switch has not downloaded the ACES, ACS sends an AAA request with the downloadable ACL name as the username so that the switch downloads the ACEs. 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, ACS takes appropriate actions required by NAC.

- **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 HTTP or Secure HTTP (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.

  If the host's posture is not healthy, ACS might send these AV pairs.

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.

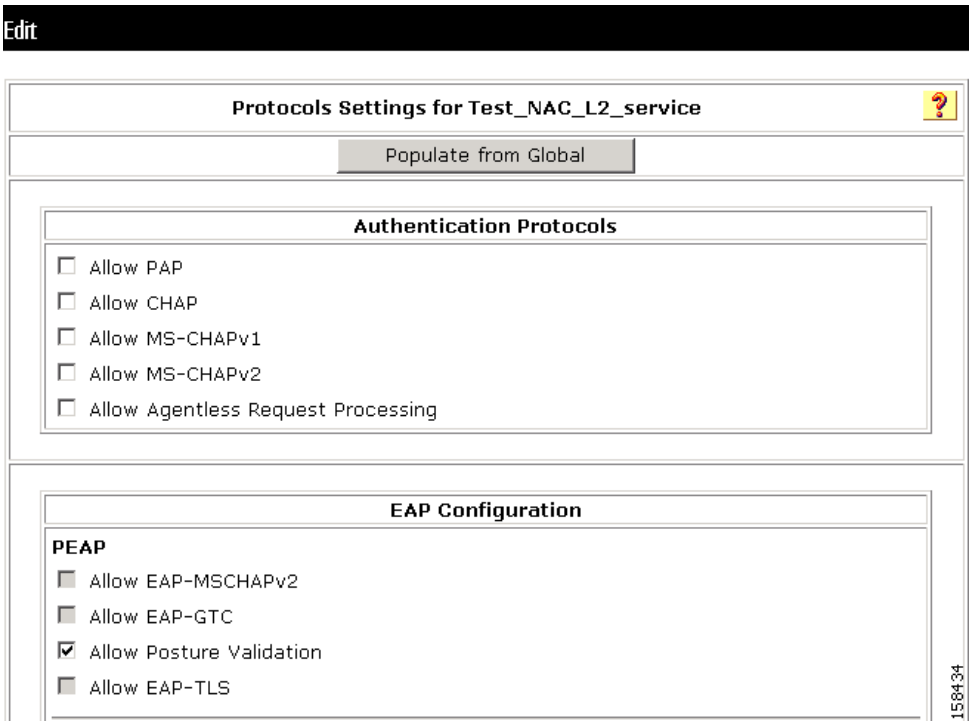
You use this template for access requests from Layer 2 devices that do not have the 802.1x client installed. The Authentication Bypass (802.1x fallback) template is used for access requests to bypass the nonclient authentication process. Users are mapped to a User Group based on their identity.

Note Do not click the **Populate from Global** button; otherwise, the settings for this authentication field will be inherited from the settings in the Global Authentication Setup in System Configuration.

Protocols Settings

Figure 7-35 shows the Protocols settings for the NAC Layer 2 template.

Figure 7-35 Protocols Setting for NAC Layer 2 Template



On this page, you can see the Layer 2 NAC template configuration for protocols. The default settings are:

- In the EAP Configuration area, posture validation is enabled.
- **Allow EAP-Fast Configuration** is checked, which means that this profile allows EAP-FAST authentication.

Authentication Policy

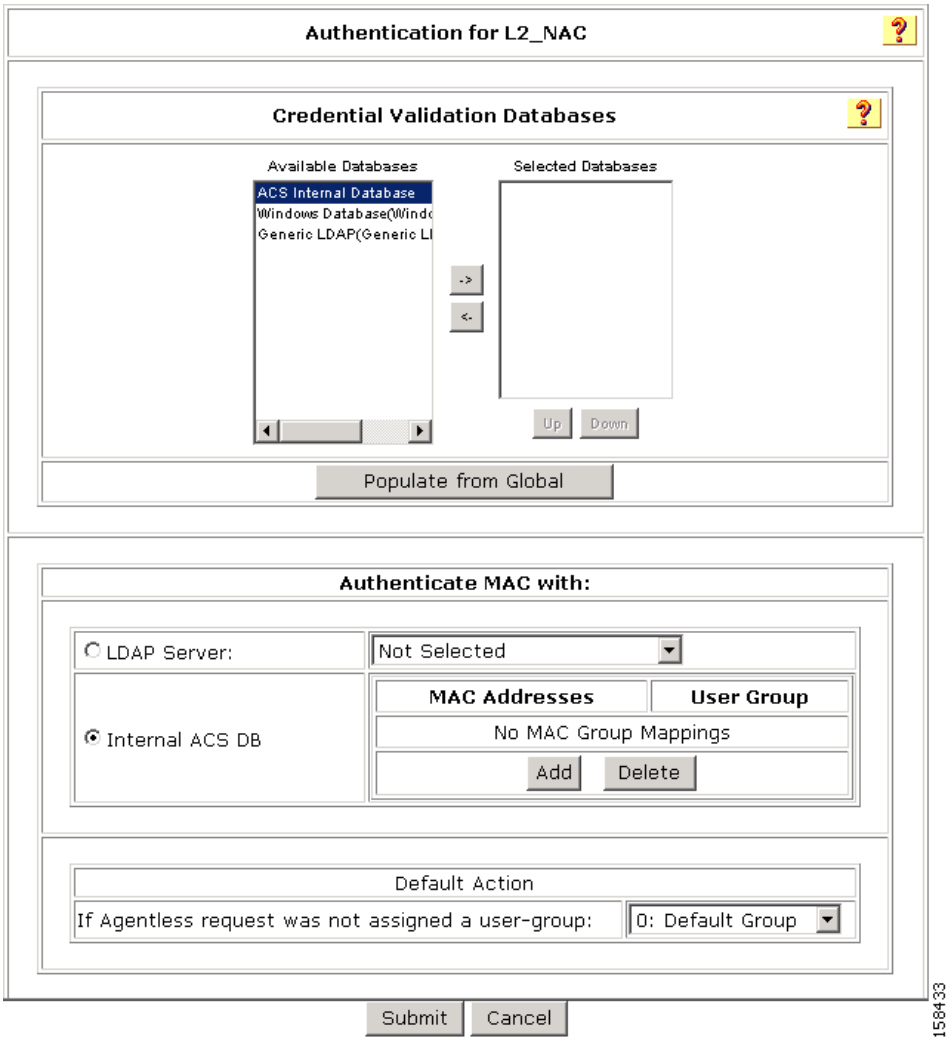
To set the authentication policy:

Step 1 In the navigation bar, click **Network Access Profiles**.

Step 2 Choose the **Authentication** link from the Policies column.

The Authentication Settings page for the NAC Layer 2 template opens, as shown in Figure 7-36.

Figure 7-36 Authentication Settings for NAC Layer 2 Template



Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

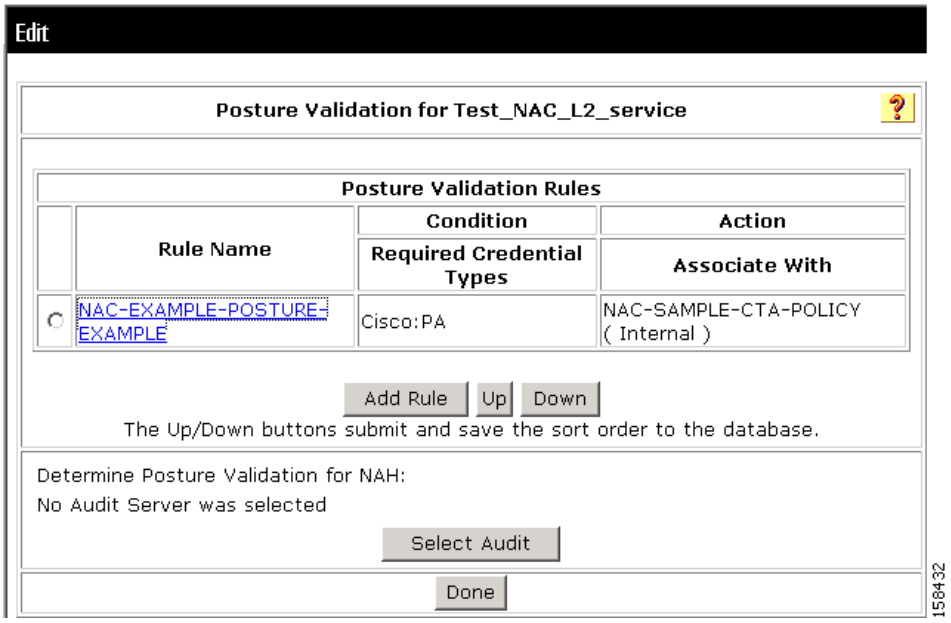
b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Sample Posture Validation Rule

Figure 7-37 shows the sample posture validation rule provided with the NAC Layer 2 template.

