CACS

Primer Introduction

Overview

This document, *ACS 4.0 Primer,* has been designed and created for use by customers as well as network engineers. It is designed to provide a primer to the Cisco Secure Access Control Server (ACS), version 4.0.

Learner Skills and Knowledge

To benefit fully from the primer, you should have an understanding of Authentication, Authorization, and Accounting (AAA) services, as used in the context of information security. You should also have knowledge of the material covered in the following Cisco curricula:

- Securing Cisco IOS Networks (SECUR)

- Cisco Secure PIX Firewall Advanced (CSPFA)

- Building Cisco Remote Access Networks (BCRAN)

Primer Goal and Objective

The purpose of this primer is to act as an introduction to the ACS product.

Upon completing this primer, you will be familiar with the ACS product and its major features.

Primer Flow

This primer covers the following major topics:

1. Getting Familiar with ACS

2. ACS Databases and Additional Server Interaction

3. ACS Authentication and NAD Interactions

4. Configuring Network Access Profiles

5. Troubleshooting ACS

Cisco Glossary of Terms

For additional information on Cisco terminology, refer to the *Cisco Internetworking Terms and Acronyms* glossary of terms at www.cisco.com/univercd/cc/td/doc/cisintwk/ita/.

Module 1

Getting Familiar with ACS

Overview

This module discusses the ACS server installation and customization process. In this module, you will learn the requirements for installing ACS on a Windows platform as well as how to navigate through the ACS interface and perform some basic customization tasks.

Module Objectives

Upon completion of this module, you will be able to install and customize ACS. This ability includes being able to meet these objectives:

- Determine which ACS product is right for your network
- Install ACS
- Customize ACS

Lesson 1

ACS Specifications and Installation

Overview

Cisco Secure Access Control Server (ACS) for Windows provides a centralized identity networking solution and simplified user management experience across all Cisco devices and security management applications. Cisco Secure ACS helps to ensure enforcement of assigned policies by allowing network administrators to control who can log into the network, the privileges a user has on the network, document security audits or account billing information, and access and command controls that are enabled for each configuration administrator. This lesson discusses what ACS is and what it can be used for, the requirements for installing ACS on Windows, and the ACS installation procedure.

Objectives

Upon completing this lesson, you will be able to determine what ACS is and where it fits into your network, as well as understand the installation requirements and the basic protocol functions of ACS. This ability includes being able to meet these objectives:

- Identify Cisco Secure ACS and where it fits into your network

- Understand the differences between Cisco Secure ACS on a software platform and on an appliance

- Identify the installation requirements for Cisco Secure ACS

- Install Cisco Secure ACS on Windows

What is ACS?

This topic describes what ACS is and identifies where it fits into a network.

Cisco Secure ACS is a main part of a Cisco trust and identity networking security solution. It extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework, allowing greater flexibility and mobility, increased security, and user productivity gains.

With Cisco Secure ACS, you can manage and administer user access for Cisco IOS routers, VPNs, firewalls, dialup and DSL connections, cable access solutions, storage, content, Voice over IP (VoIP), Cisco wireless solutions, and Cisco Catalyst switches using IEEE 802.1x access control.

Advanced features of Cisco Secure ACS include:

- Automatic service monitoring, database synchronization, and importing of tools for large-scale deployments

- Lightweight Directory Access Protocol (LDAP) and Open Database Connectivity (ODBC) user authentication support

- Flexible 802.1x authentication type support, including Extensible Authentication Protocol Transport Layer Security (EAP-TLS), Protected EAP (PEAP), Cisco LEAP, EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), and EAP-Message Digest Algorithm 5 (EAP-MD5)

- Downloadable access control lists for any Layer 3 device, including Cisco routers, Cisco PIX® firewalls, and Cisco VPNs

- Device command set authorization

- Network access restrictions

- User and administrative access reporting

- Dynamic quota generation

- Access restrictions such as time of day and day of week

- User and device group profiles

- Network Access Profiles (provides the ability to process network access requests differently depending on characteristics of the request)

ACS Installation Requirements

The ACS server must meet certain minimum hardware, operating system, and third-party software requirements. Additionally, if you are upgrading from a previous version of Cisco Secure ACS, you should refer to Cisco Secure ACS Upgrade Requirements on Cisco.com.

Hardware Requirements

The server running Cisco Secure ACS must meet the following minimum hardware requirements:

- Pentium III processor, 1.8 GHz or faster.

- 1 GB of RAM.

- At least 500 MB to 1 GB of free disk space. If you are running the database on the same computer, more disk space is required.

- Minimum graphics resolution of 256 colors at 800x600 pixels.

Operating System Requirements

Cisco Secure ACS for Windows Servers 4.0 supports the Microsoft Windows operating systems listed below. Both the operating system and the service pack must be English-language versions.

- Windows 2000 Server, with Service Pack 4 installed

- Windows 2000 Advanced Server, with the following conditions:

  — Service Pack 4 installed

  — Without Microsoft clustering service installed

  — Without other features specific to Windows 2000 Advanced Server enabled, such as Terminal Services.

Note   The multi-processor feature of Windows 2000 Advanced Server has not yet been tested, and cannot be considered supported. Windows 2000 Data Center Server is not a supported operating system.

- Windows Server 2003 Enterprise Edition

- Windows Server 2003 Standard Edition

The Windows service packs can be applied before or after installing Cisco Secure ACS. If you do not install a required service pack before installing Cisco Secure ACS, the Cisco Secure ACS installation program may warn you that the required service pack is not present. If you receive a service pack message, continue the installation, and then install the required service pack before starting user authentication with Cisco Secure ACS.

For the most recent information about supported operating systems and service packs, see the Cisco Secure ACS release notes found on Cisco.com.

Third-Party Software Requirements

The ACS release notes provide information about third-party software products that Cisco has tested with Cisco Secure ACS and that Cisco supports, including applications such as:

- Web browsers and Java virtual machines

- Novell NDS clients

- Token-card clients

Other than the software products described in the release notes, Cisco has not tested the interoperability of Cisco Secure ACS and other software products on the same computer. Cisco will only support interoperability issues of software products that are mentioned in the release notes. The most recent version of the ACS release notes is posted on Cisco.com.

Network and Port Requirements

The network should meet the following requirements before you begin deploying Cisco Secure ACS:

- For full TACACS+ and RADIUS support on Cisco IOS devices, Authentication, Authorization, and Accounting (AAA) clients must run Cisco IOS Release 11.2 or later.

- Cisco devices that are non-Cisco IOS AAA clients must be configured with TACACS+ and/or RADIUS.

- Dial-in, VPN, or wireless clients must be able to connect to the applicable AAA clients.

- The computer running Cisco Secure ACS must be able to reach all AAA clients using ping.

- Gateway devices between the Cisco Secure ACS and other network devices must permit communication over the ports needed to support the applicable feature or protocol.

- A supported web browser must be installed on the computer running Cisco Secure ACS. For the most recent information about tested browsers, see the release notes. The most recent version of the release notes is posted on Cisco.com.

- All network cards in the computer running Cisco Secure ACS must be enabled. If there is a disabled network card on the computer running Cisco Secure ACS, installing Cisco Secure ACS may proceed slowly due to delays caused by the Microsoft CryptoAPI.

- If you want Cisco Secure ACS to use the "Grant Dial-in Permission to User" feature in Windows when authorizing network users, this option must be selected in the Windows User Manager or Active Directory Users and Computers for the applicable user accounts.

Installing ACS

This topic describes how to install ACS. This course only covers new installations of the ACS product. For information on other scenarios, refer to Cisco.com. There you will find installation scenarios including:

- Reinstallation, preserving the Cisco Secure user database and Cisco Secure ACS configuration
- Reinstallation, overwriting the Cisco Secure user database and Cisco Secure ACS configuration
- Upgrade, preserving the Cisco Secure user database and Cisco Secure ACS configuration
- Upgrade, overwriting the Cisco Secure user database and Cisco Secure ACS configuration

New Installation

To install Cisco Secure ACS, follow these steps:

Step 1   Using a local administrator account, login to the computer on which you want to install Cisco Secure ACS.

Note	Only installations performed at the computer you are installing Cisco Secure ACS on are supported. Remote installations performed using Windows Terminal Services or products such as Virtual Network Computing (VNC), are not tested, and are not supported.

Step 2   Insert the Cisco Secure ACS CD into a CD-ROM drive on the computer.

If the CD-ROM drive supports the Windows autorun feature, the Cisco Secure ACS for Windows Server dialog box appears.

Note	If the computer does not have a required service pack installed, a dialog box appears. Windows service packs can be applied either before or after installing Cisco Secure ACS. You can continue with the installation, but the required service pack must be applied after the installation is complete; otherwise, Cisco Secure ACS may not function reliably.

Step 3   Do one of the following:

- If the Cisco Secure ACS for Windows Server dialog box appears, click **Install**.
- If the Cisco Secure ACS for Windows Server dialog box does not appear, run `setup.exe`, located in the root directory of the Cisco Secure ACS CD.

The Cisco Secure ACS Setup dialog box displays the software license agreement.

Step 4   Read the software license agreement. If you accept the software license agreement, click **Accept**.

The Welcome dialog box displays basic information about the setup program.

Step 5   After you have read the information in the Welcome dialog box, click **Next >**.

Step 6 The Before You Begin dialog box lists items that you must complete before continuing with the installation. If you have completed all items listed in the Before You Begin dialog box, check the corresponding box for each item, and click **Next** >.

Note	If you have not completed all items listed in the Before You Begin dialog box, click **Cancel**, and then click **Exit Setup**. After completing all items listed in the Before You Begin dialog box, restart the installation.

The Choose Destination Location dialog box appears. Under Destination Folder, the installation location appears. This is the drive and path where the setup program installs Cisco Secure ACS.

Step 7 If you want to change the installation location, follow these steps:

1. Click **Browse**. The Choose Folder dialog box appears. The Path box contains the installation location.

2. Change the installation location. You can either type the new location in the Path box or use the Drives and Directories lists to select a new drive and directory. The installation location must be on a drive local to the computer.

Note	Do not specify a path that contains a percent character, "%". If you do so, installation may appear to continue properly but will fail before it completes.

3. Click **OK**.

Note	If you specified a folder that does not exist, the setup program displays a dialog box to confirm the creation of the folder. To continue, click **Yes**.

In the Choose Destination Location dialog box, the new installation location appears under Destination Folder.

Step 8 Click **Next >**.

The Authentication Database Configuration dialog box lists options for authenticating users. You can authenticate with the CiscoSecure user database only, or also with a Windows user database.

Note	After you have installed Cisco Secure ACS, you can configure authentication support for all external user database types in addition to Windows user databases.

Step 9 If you want to authenticate users with the CiscoSecure user database only, choose the **Check the CiscoSecure ACS database only** option.

Step 10 If you want to authenticate users with a Windows Security Access Manager (SAM) user database or Active Directory user database in addition to the CiscoSecure user database, follow these steps:

1. Choose the **Also check the Windows User Database** option.

The **Yes, refer to "Grant dialin permission to user" setting** check-box becomes available.

Note	The **Yes, refer to "Grant dialin permission to user" setting** check-box applies to all forms of access controlled by Cisco Secure ACS, not just dial-in access. For example, a user accessing the network through a VPN tunnel is not dialing into a network access server; however, if the **Yes, refer to "Grant dialin permission to user" setting** box is checked, Cisco Secure ACS applies the Windows user dial-in permissions to determine whether to grant the user access to the network.

2. If you want to allow access to users who are authenticated by a Windows domain user database only when they have dial-in permission in their Windows account, check the **Yes, refer to "Grant dialin permission to user" setting** box.

Step 11 Click **Next >**.

The setup program installs Cisco Secure ACS and updates the Windows Registry.

The Advanced Options dialog box lists several features of Cisco Secure ACS that are not enabled by default. For more information about these features, see the *User Guide for Cisco Secure ACS for Windows Server*, version 4.0.

Note	The listed features appear in the Cisco Secure ACS HTML interface only if you enable them. After installation, you can enable or disable them on the Advanced Options page in the Interface Configuration section.

Step 12 For each feature you want to enable, check the corresponding box.

Step 13 Click **Next >**.

The Active Service Monitoring dialog box appears.

Note	After installation, you can configure active service monitoring features on the Active Service Management page in the System Configuration section.

Step 14 If you want Cisco Secure ACS to monitor user authentication services, check the **Enable Log-in Monitoring** box. From the Script to execute list, choose the option you want applied in the event of authentication service failure:

—**No Remedial Action:** Cisco Secure ACS will not run a script.

Note	This option is useful if you enable event mail notifications.

—**Reboot:** Cisco Secure ACS runs a script that reboots the computer that runs Cisco Secure ACS.

—**Restart All:** Cisco Secure ACS restarts all Cisco Secure ACS services.

—**Restart RADIUS/TACACS+:** Cisco Secure ACS restarts only the RADIUS and TACACS+ services.

Step 15 If you want Cisco Secure ACS to send an e-mail message when service monitoring detects an event, check the **Mail Notification** box.

Step 16   Click **Next >**.

The Database Encryption Password dialog box appears.

Note	The Database Encryption Password is encrypted and stored in the ACS registry. This password may have to be reused when critical problems arise and the database needs to be accessed manually. Keep this password at hand so that technical support can gain access to the database. The password can be changed each expiration period.

Step 17   Enter a password for database encryption. The password should be at least 8 characters long and should contain both characters and digits. There are no invalid characters. Click **Next >**:

The setup program finishes and the Cisco Secure ACS Service Initiation dialog box appears.

Step 18   For each CiscoSecure ACS Services Initiation option you want, check the corresponding box. The actions associated with the options occur after the setup program finishes.

- **Yes, I want to start the CiscoSecure ACS Service now:** Starts the Windows services that compose Cisco Secure ACS. If you do not select this option, the Cisco Secure ACS HTML interface is not available unless you reboot the computer or start the CSAdmin service.

- **Yes, I want Setup to launch the CiscoSecure ACS Administrator from my browser following installation:** Opens the Cisco Secure ACS HTML interface in the default web browser for the current Windows user account.

- **Yes, I want to view the Readme file:** Opens the README.TXT file in Windows Notepad.

Step 19   Click **Next >**.

If you selected the option, the Cisco Secure ACS services start. The Setup Complete dialog box displays information about the Cisco Secure ACS HTML interface.

Step 20   Click **Finish**.