Figure 7-37 Sample Posture Validation Policy for NAC Layer 2 Template



Sample NAC Layer 2 802.1x Template

This template creates a profile for Layer 2 NAC 802.1x requests. Before you use this template, you should choose **System Configuration > Global Authentication Setup** and check the **Enable Posture Validation** check box**.**

To create a Layer 2 NAC 802.1x profile template:

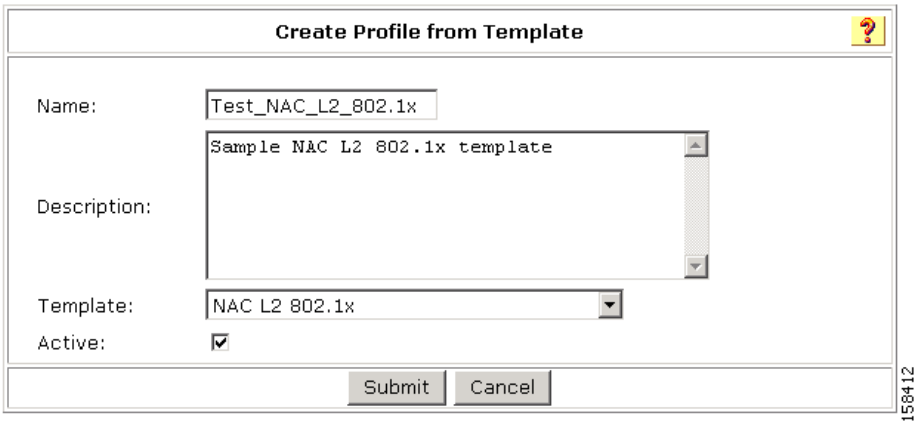
Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 2 Click **Add Template Profile**.

The Create Profile from Template page opens, as shown in Figure 7-38.

Figure 7-38 Create Profile From Template Page



Step 3 Enter a Name and Description (optional).

Step 4 From the **Template** drop-down list, choose **NAC L2 802.1x**.

Step 5 Check the **Active** check box.

Step 6 Click **Submit**.

If no error appears, then you have created a Profile that can authenticate Layer 2 NAC hosts.

The Edit Network Access Profile page opens, and the new profile appears in the Name column.

The predefined values for the Layer 2 NAC 802.1x template include:

- Profile Setup
- Protocols
- A sample posture validation policy
- Authentication policy

Step 7 To select a predefined set of values, click on one of the configuration options:

- The profile name (to select the profile setup page for the profile)
- Protocols
- Authentication Policy
- Sample Posture Validation Rules

Profile Setup

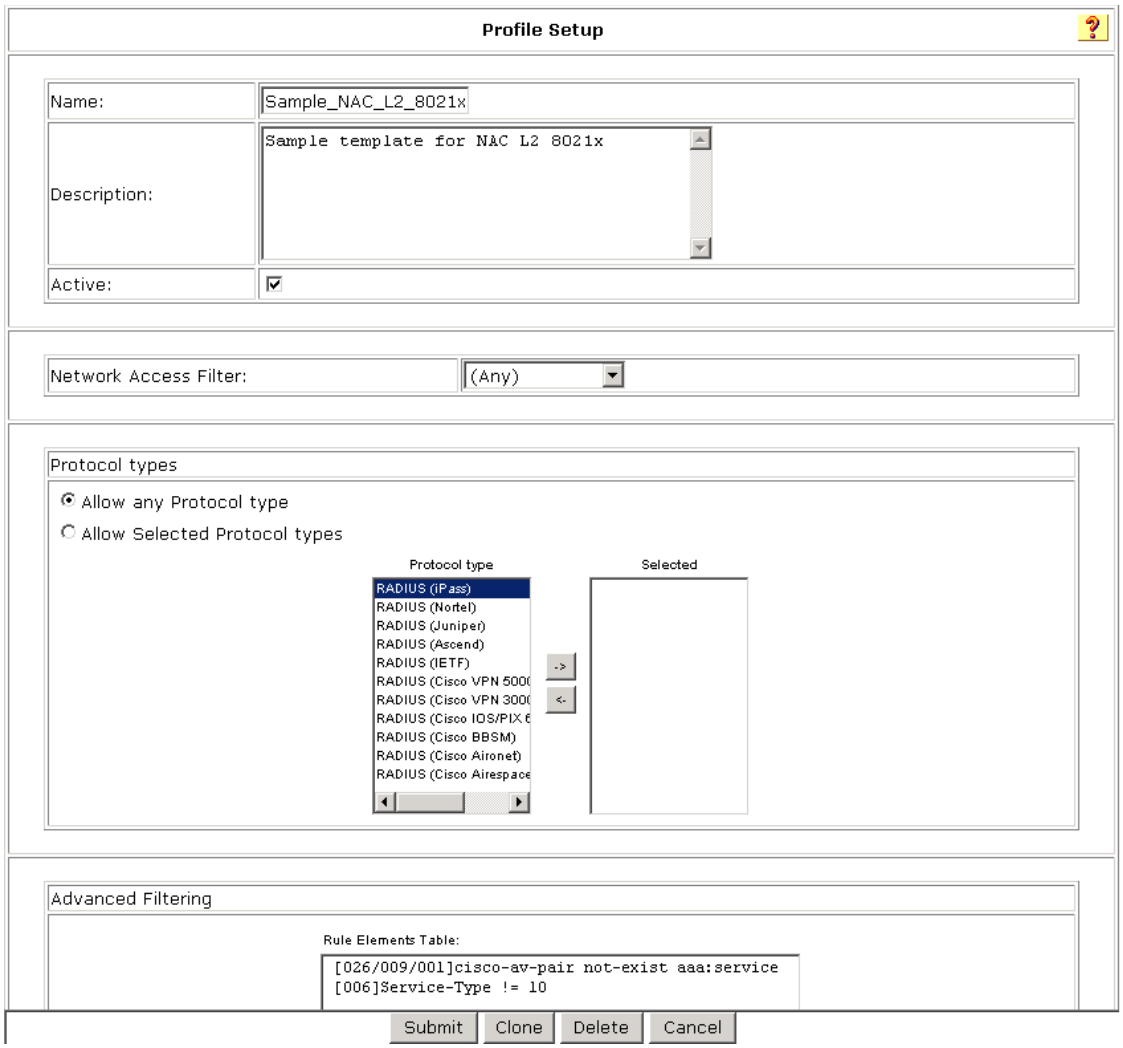
To use the Profile Setup settings from the template:

Step 1 In the navigation bar, click **Network Access Profiles**.

Step 2 Choose the profile that you created.

Step 3 The Profile Setup page appears, as shown in Figure 7-30.

Figure 7-39 Profile Setup Page for NAC Layer 2 802.1x Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can select the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

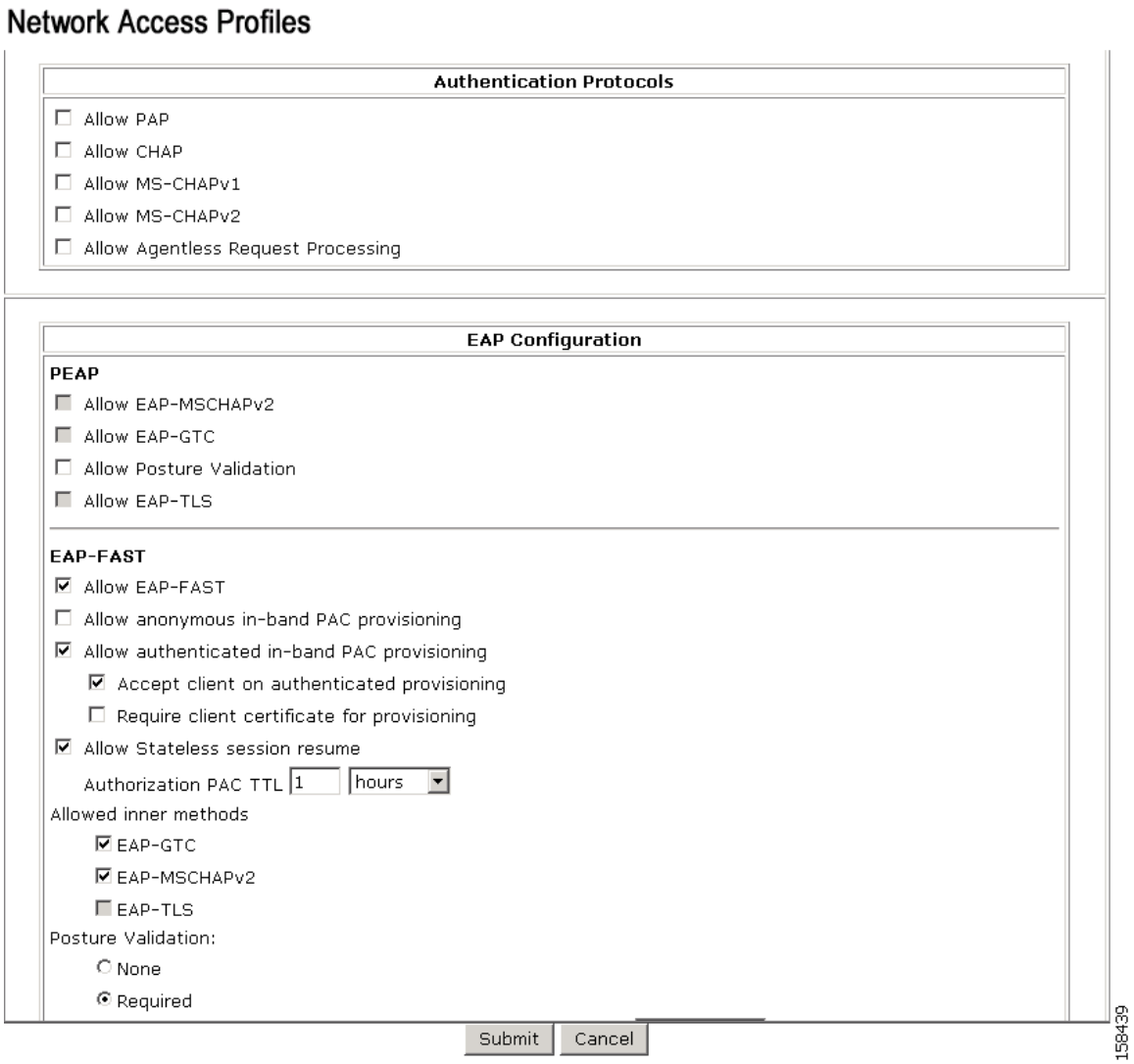
  ```
  [026/009/001]Cisco-av-pair = aaa:service=ip admission
  [006]Service-Type != 10
  ```

  These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

Protocols Policy

Figure 7-40 shows the Protocols settings for the NAC Layer 2 802.1x template.

Figure 7-40 Protocols Setting for NAC Layer 802.1x Template



In the EAP Configuration section, Posture Validation is enabled.

Authorization Policy

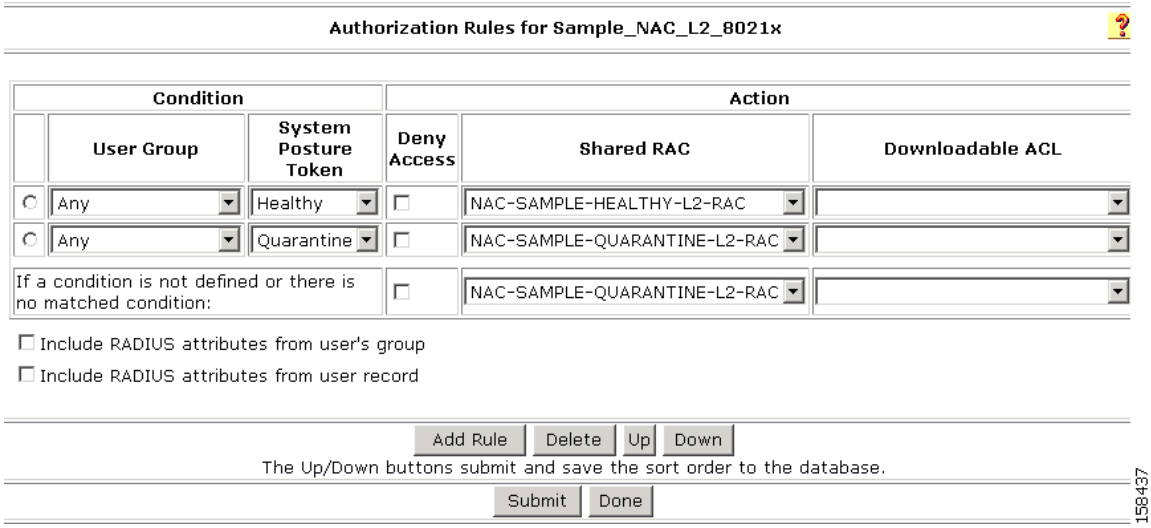
To configure an authorization policy for the NAC Layer 2 802.1x template:

Step 1 Go to **Network Access Profiles**.

Step 2 Choose the **Authorization** link from the Policies column.

The Authentication page for the NAC Layer 2 802.1x template profile appears, as shown in Figure 7-41.

Figure 7-41 Authentication Page for NAC Layer 2 802.1x Profile Template



On this page, you can see the Layer 2 NAC 802.1x template configuration for authorization.

Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

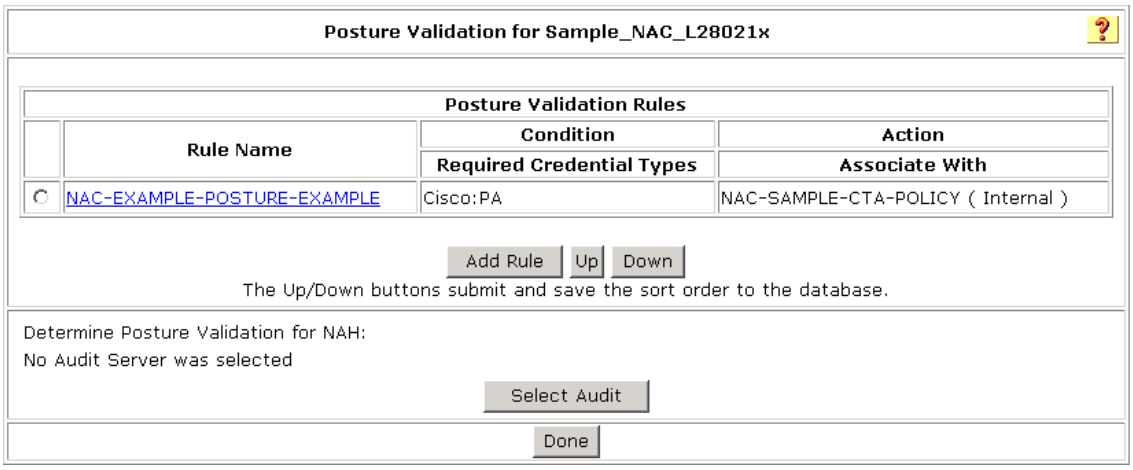
b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Sample Posture Validation Rule

Figure 7-42 shows the sample posture validation policy provided with the NAC Layer 2 802.1x template.

Figure 7-42 Sample Posture Validation Policy for NAC Layer 2 802.1x Template



Sample Wireless (NAC L2 802.1x) Template

This template creates a profile for Layer 2 NAC 802.1x requests in wireless networks. Before you use this template, you should choose **System Configuration > Global Authentication Setup** and check the **Enable Posture Validation** check box**.**

To create a wireless (NAC L2 802.1x) NAC profile template:

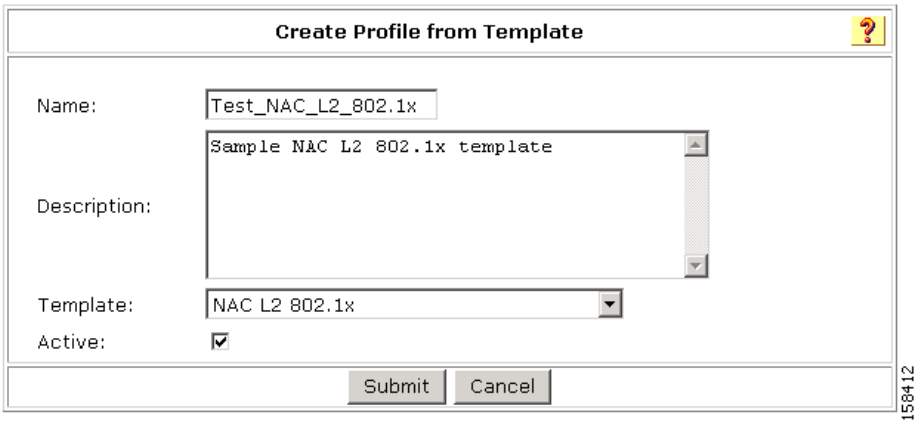
Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 2 Click **Add Template Profile**.

The Create Profile from Template page opens, as shown in Figure 7-43.

Figure 7-43 Create Profile From Template Page



Step 3 Enter a Name and Description (optional).

Step 4 From the Template drop-down list, choose **Wireless (NAC L2 802.1x)**.

Step 5 Check the **Active** check box.

Step 6 Click **Submit**.

If no error appears, then you have created a Profile that can authenticate wireless NAC Layer 2 802.1x hosts.

The Edit Network Access Profile page opens, and the new profile is listed in the Name column.