The setup program will exit. If, in Step 18, you chose the options to view the HTML interface or README.TXT file, those options occur now.

On the computer running Cisco Secure ACS, you can access the Cisco Secure ACS HTML interface using the ACS Admin desktop icon or you can type the following URL into the Address line of a supported web browser: http://127.0.0.1:2002.

Note	The Cisco Secure ACS HTML interface is available only if you chose to start Cisco Secure ACS services in Step 18. If you did not choose this option, you can make the HTML interface available by rebooting the computer or by entering **net start csadmin** at a command prompt.

Step 21   If you want Cisco Secure ACS to authenticate users with a Windows domain user database, you must perform additional Windows configuration. See the *Windows Authentication Configuration* section in the *Installation Guide for Cisco Secure ACS for Windows Server* for more details.

Software versus Appliance

This topic discusses the differences between implementing Cisco Secure ACS in the network using software installed on a server or an appliance solution.

Cisco Secure ACS is available in a software only format where the customer installs the software on their own Windows server and as a hardware appliance where the ACS software is preinstalled on a hardened, rack-mountable PC server.

Customers who opt for the software version often prefer this format as they can select the hardware it will be installed on, and can also have normal access to the Windows operating system. The ACS software has more direct integration with Active Directory than does the ACS appliance.

The ACS appliance offers other advantages though. The ACS software comes preinstalled on a PC server so the customer does not have to purchase hardware separately. The appliance operating system is hardened by turning off unnecessary services and ports. It also comes with Cisco Security Agent for addition protection. Operating system access is not available - instead maintenance functions can be performed from a console command-line interface and from the ACS web user interface itself. The customer can have a one stop shop for both the ACS software and the hardware support.

For other benefits and differences between the ACS software and appliance, see the Cisco Secure Access Control Server Solution Engine 4.0 Q&A:

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

Summary

This topic summarizes the key points discussed in this lesson.

- Cisco Secure ACS can manage and administer user access for Cisco devices.

- There are specific memory, CPU, and disk requirements for the installation of ACS.

- There are many steps to installing ACS.

- There are advantages and disadvantages to deploying Cisco Secure ACS as either a software implementation or an appliance deployment.

Lesson 2

AAA Concepts

Overview

Authentication, authorization, and accounting (AAA) services are an architectural framework for configuring a set of three independent security functions in a consistent manner. AAA network security services provide a modular way of performing these features.

Objectives

Upon completing this lesson, you will have a basic understanding of the AAA components. This ability includes being able to meet these objectives:

- Define AAA
- Describe Authentication
- Describe Authorization
- Describe Accounting
- Compare TACACS+ to Radius

What is AAA?

AAA network security services provide the primary framework through which you set up access control. AAA provides a modular way of performing authentication, authorization and accounting services. We will discuss these services in the following topics.

In many circumstances, AAA uses protocols such as RADIUS, TACACS+, or Kerberos to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS, TACACS+, or Kerberos security server.

Although AAA is the primary (and recommended) method for access control, Cisco IOS software provides additional features for simple access control that are outside the scope of AAA, such as local username authentication, line password authentication, and enable password authentication. However, these features do not provide the same degree of access control that is possible by using AAA.

What is Authentication?

Authentication provides the method used to identify a user prior to them gaining access to the network and network services. Authentication can include a login and password dialog, challenge and response, messaging support, and, depending on the security protocol you select, encryption.

You configure AAA authentication by defining a named list of authentication methods, and then applying that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they will be performed; it must be applied to a specific interface before any of the defined authentication methods will be performed. The only exception is the default method list (which is named "default"). The default method list is automatically applied to all interfaces if no other method list is defined. A defined method list overrides the default method list.

You must define all authentication methods, except for local, line password, and enable authentication, through AAA.

What is Authorization?

Authorization provides the method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet.

AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the actual capabilities and restrictions of the user. The database can be located locally on the access server or router, or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user. You must define all authorization methods through AAA.

As with authentication, you configure AAA authorization by defining a named list of authorization methods, and then applying that list to various interfaces.

What is Accounting?

Accounting provides a method for collecting and sending security server information used for billing, auditing, and reporting purposes. Accounting can collect such information as user identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

Accounting enables you to track the services users are accessing as well as the amount of network resources they are consuming. When you activate AAA accounting, the network access server reports user activity to a RADIUS or TACACS+ security server (depending on which security method you have implemented) in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server. You can then analyze this data for network management, client billing, and/or auditing. You must define all accounting methods through AAA. As with authentication and authorization, you configure AAA accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

Comparison of RADIUS and TACACS+

The following table provides a comparison of RADIUS and TACACS+.

RADIUS vs. TACACS+

RADIUS	TACACS+
RADIUS uses UDP.	TACACS+ uses TCP.
RADIUS encrypts only the password in the access-request packet; less secure.	TACACS+ encrypts the entire body of the packet; more secure.
RADIUS combines authentication and authorization.	TACACS+ uses the AAA architecture, which separates authentication, authorization, and accounting.
Industry standard (created by Livingston).	Cisco Proprietary.
RADIUS does not support ARA access, Net BIOS Frame Protocol Control protocol, NASI, and X.25 PAD connections.	TACACS+ offers multiprotocol support.
RADIUS does not allow users to control which commands can be executed on a router.	TACACS+ provides two ways to control the authorization of router commands: on a per-user or per-group basis.

Summary

This topic summarizes the key points discussed in this lesson.

- AAA network security services provide the primary framework through which you set up access control.

- Authentication provides the method used to identify a user prior to them gaining access to the network and network services.

- Authorization provides the method for remote access control.

- Accounting provides a method for collecting and sending security server information used for billing, auditing, and reporting purposes.

- AAA uses both RADIUS and TACACS+ to administer security functions.

ACS Interface

Overview

The ACS interface is a very basic HTML interface that can be viewed in a web browser. Although it is a simple interface to navigate and configure, there are many different options that you can configure. This lesson will discuss how the interface works, how to navigate within it, and how to customize the look of the interface.

Objectives

Upon completing this lesson, you will be able to understand how the ACS interface is configured and navigated. This ability includes being able to meet these objectives:

■ Know how the ACS HTML interface is accessed and used

■ Understand how to navigate the HTML interface

■ Customize the HTML interface

How the HTML Interface Works

This topic describes how to access and use the HTML interface.
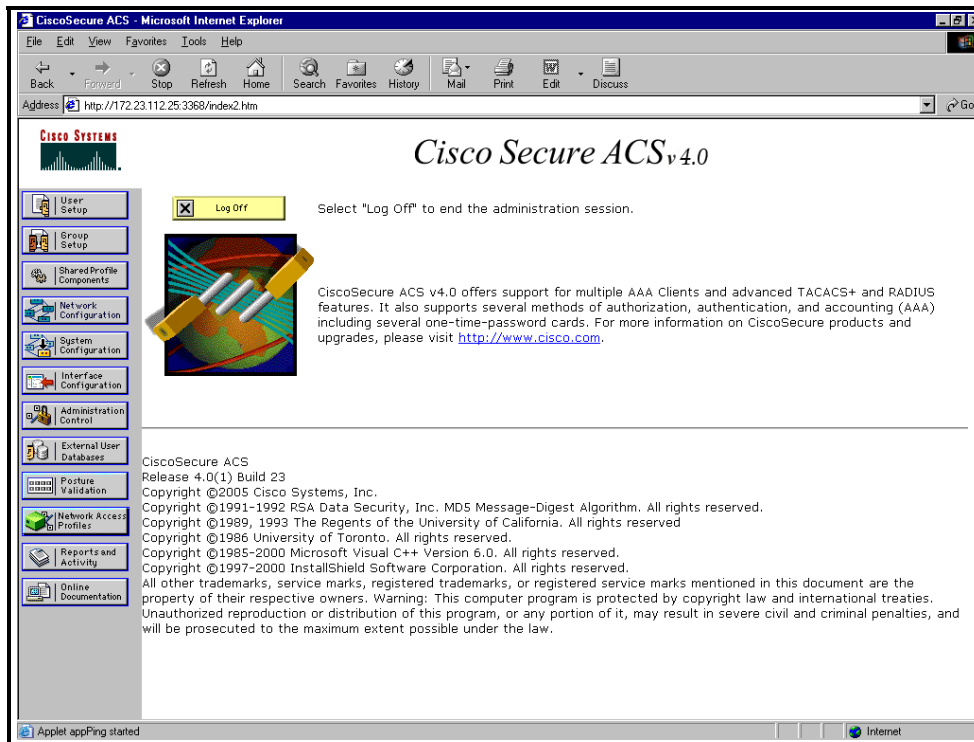
The ACS HTML interface is very simple to use. In order to access ACS from the server on which ACS is installed, browse to http://127.0.0.1:2002. There is also an ACS ADMIN link created during the installation. If you are browsing from the network, you will have to enable an administrator first. By default, an administrative account is not created. To create an administrative account, follow these steps:

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

Step 2   Click **Add Administrator**.

The Add Administrator page appears.

Step 3   Complete the boxes in the Administrator Details table:

—   In the Administrator Name box, type the login name (up to 32 characters) for the new Cisco Secure ACS administrator account.

—   In the Password box, type the password (up to 32 characters) for the new Cisco Secure ACS administrator account.

—   In the Confirm Password box, type the password a second time.

Step 4   To choose all privileges, including user group editing privileges for all user groups, click **Grant All**.

All privilege options are selected. All user groups move to the Editable groups list.

Tip	To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

Step 5 To grant user and user group editing privileges, follow these steps:

— Check the desired boxes under User & Group Setup.

— To move a user group to the Editable groups list, choose the group in the Available groups list, and then click **-->** (right-arrow button). The selected group moves to the Editable groups list.

— To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click **<--** (left-arrow button). The selected group moves to the Available groups list.

— To move all user groups to the Editable groups list, click **>>**. The user groups in the Available groups list move to the Editable groups list.

— To remove all user groups from the Editable groups list, click **<<**. The user groups in the Editable groups list move to the Available groups list.

Step 6 To grant any of the remaining privilege options, in the Administrator Privileges table, check the applicable boxes.

Step 7 Click **Submit**.

Configuring Administrative Access Parameters

The Access Policy feature affects access to the Cisco Secure ACS HTML interface. You can limit access by IP address and by the TCP port range used for administrative sessions. You can also enable a Secure Socket Layer (SSL) for access to the HTML interface.

In addition to Access Policy, the Session Policy feature controls various aspects of Cisco Secure ACS administrative sessions.

To set up Cisco Secure ACS Access Policy, follow these steps:

Step 1 In the navigation bar, click **Administration Control**. Cisco Secure ACS displays the Administration Control page.

Step 2 Click **Access Policy**. The Access Policy Setup page appears.

Step 3 To allow remote access to the HTML interface from any IP address, in the IP Address Filtering table, choose the **Allow all IP addresses to connect** option.

Step 4 To allow remote access to the HTML interface only from IP addresses *within* a range or ranges of IP addresses, follow these steps:

— In the IP Address Filtering table, choose the **Allow only listed IP addresses to connect** option.

— For each IP address range for which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. In the Start IP Address box, enter the lowest IP address (up to 16 characters) in the range. In the End IP Address box, type the highest IP address (up to 16 characters) in the range. Use dotted decimal format.

Note	The IP addresses entered to define a range must differ only in the last octet.

Step 5   To allow remote access to the HTML interface only from IP addresses *outside* a range or ranges of IP addresses, follow these steps:

—   In the IP Address Filtering table, choose the **Reject connections from listed IP addresses** option.

—   For each outside IP address range from which you want to prohibit remote access to the HTML interface, complete one row of the IP Address Ranges table. Enter the lowest IP address (up to 16 characters) in the range in the Start IP Address box. Type the highest IP address (up to 16 characters) in the range in the End IP Address box.

Note   The IP addresses entered to define a range must differ only in the last octet.

Step 6   If you want to allow Cisco Secure ACS to use any valid TCP port for administrative sessions, under HTTP Port Allocation, choose the **Allow any TCP ports to be used for Administration HTTP Access** option.

Step 7   If you want to allow Cisco Secure ACS to use only a specified range of TCP ports for administrative sessions, follow these steps:

—   Under HTTP Port Allocation, choose the Restrict Administration Sessions to the following port range From Port *X* to Port *Y* option.

—   In the *X* box, type the lowest TCP port (up to 5 characters) in the range.

—   In the *Y* box, type the highest TCP port (up to 5 characters) in the range.

Step 8   If you want to enable SSL encryption of administrator access to the HTML interface, under Secure Socket Layer Setup, check the **Use HTTPS Transport for Administration Access** box.

Step 9   Click **Submit**.

To setup Cisco Secure ACS Session Policy, follow these steps:

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

Cisco Secure ACS displays the Administration Control page.

Step 2   Click **Session Policy**.

The Session Policy Setup page appears.

Step 3   To define the number of minutes of inactivity after which Cisco Secure ACS ends an administrative session, in the Session idle timeout (minutes) box; enter the number of minutes (up to 4 characters).

Step 4   Set the automatic local login policy:

—   To allow administrators to log into Cisco Secure ACS locally without using their administrator names and passwords, check the **Allow Automatic Local Login** box.

—   To require administrators to log into Cisco Secure ACS locally using their administrator names and passwords, clear the **Allow Automatic Local Login** checkbox.

Step 5   Set the invalid IP address response policy:

— To configure Cisco Secure ACS to respond with a message when an administrative session is requested from an invalid IP address, check the **Respond to invalid IP address connections** box.

— To configure Cisco Secure ACS to send no message when an administrative session is requested from an invalid IP address, clear the **Respond to invalid IP address connections** checkbox.

Step 6   Set the failed administrative login attempts policy:

— To enable Cisco Secure ACS to lock out an administrator after a specified number of successive failed administrative login attempts, check the **Lock out Administrator after *X* successive failed attempts** box.

— In the *X* box, type the number of successive failed login attempts after which Cisco Secure ACS locks out an administrator. The *X* box accepts up to four characters.

Step 7   Click **Submit**.