The predefined values for the NAC Layer 2 802.1x template include:

- Profile Setup
- Protocols
- A sample posture validation policy
- Authentication policy

Step 7 To select a predefined set of values, click on one of the configuration options:

- The profile name (to select the profile setup page for the profile)
- Protocols
- Authentication Policy
- Sample Posture Validation Rules

Profile Setup

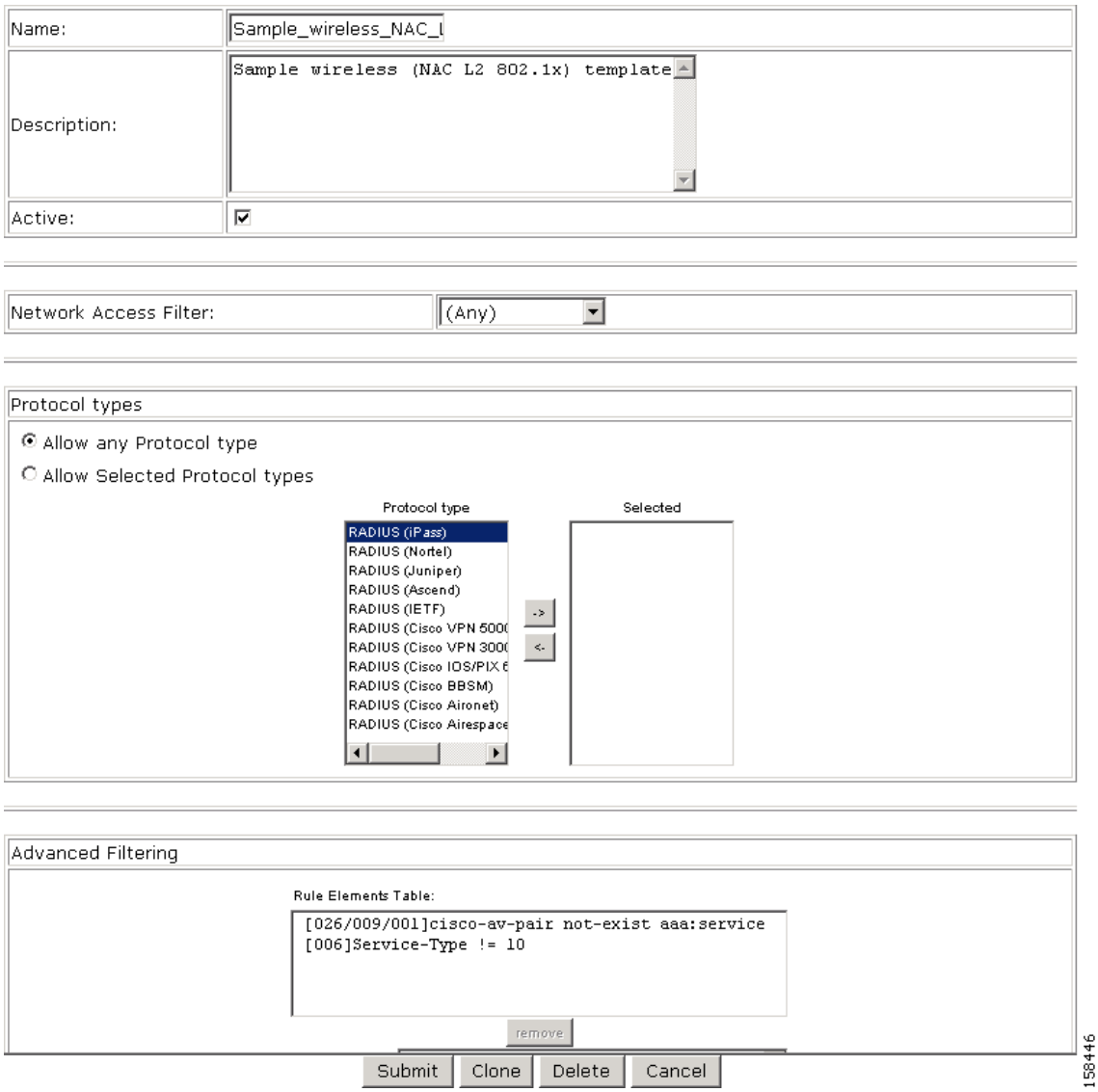
To use the Profile Setup settings from the template:

Step 1 Go to Network Access Profiles.

Step 2 Choose the profile that you created.

Step 3 The Profile Setup page appears, as shown in Figure 7-44.

Figure 7-44 Profile Setup Page for Wireless (NAC L2 802.1x)Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- In the Protocol types list, **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can click the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

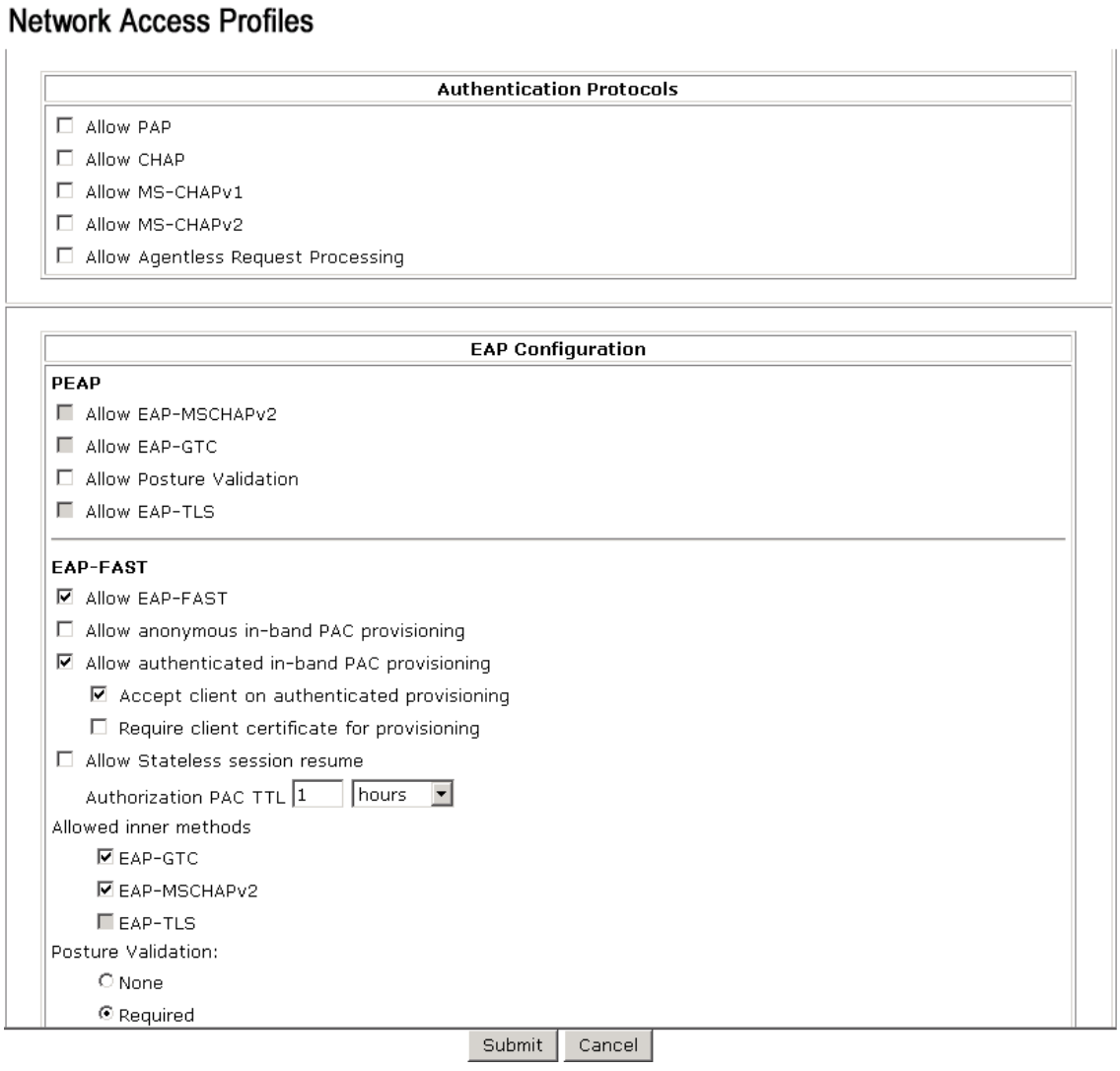
```
[026/009/001]Cisco-av-pair = aaa:service=ip admission
[006]Service-Type != 10
```

These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

Protocols Policy

Figure 7-45 shows the Protocols settings for the Wireless (NAC L2 802.1x) template.

Figure 7-45 Protocols Setting for Wireless NAC 802.1x Template



In the EAP Configuration section, Posture Validation is enabled.

Authorization Policy

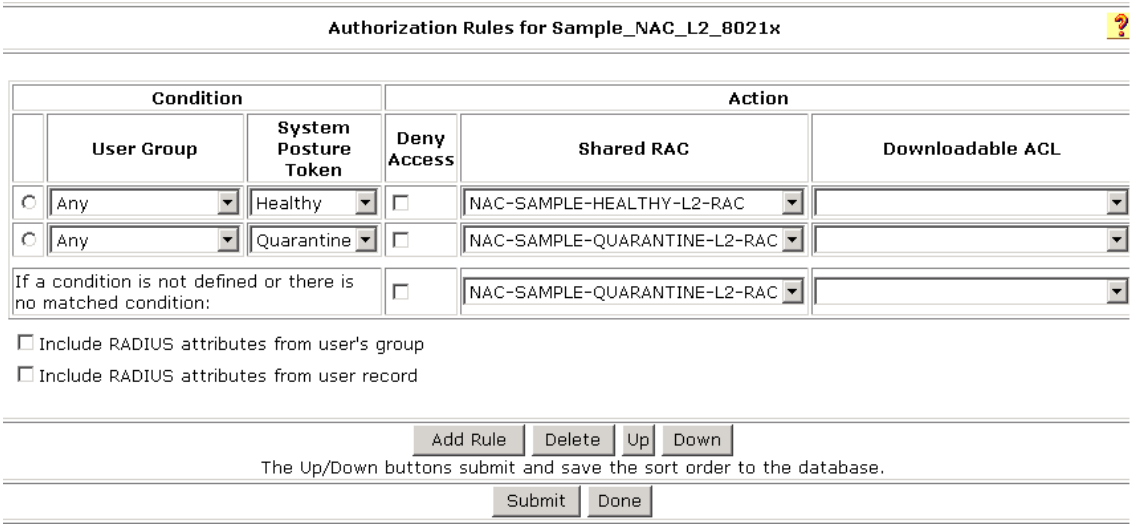
To configure an authorization policy for the Wireless NAC Layer 2 802.1x template:

Step 1 Go to **Network Access Profiles**.

Step 2 Choose the **Authorization** link from the Policies column.

The Authentication page for the profile appears, as shown in Figure 7-46.

Figure 7-46 Authorization Page for Wireless (NAC L2 802.1x) Profile Template



On this page, you can see the Wireless (NAC L2 802.1x) template configuration for authentication:

Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

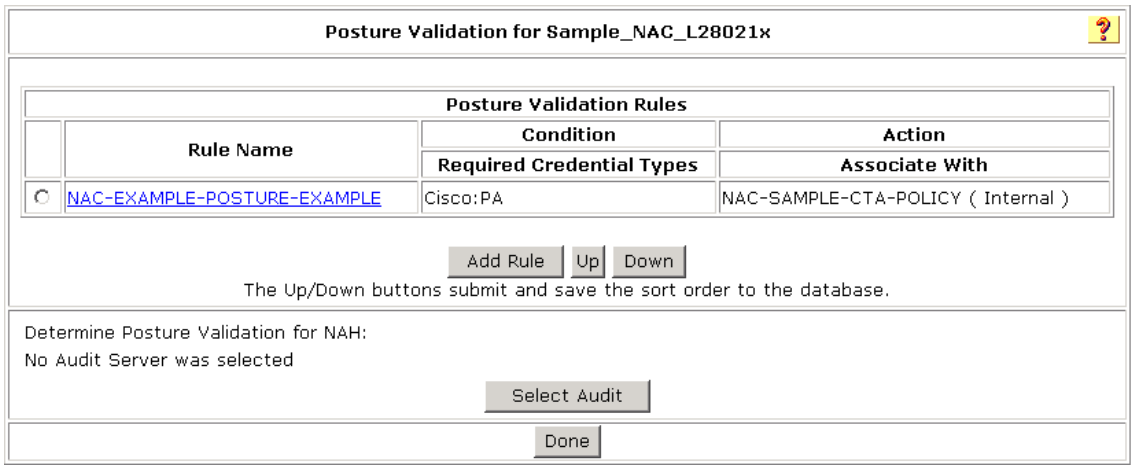
b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Sample Posture Validation Rule

Figure 7-47 shows the sample posture validation policy provided with the Wireless (NAC L2 802.1x) template.

Figure 7-47 Sample Posture Validation Policy for Wireless (NAC L2 802.1x) Template



Note The posture validation policy for the wireless NAC L2 802.1x template is the same as for the NAC L2 802.1x template.

Using a Sample Agentless Host Template

ACS 4.1 provides two sample templates for agentless host processing:

- Agentless Host for L3
- Agentless Host for L2 (802.1x fallback)

These two templates are almost identical. This section documents the steps for using the Agentless Host for Layer 3 template.

Note You can use the Agentless Host for L2 (802.1x Fallback) profile template to create a profile that matches a RADIUS request a switch sends. 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 (AV pair) that contains the keyword `service`. Therefore, the template enables two entries in the Advanced Filtering section.

The Agentless Host for Layer 3 template creates a profile for Layer 3 requests that involve agentless host processing. Before you use this template, you should choose **System Configuration > Global Authentication Setup** and check the **Enable Posture Validation** check box**.**

To create an agentless host for Layer 3 profile template:

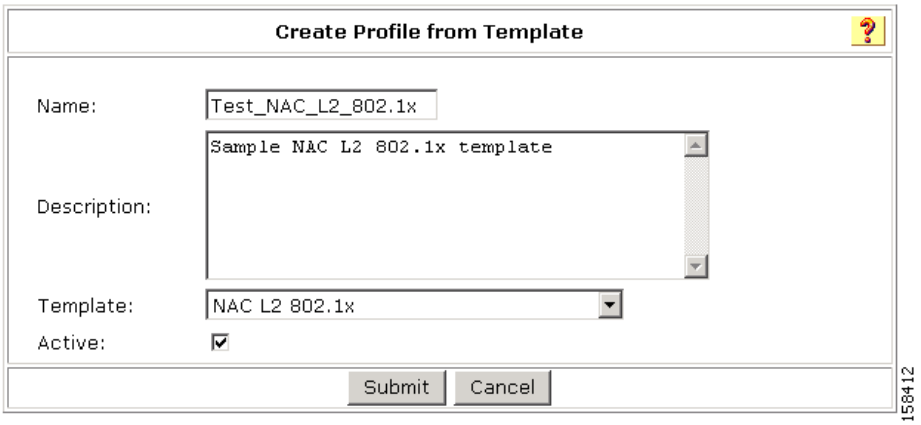
Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 2 Click **Add Template Profile**.

The Create Profile from Template page opens, as shown in Figure 7-48.

Figure 7-48 Create Profile From Template Page



Step 3 Enter a Name and Description (optional).

Step 4 From the **Template** drop-down list, choose **Agentless Host for L3**.

Step 5 Check the **Active** check box.

Step 6 Click **Submit**.

If no error appears, then you have created a profile that can authenticate Layer 3 NAC hosts.

The Edit Network Access Profile page opens, and the new profile is listed in the Name column.

The predefined values for the Agentless Host for Layer 3 template include:

- Profile Setup
- Protocols
- A sample posture validation policy
- Authentication policy

Step 7 To select a predefined set of values, click on one of the configuration options.

- The profile name (to select the profile setup page for the profile)
- Protocols
- Authentication Policy
- Sample Posture Validation Rules

Profile Setup

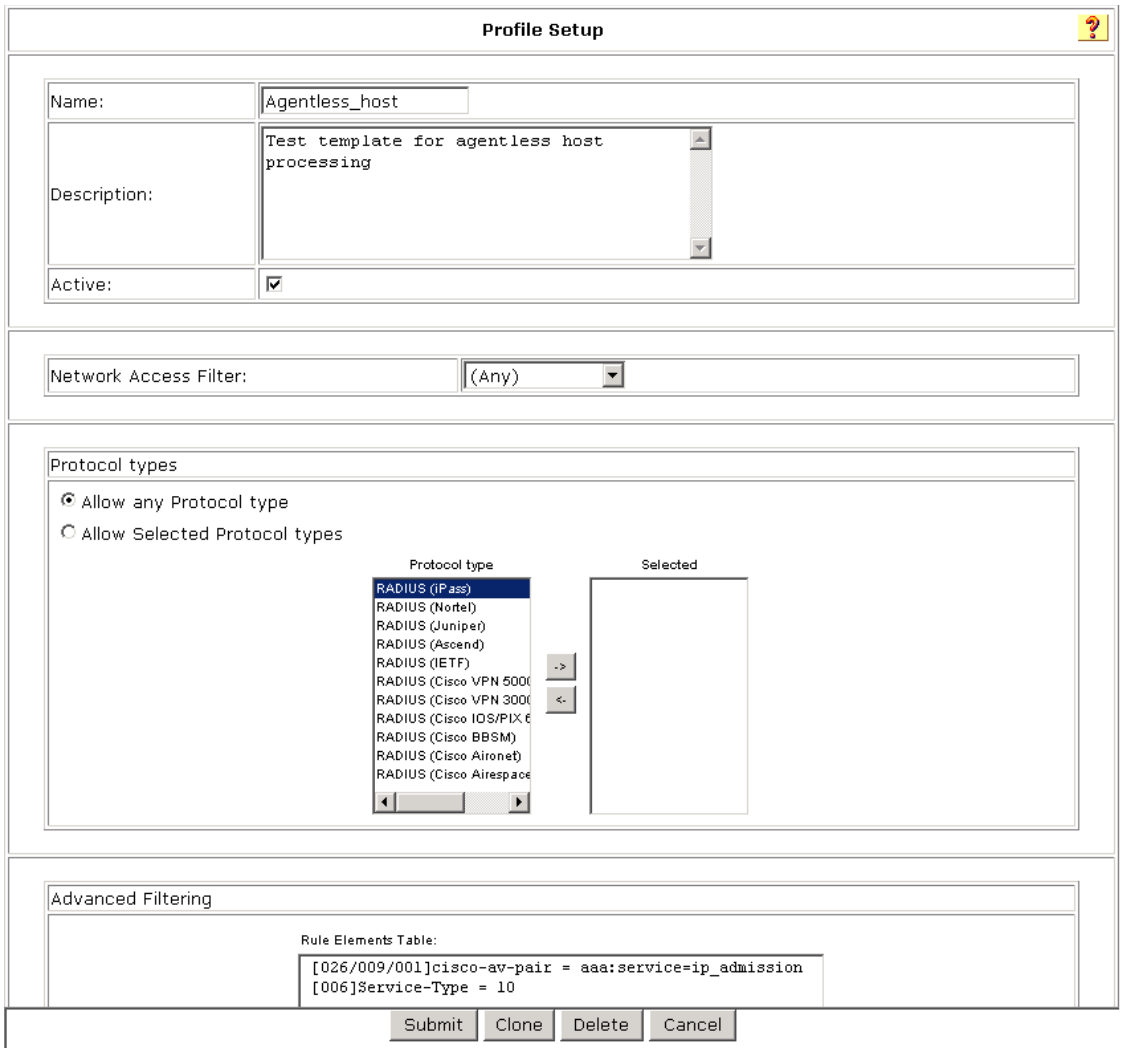
To use the Profile Setup settings from the template:

Step 1 Go to Network Access Profiles.