Navigating the HTML Interface

This topic describes the navigation of the HTML interface and a brief overview of each section of the interface.
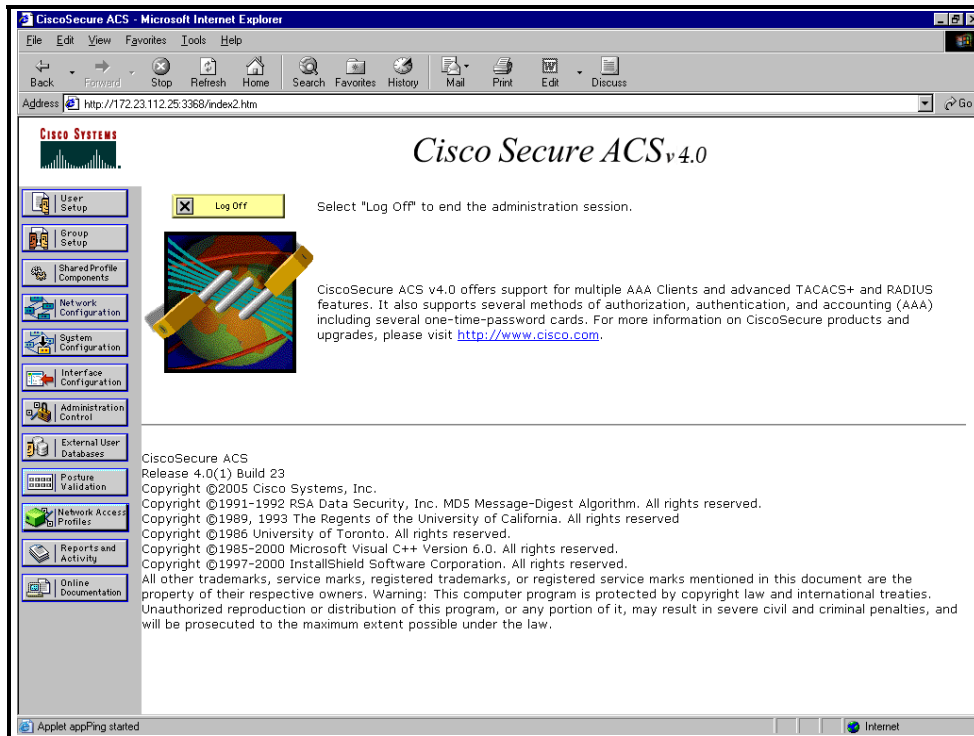
If this is your first time using ACS, it is important to take the time to learn how to navigate within the user interface. The main web page of ACS is divided into frames. You access different menu items on the left-hand menu frame, perform configuration in the main frame, and have access to some help on the right-hand frame. Because you will use the menu a great deal in your configurations, the next sections look at each menu item and what types of configuration can be performed at each level.

User Setup

In User Setup, you can add a new user, search for an existing user, find users alphabetically or numerically, or simply list all users at once.

Group Setup

Group Setup is where you will configure any parameters that are common to a group of users. In this section, you can apply configuration from Shared Profile Components, as well as specific TACACS+ and RADIUS attributes.

Shared Profile Components

Shared Profile Components allows you to specify Shell Command Authorization Sets and PIX Shell Command Authorization Sets. By creating these command authorization sets, you can control the commands a user can execute on a device by applying the command authorization set to the user profile in the TACACS+ settings, or at the group level. By default, you can choose **Shell Command Authorization Sets and PIX Shell Command Authorization Sets**.

Optionally, you can configure Downloadable ACLs or Management Center Authorization Sets. For these options to be visible, you must select them in the Interface Configuration page. Another benefit to the Shared Profile Components configuration page is the ability to configure Shared Network Access Restrictions.

Network Configuration

The Network Configuration section is where you add, delete, or modify settings for AAA clients. The layout of this page changes depending on the settings for interface configuration. If you are using Network Device Groups (NDGs), after you click Network Configuration in the navigation bar, only the Network Device Groups table and Proxy Distribution Table information appears. If you are not using NDGs, the AAA Clients table and the AAA Servers table appears in place of the Network Device Groups table.
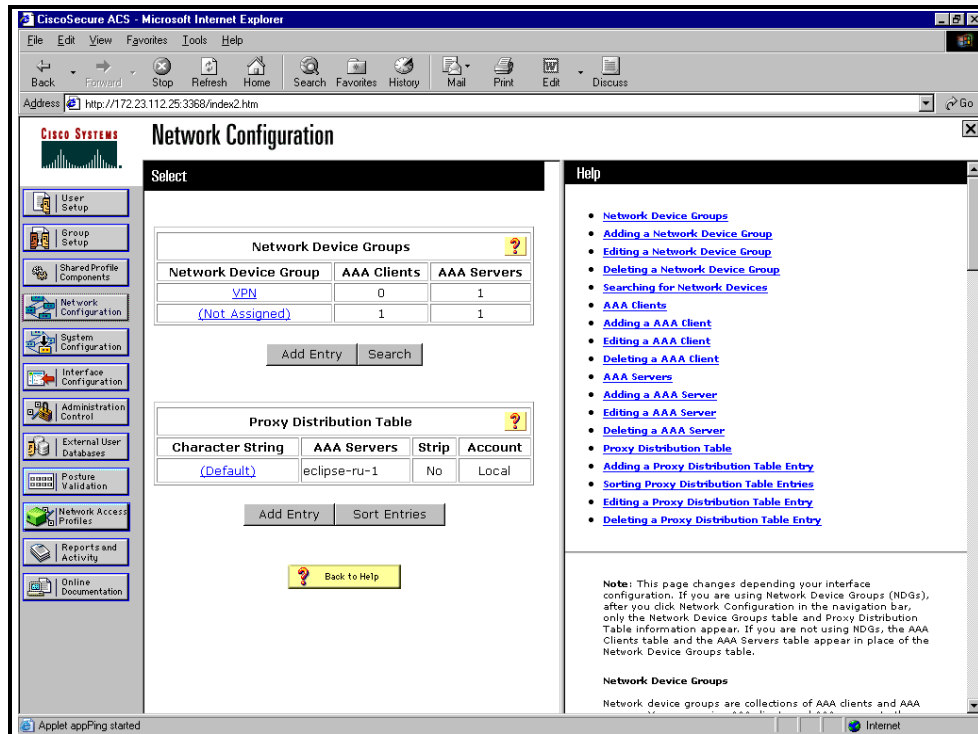
System Configuration

Under System Configuration, you will find many sub-configuration links.

Service Control

From Service Control, you can start and stop the ACS services. You can also start and stop the ACS services in the Control Panel of Windows. By stopping the ACS service from within ACS, you do not stop the ACS web server. If you want to stop the ACS web server, you need to do so in the Control Panel of Windows. This service is called CSAdmin.

Logging

From the Logging task, you can configure local logging, such as failed attempts as well as TACACS+ and RADIUS accounting. You can also configure Open Database Connectivity (ODBC) and remote logging here, as well as other ACS devices.

Date Format Control

The Date Format Control option allows you to change the format of the date displayed on reports. After you change the format, you must logout of the server to actually see the changes take affect. You can logout of ACS in a few ways. One way is by clicking the Cisco Systems logo in the top-left corner of the web browser screen and then clicking the **Log off** button. Another method is by clicking the **X** in the top-right corner of the window.

Local Password Management

From this task, you can set password length, as well as password options. You can also configure options for Remote Password Change and logging of password changes.

ACS Backup

This option allows you to schedule backups to be performed manually or automatically at specific times. You can also specify a location for the backup files to be stored as well as manage the backup files. When ACS is backed up, it creates a file with the extension of .dmp. This file will be present when you enter the ACS Restore link. Here you have the ability to select from numerous backup files, as well as determine if you want to restore the Users and Groups, System Configuration, or both.