Step 2 Choose the profile that you created.

Step 3 The Profile Setup page appears, as shown in Figure 7-49.

Figure 7-49 Profile Setup Page for Agentless Host for Layer 3 Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- In the Protocol types list, **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can click the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

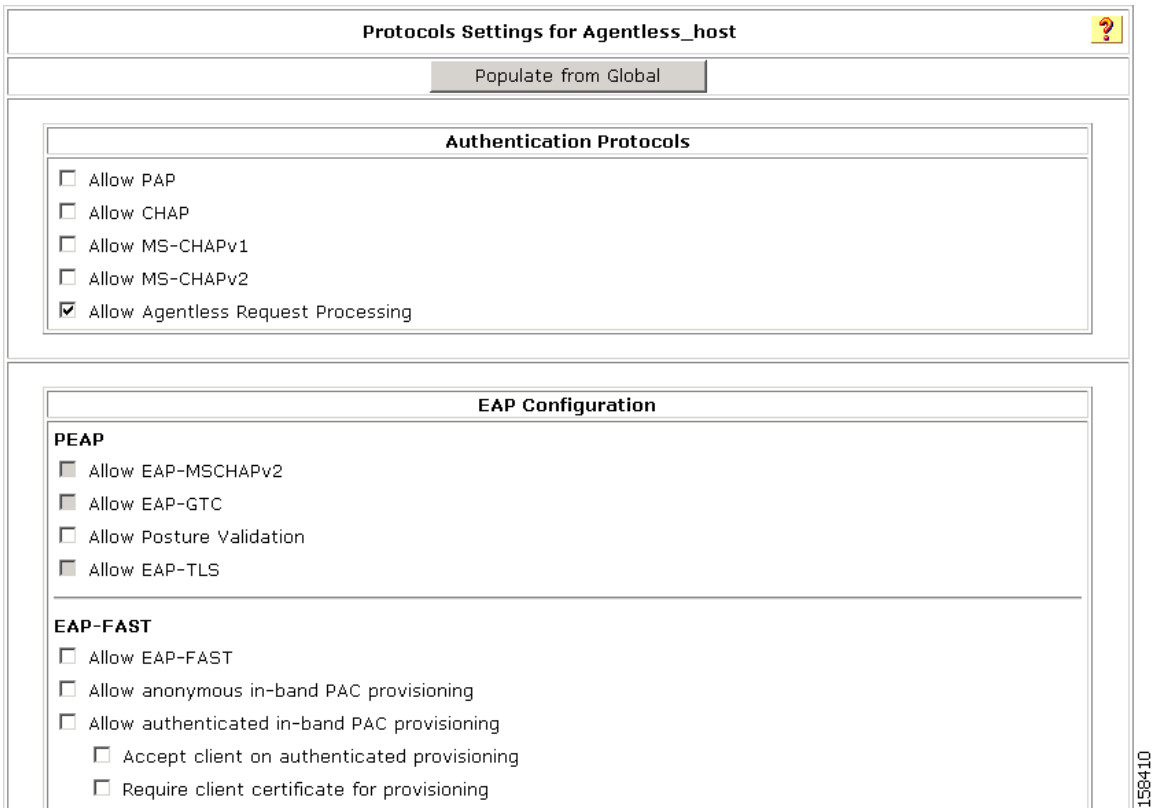
  ```
  [026/009/001]Cisco-av-pair = aaa:service=ip admission
  [006]Service-Type != 10
  ```

  These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

Protocols Policy

Figure 7-50 shows the Protocols settings for the Agentless Host for Layer 3 template.

Figure 7-50 Protocols Setting for Agentless Host for Layer 3 Template



In the Authentication Protocols section, check Agentless Host processing.

Authentication Policy

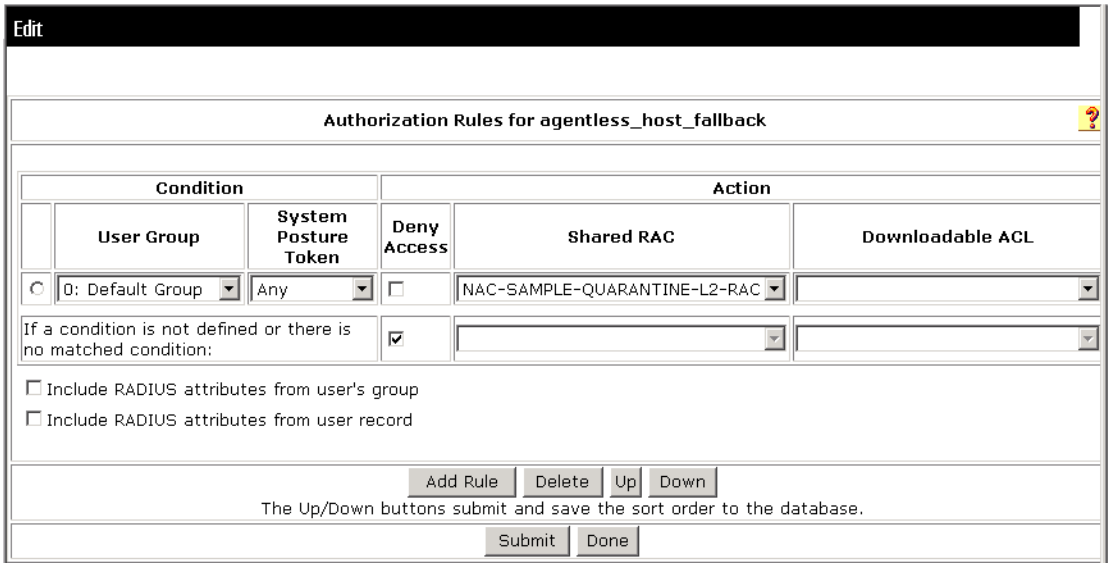
To configure an authentication policy for the Agentless Host for Layer 3 template:

Step 1 Go to **Network Access Profiles**.

Step 2 Choose the **Authentication** link from the Policies column.

The Authentication page for the profile appears, as shown in Figure 7-51.

Figure 7-51 Authentication Page for Agentless Host for Layer 3 Profile Template



On this page, you can see the Agentless Host for Layer 3 template configuration for authentication:

Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Step 15: Map Posture Validation Components to Profiles

To add an internal posture validation policy, external posture validation server, or both, to a profile:

Step 1 Choose **Network Access Profiles**.

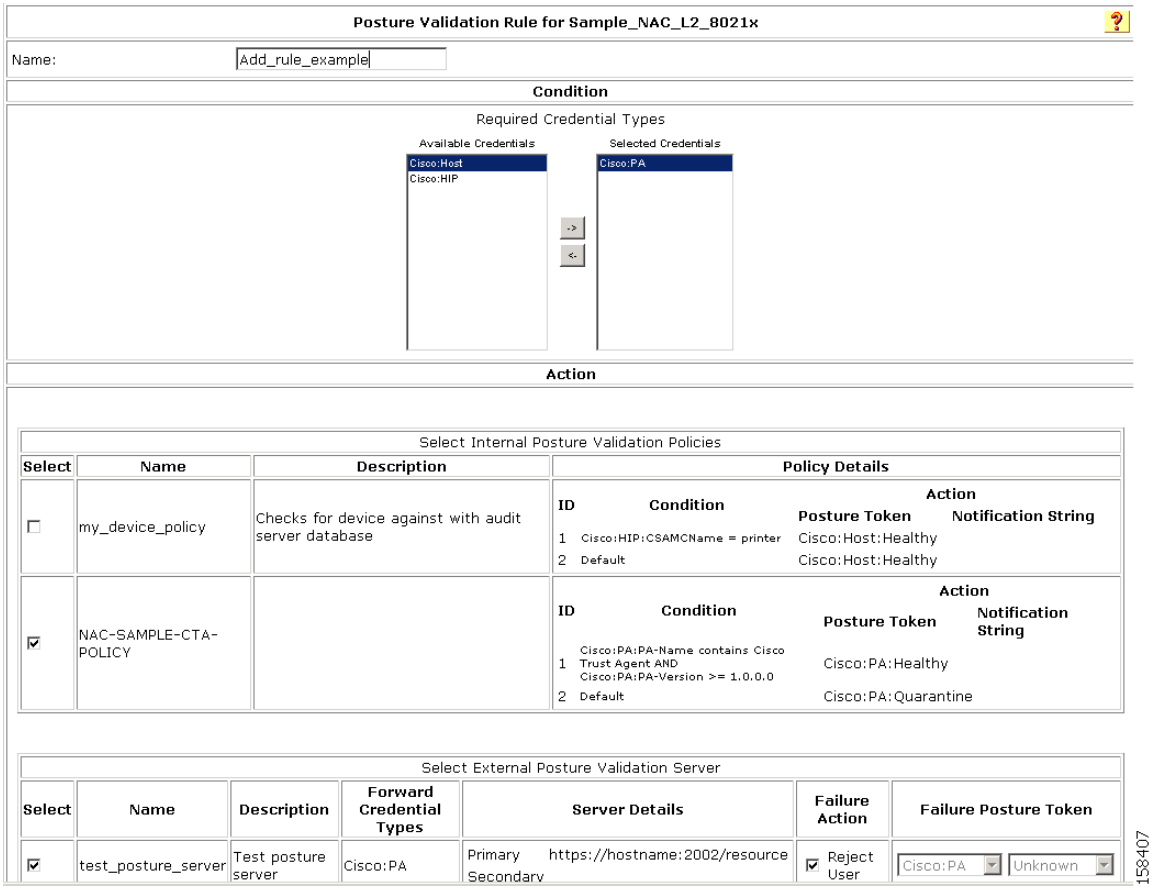
Step 2 Choose the relevant profile **Posture Validation** policy.

Step 3 Click **Add Rule**.

Step 4 Enter a Name for the rule.

The Add/Edit Posture Validation Rule page for the specified rule appears, as shown in Figure 7-52.

Figure 7-52 Add/Edit Posture Validation Rule Page



Step 5 Choose the Required Credential Types.

Step 6 In the Select External Posture Validation Sever section, select the policies or server that you want to map to this profile. To select a:

- Posture Server, check the check box next to the server name.
- Policy, check the check box next to a policy in the Failure Action column.

Step 7 Click **Submit**.

Step 8 Click **Back** to return to the Posture Validation policy.

Step 9 Click **Apply + Restart**.

Step 16: Map an Audit Server to a Profile

To add an external posture validation audit server to a profile:

Step 1 Choose **Network Access Profiles**.

Step 2 Click the **Protocols** link for the relevant Posture Validation Policy.

The Protocols Settings page for the selected policy opens.

Step 3 Check the **Allow Agentless Request Processing** check box.

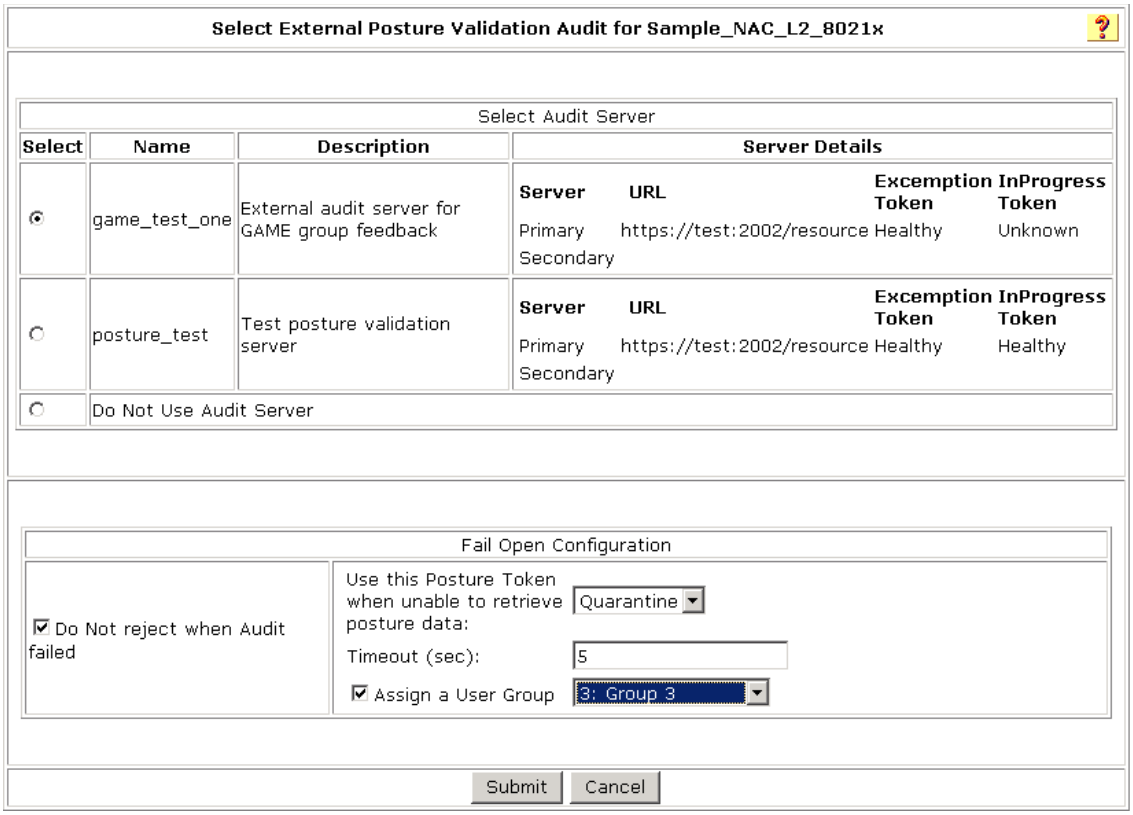
Step 4 Click **Submit**.

Step 5 Click the Posture Validation link for the relevant profile Posture Validation policy.

Step 6 Click **Select Audit**.

The Select External Posture Validation Audit Server page opens, as shown in Figure 7-53.

Figure 7-53 Select External Validation Audit Server Page



Step 7 Select the audit server to use.

Step 8 To specify a Fail Open configuration to use if the audit fails:

a. Check the **Do not reject when Audit failed** check box.

b. From the **Use this Posture Token when unable to retrieve posture data** drop-down list, choose a posture token to apply if the audit fails.

c. Enter a timeout value in seconds.

d. If you want to specify a user group to which to assign the supplicant if the audit fails, check the **Assign a User Group** check box and then from the **Assign a User Group** drop-down list, choose a user group.

Step 9 Click **Submit**.

Step 10 Click **Done.**

Step 11 Click **Apply and Restart**.

Step 17 (Optional): Configure GAME Group Feedback

If you are using ACS in a NAC environment with agentless hosts, then you must configure GAME group feedback.

To configure GAME group feedback:

Step 1 Import an audit vendor file by using **CSUtil.exe**.

See Import an Audit Vendor file Using CSUtil, page 7-67 for details.

Step 2 Import a device-type attribute file by using **CSUtil.exe**.

See Import a Device-Type Attribute File Using CSUtil, page 7-67 for details.

Step 3 Import NAC attribute-value pairs.

See Import NAC Attribute-Value Pairs, page 7-67 for details.

Step 4 Configure database support for agentless host processing.

The database that you use can be an external LDAP database (preferred) or the ACS internal database. See Configure Database Support for Agentless Host Processing, page 7-68 for details.

Step 5 Enable Posture Validation.

See Enable Posture Validation, page 7-68 for details.

Step 6 Configure an external audit server.

See Configure an External Audit Server, page 7-68 for details.

Step 7 Enable GAME Group feedback.

To enable GAME Group feedback, in the external audit server posture validation setup section, configure:

- Which hosts are audited
- GAME group feedback
- Device-type retrieval and mapping for vendors who have a device attribute in the RADIUS dictionary

See Enable GAME Group Feedback, page 7-68 for details.

Step 8 Set up a device group policy.

See Enable GAME Group Feedback, page 7-68 for details.

Import an Audit Vendor file Using CSUtil

For information on importing an audit vendor file by using **CSUtil.exe**, see the "Adding a Custom RADIUS Vendor and VSA Set" section in Appendix D of the User Guide for Cisco Secure Access Control Server 4.1, "*CSUtil Database Utility*."

Import a Device-Type Attribute File Using CSUtil

Before you can configure GAME group feedback, you must import an attribute file that contains a **device-type** attribute.

The format of a text file to set up a device-type attributes is:

```
[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
atribute-type=string
```

To import the file:

Step 1 Save the text file that sets up the device-type attribute in an appropriate directory.

Step 2 Open a DOS command window.

Step 3 Enter:

`CSUtil -addAVP <`*`device-type filename`*`>`

where *device-type filename* is the name of the text file that contains the device-type attribute.

Step 4 Restart ACS:

a. In the navigation bar, click **System Configuration**.

b. Click **Service Control**.

c. Click **Restart**.

Import NAC Attribute-Value Pairs

To import NAC attribute-value pairs:

Step 1 Obtain a NAC attribute-value pairs file.

Step 2 Import the file by using **CSUtil.exe**.

a. Start a DOS command window.

b. Enter:

`CSUtil -addAVP <`*`NAC AV-pair filename`*`>`

where *`NAC AV-pair filename`* is the name of the text file that contains the device-type attribute.

Step 3 Restart ACS:

a. In the navigation bar, click **System Configuration**.

b. Click **Service Control**.

c. Click **Restart**.

Configure Database Support for Agentless Host Processing

The database that you use can be an external LDAP database (preferred) or the ACS internal database.

For information on configuring database support for agentless host processing, see Step 4: Configure LDAP Support for MAB, page 4-9 in Chapter 4, "Agentless Host Support Configuration Scenario".