ACS Service Management

ACS Service Management enables the administrator to determine how often to test the availability of ACS authentication services. This is the CSMon service configuration. This allows ACS to test itself and take action when the test is unsuccessful. If no authentications are recorded, the available actions are:

- Restart all

- Restart RADIUS/TACACS

- Reboot

- Take no action

If the reboot option is selected, this causes the server running ACS to reboot. You also have the ability to add custom actions to this list. In addition, you can choose to log the attempts to log in using a disabled account. Do this by checking the **Generate event when an attempt is made to log in to a disabled account** box.

Under ACS Service Management, you can also configure e-mail notifications and setup the NT Event Log. The ACS Certificate Setup is where you configure the ACS device with digital certificates. Use this when you configure the ACS to use SSL for administrative sessions. Global Authentication Setup is where you can allow protocols such as PEAP, EAP-TLS, EAP-MD5, and MS-CHAP.

Interface Configuration

In the Interface Configuration section, as seen below, you will find a selection from the following sub-configuration links, depending on whether you have selected TACACS+ or a form of RADIUS when you entered your AAA client:

- User Data Configuration
- TACACS+ (Cisco IOS)
- RADIUS (Microsoft)
- RADIUS (Ascend)
- RADIUS (IETF)
- RADIUS (IOS/PIX)
- Advanced Options

Note   If you do not see RADIUS options here, you need to add an AAA client that uses the RADIUS protocol. Interface Configuration is directly affected by the settings in Network Configuration.
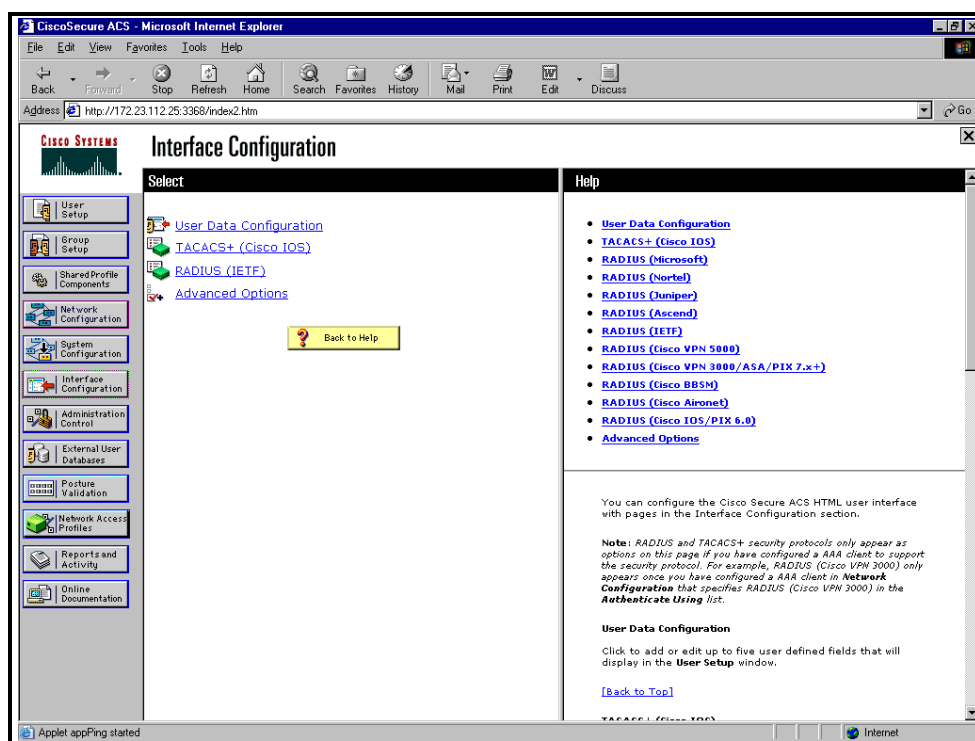
The User Data Configuration link enables you to customize the fields that appear in the user setup and configuration page. Here you can add fields such as phone number, work location, supervisor name, or any other information you feel is pertinent.

The TACACS+ (Cisco IOS) link enables the administrator to configure TACACS+ settings as well as add new TACACS+ services. You can also configure advanced options that affect what you see in your interface. It is important that you understand how this works. Depending on the current configuration of your server, if you go to the TACACS+ link, you may or may not see

two columns. If you *do* see two columns, you are able to configure user-level settings as well as group-level settings.

Administration Control

The Administration Control section is where you configure all aspects of ACS for administrative access. Here you have the ability to add administrators and configure access policy. Information such as which IP addresses are allowed or not allowed to access ACS, and HTTP port allocation can be configured here.

Recall that ACS uses port 2002 as the listening port, but after a connection is made to that port, you are redirected to a random port number. When ACS is positioned behind a firewall, this random port assignment becomes a security issue. You have the ability to specify a range of ports used so that you can configure access restrictions within your firewall. This is especially helpful when using a PIX Firewall.

Note	The Secure Socket Layer Setup option is not available in ACS v3.0.

The Session Policy feature allows you to control these options: alter the timeout, allow automatic local logins, and respond to invalid IP addresses. You can also choose to lock administrator access after a certain number of invalid tries.

Note	Audit Policy feature allows you to configure File Management and Directory Management options.

External User Databases

The External User Database section consists of three sub-sections. In addition to configuring the parameters to communicate with the external databases, you will configure how ACS handles requests from users that are not in the local ACS database (Unknown User Policy), as well as a mapping from the external database group, to the local ACS database group.
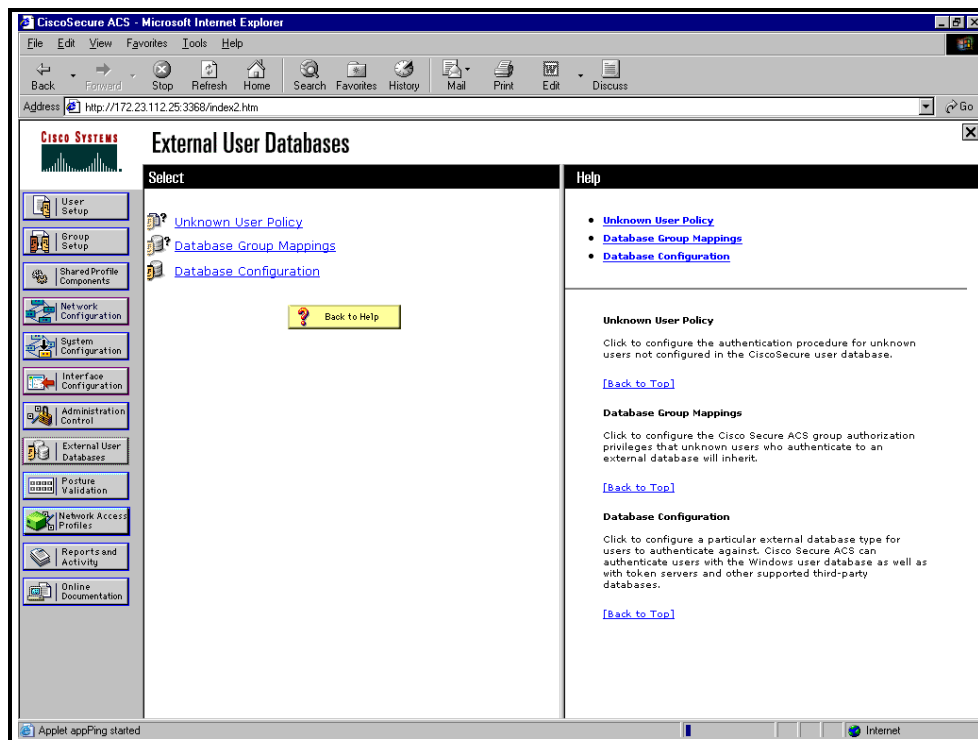
In this section, you configure an unknown user policy. This same topic is covered in the *System Configuration* lesson. You also configure database group mappings to external user databases as well as perform the actual database configuration. Further, you are given a list of compatible databases, and you can choose which one you will configure to be used with ACS.