Enable Posture Validation

You must enable posture validation in two places. In the:

- Global Authentication Page, as part of the configuration for PEAP.
- EAP configuration section of the Protocols page for the Network Access Profile that enables agentless host support.

Configure an External Audit Server

For detailed instructions on configuring an external audit server, see Configure an External Posture Validation Audit Server, page 7-34.

Enable GAME Group Feedback

To enable GAME Group feedback:

Step 1 On the External Posture Validation Audit Server Setup page, in the GAME Group Feedback section, check the **Request Device Type from Audit Server** check box.

If this check box is not available, define an audit device type attribute for the vendor in the internal ACS dictionary.

ACS for Windows:

With ACS for Windows, you use the **CSUtil.exe** command. For detailed information, see "Posture Validation Attributes" in Appendix D of the *User Guide for Cisco Secure ACS*.

ACS Solution Engine:

With ACS Solution Engine, you use the NAC Attributes Management page in the web interface. See "NAC Attribute Management (ACS Solution Engine Only)" in Chapter 8 of the *User Guide for Cisco Secure ACS* for more information.

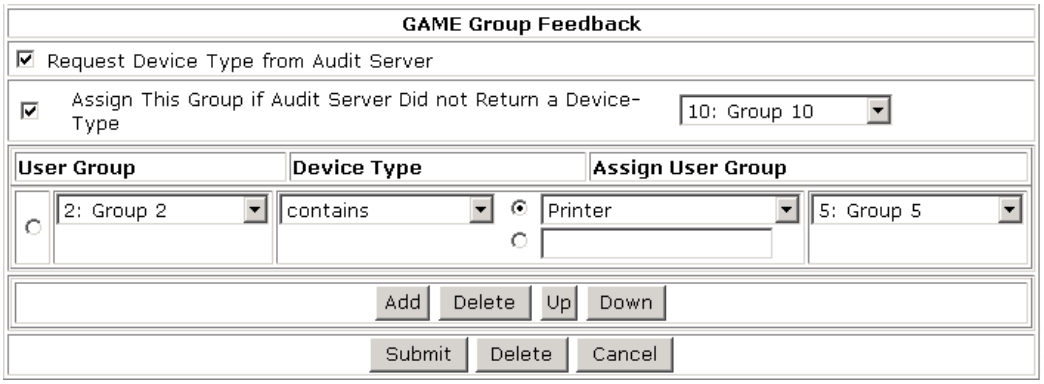
Step 2 If you want to configure a default destination group that ACS uses if the audit server does not return a device type, check the **Assign This Group if Audit Server Did not Return a Device-Type** check box.

You should now add entries to the group assignment table. The group assignment table is a list of rules that set conditions that determine the user group to which to assign a particular device type that is returned from the audit server.

Step 3 Click **Add** to display the group assignment table and add a device-type feedback rule.

The group assignment table appears, as shown in Figure 7-54.

Figure 7-54 GAME Group Feedback Section with Group Assignment Table



Step 4 Specify the following in the group assignment table:

- **User Group**—Lists all user groups, including **Any**. The device type that the MAC authentication returns is initially compared with this list of device types.
- **Match Condition**—Valid values for the operator are:
  - match-all
  - =
  - ! =
  - contains
  - starts-with
  - regular-expression
- **Device Type**—Defines the comparison criteria for the User Group by using an operator and device type. Valid values for the device type drop-down list include:
  - Printer
  - IP Phone
  - Network Infrastructure
  - Wireless Access Point
  - Windows
  - UNIX
  - Mac
  - Integrated Device

- PDA
- Unknown

Note Type a device type in the text box if the device type drop-down does list not contain a particular device.

- **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.

Step 5 To add additional policies, click **Add**.

Step 6 To delete a policy, select the policy and click **Delete**.

Step 7 To move the policies up and down in the group assignment table, click the **Up** and **Down** buttons.

Step 8 When you finish setting up policies for group assignment, click **Submit**.

Step 9 Click **Apply and Restart.**

GLOSSARY

A

AAA — Authentication, Authorization, and Accounting server.-(Authentication, authorization, and accounting is pronounced “triple-A.” An AAA server is the central server that aggregates one or more authentication, authorization, or both decisions into a single system-authorization decision, and maps this decision to a network-access profile for enforcement on the NAD.

Access -Accept — Response packet from the RADIUS server notifying the access server that the user is authenticated. This packet contains the user profile, which defines the specific AAA functions assigned to the user.

Access-Challenge — Response packet from the RADIUS server requesting that the user supply additional information before being authenticated.

Access-Request — Request packet that the access server sends to the RADIUS server requesting authentication of the user.

Accounting — Accounting in network management subsystems is responsible for collecting network data relating to resource usage.

Agentless host processing — A method that ACS uses to process authentication requests from hosts that do not have an authentication agent installed, such as Cisco Trust Agent.

ACL — Access Control List-Each ACL consists of a set of ACL entries.

ACE — Access Control Entry-An ACL Entry contains a type, a qualifier for the user or group to which the entry refers, and a set of permissions. For some entry types, the qualifier for the group or users is undefined.

APT — Application Posture Token-The result of a posture validation check for a given vendor’s application.

Audit server — A server that can determine the posture credentials of a host without relying on the presence of a PA on the host. The server must be able to determine the posture credentials of a host and act as a posture-validation server.

Authentication — In network management security, the verification of the identity of a person or a process.

AV pair — Attribute-value pair-Encoding that the RADIUS protocol uses to specify an action that the host performs when a condition represented by the attribute value is met.

C

Cisco Trust Agent — Cisco Trust Agent. The Cisco implementation of the PA.

E

EAP Extensible Authentication Protocol-Provides the ability to deploy RADIUS into Ethernet network environments. EAP is defined by Internet Engineering Task Force (IETF) RFC 2284 and the IEEE 802.1x standards.

EAP-TLS Extensible Authentication Protocol-Transport Layer Security-Uses the TLS protocol (RFC 2246), which is the latest version of the Secure Socket Layer (SSL) protocol from the IETF. TLS provides a way to use certificates for user and server authentication and for dynamic session key generation.

Endpoint Device Any machine that attempts to connect to or use the resources of a network. Also referred to as a host.

External Posture Validation Server A Cisco or third-party server used to perform posture validation. A posture-validation server acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules.

G

GAME group feedback Generic Authorization Message Exchange-A Cisco protocol that is used in the Cisco Network Admission Control (NAC) environment. GAME group feedback provides an added security check for MAC address authentication by checking the device type categorization that ACS determines by associating a MAC address with a user group against information stored in a database on an audit server

H

Host Another name for an endpoint device.

L

LDAP Lightweight Directory Access Protocol-A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler.

M

MAB MAC authentication bypass-An authentication method that uses the MAC address of a device to authenticate the device, instead of using an IP address.

N

NAC Network Admission Control-NAC is a Cisco-sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources; thereby limiting damage from viruses and worms. NAC is part of the Cisco Self-Defending Network, an initiative to increase network intelligence in order to enable the network to automatically identify, prevent, and adapt to security threats.

NAC-compliant applications Applications that integrate with the NAC client. Examples of such applications are Cisco Security Agent and antivirus programs that provide the NAC client with attributes about themselves, such as the version number of a virus definition file.

NAD Network Access Device-A network access device acts as a policy-enforcement point for the authorized network-access privileges that are granted to a host.

NAF Network Access Filter-A NAF is a named group of any combination of one or more of the following network elements: IP addresses, AAA clients (network devices), and network device groups (NDGs).

Using a NAF to specify a downloadable IP ACL or Network Access Restriction based on the AAA clients by whom the user may access the network saves you the effort of listing each AAA client explicitly.

NDG Network Device Group-A collection of network devices that act as a single logical group.

NRH Nonresponsive host-A host that does not have the Cisco Trust Agent installed to perform posture validation. An NRH is also known as a “agentless” host.

P

PA Posture Agent-An application that serves as the single point of contact on the host for aggregating posture credentials from potentially multiple posture plug-ins and communicating with the network.

PDP Policy Decision Point-Provides facilities for policy management and conditional filters.

PEP Policy Enforcement Point-ACS acts as the policy enforcement point for policy management.

PEAP Protected Extensible Authentication Protocol-An 802.1x authentication type for wireless LANs (WLANs). PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging. PEAP is based on an Internet Draft that Cisco Systems, Microsoft, and RSA Security submitted to the IETF.

Posture credentials State information of a network endpoint at a given point in time that represents hardware and software (OS and application) information.

Posture plug-in A third-party DLL that provides host posture credentials to a posture agent on the same endpoint for endpoint posture validation and network authorization.

PV Posture Validation-Posture validation validates the collection of attributes that describe the general state and health of the user’s machine (the “host”).

PVS Posture Validation Server-A posture-validation server acts as an application-specific policy-decision point in NAC for authorizing a set of posture credentials against a set of policy rules.

Posture validation The authorization of a network endpoint's posture credentials by one or more posture-validation servers and their associated compliance policies.

R

RAC RADIUS Attribute Component.

RADIUS A widely deployed protocol enabling centralized authentication, authorization, and accounting for network access.

V

VSA Vendor Specific Attribute-Most vendors use the VSA to support value-added features.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W