The following servers are available for use as an external database:

- Windows NT/2000
- Novell NDS
- Generic LDAP
- External ODBC Database
- LEAP Proxy RADIUS Server
- RADIUS Token Server
- VASCO Token Server
- ActivCard Token Server
- PassGo Defender Token Server
- CRYPTOCard Token Server
- SafeWord Token Server
- RSA SecurID Token Server

Each version of ACS includes more and more support for external databases while greatly improving the functionality of the ACS database. Check the release notes for more information.

Posture Validation

ACS supports the Network Admission Control (NAC) initiative. NAC is used to ensure every end-point conforms to security policy before being granted access to the network. Posture Validation is the mechanism used to determine the state of the end-point requesting network access. The Posture Validation section is used to configure the different ways you can set up posture validation policies.
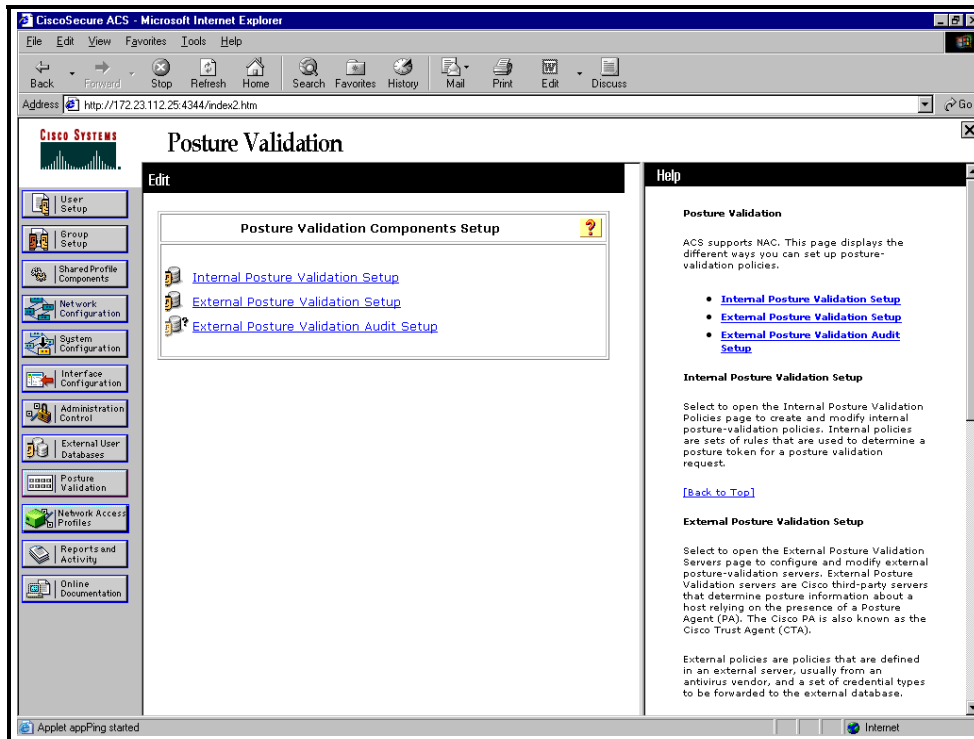
The administrator can choose to create and modify internal posture validation policies, or configure ACS to forward selected credentials to external policy-validation servers. Audit servers can also be configured to determine the posture of end-points without the presence of a posture agent (used to forward end-point credentials).

Network Access Profiles

A Network Access Profile is a means to classify access requests, according to 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. The use of Network Access Profiles allows the administrator to configure different authentication mechanisms and authorizations depending on the characteristics of the access request resulting in increased flexibility.
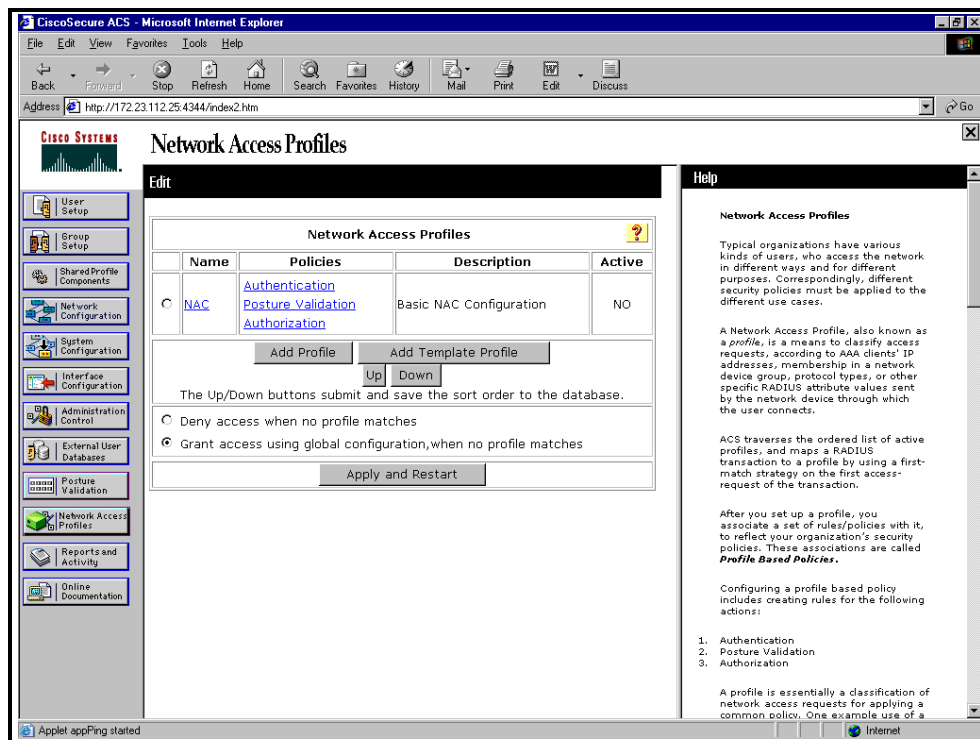
The Network Access Profile section is used to create profiles, and associate a set of rules and policies with them. Network Access Profiles are discussed in more detail in Module 4.

Reports and Activity

The Reports and Activity section provides a wealth of tools you can use for both troubleshooting and monitoring the network. But remember, logging consumes resources and the log files should be checked periodically for content and size.

Within ACS, you have the ability as an administrator to monitor your network security on a number of levels. The available logs that ACS keeps for you are:

- **TACACS+ Accounting:** All of the Accounting reports include information such as time/date, username, type of connection, amount of time logged in, and bytes transferred. The information that is included in these reports is configurable by the administrator in the System Configuration section under Logging. These reports can be found at Program Files\CiscoSecure ACSv3.x\Logs\TACACS+Accounting.

- **TACACS+ Administration:** The TACACS+ Administration reports include all of the command requests from AAA clients, such as routers or firewalls where command authorization is configured. These reports can be found at Program Files\CiscoSecure ACS v3.x\Logs\TACACS+Administration.

- **RADIUS Accounting:** The RADIUS Accounting report includes the same type of information as mentioned under the TACACS+ Accounting log. The information included in this report is also configurable by the administrator under System Configuration, Logging. These reports can be found in Program Files\CiscoSecure ACS v3.x\Logs\RADIUSAccounting.

- **VoIP Accounting:** This log includes information on VoIP sessions, including session duration, and AAA usernames. These reports can be found in Program Files\CiscoSecure ACS v3.x\Logs\VoIP Accounting.

- **Passed Authentications:** The information contained in these reports assists with user administration, as well as in troubleshooting users that are failing authentication. It lists successful authentication requests. These reports can be found in Program Files\CiscoSecure ACS v3.x\Logs\Passed Authentications.

- **Failed Attempts:** Similar to Passed Authentications, this report assists with user administration as well as in troubleshooting users that are failing authentication. It lists authentication and authorization failures with an indication of the cause. These reports can be found in Program Files\CiscoSecure ACS v3.x\Logs\Failed Attempts.

- **Logged-in Users:** This report also assists with user administration as well as in troubleshooting users that are failing authentication. However, the Logged-in Users file is rather unique. Most of the logging files in ACS are stored as comma-separated value (CSV) files and are stored for a period of time, usually one day, on the hard drive of the server. The Logged-in Users file is not saved as a CSV file. As users log in, they are maintained in this file, organized by the name of the AAA client. You can purge the entries if they appear to be entries that have locked up.

- **Disabled Accounts:** This report enables you to view accounts that have been disabled.

- **ACS Backup and Restore:** The ACS Backup and Restore report is available only if the option in Interface Configuration is enabled. This log maintains a history of the dates and times that ACS was backed up and/or restored. These reports can be found in Program Files\CiscoSecure ACS v3.x\Logs\Backup and Restore.

- **Remote Database Management Source (RDBMS) Synchronization:** The RDBMS Synchronization is also available only when the option is configured in the Interface Configuration Advanced Options. You do not enable the report; you enable RDBMS Synchronization. This log allows ACS to keep report information on RDBMS Synchronization. It logs the time and reason for RDBMS Synchronization. These reports can be found in Program Files\CiscoSecureACS v3.x\Logs\DbSync.

- **Database Replication:** Database Replication is another report that must be enabled in Interface Configuration. This report logs the time that the ACS database was replicated to the backup server. These reports can be found in Program Files\CiscoSecure ACS v3.x\Logs\DBReplicate.

- **Administration Audit:** Administration Audit logs all of the activity in ACS that is performed by administrators. This keeps track of who logged in, what users and groups they made changes to, and what time they logged out. These reports can be found in Program Files\CiscoSecure ACS v3.x\Logs\AdminAudit.

- **User Password Changes:** This report tracks changes that were made to user passwords using the User Changeable Password Module. These reports can be found in Program Files\CiscoSecure ACS v3.x\CSAuth\PasswordLogs.

- **ACS Service Monitoring:** This report keeps track of all of the events that occur to Cisco Secure ACS services that are monitored. An example of a service that might be monitored is CSAdmin or CSTacacs. By default CSMon is enabled, however, this is configurable. To configure this, you must go to **System Configuration > ACS Service Management**. Here, you can choose to monitor the login process, generate events when someone tries to log into disabled accounts, and so on. These reports can be found in Program Files\CiscoSecureACSv4.x\Logs\ServiceMonitoring.

You can view these reports in the ACS HTML interface or from the hard drive of the ACS server. The logs are stored as CSV files, except where noted, therefore you can view them in a spreadsheet program such as Microsoft Excel. For even more functionality, you can import the files into third-party software, such as Crystal Reports. If you do not have access to the hard drive of the ACS server, you have the ability to download the logs using the ACS HTML interface.

Online Documentation

The online documentation of ACS is there to help you out if you need additional help. The online help also has detailed configuration information. You can access the PDF form if you have the CD-ROM, or it is available in a compressed ZIP file that you can download from Cisco.com. In addition to the detailed online documentation, some configuration menus throughout ACS will contain brief help on the right-hand side of the screen in the browser window.

Customizing the HTML Interface

This topic describes how to customize the HTML interface.
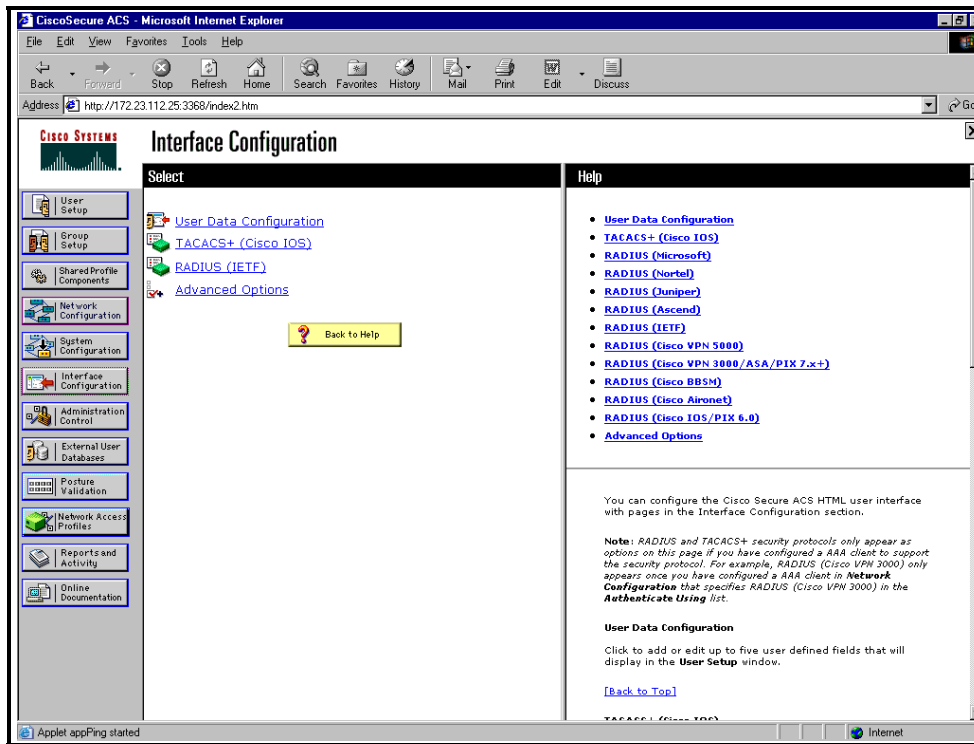
The HTML interface is customizable. This process is done in the **Interface Configuration** section of ACS. The following sections cover each of the customization areas.

User Data Fields

The Configure User Defined Fields page enables you to add (or edit) up to five fields for recording information on users. The fields you define in this section appear in the Supplementary User Information section at the top of the User Setup page. For example, you could add fields such as the user's company name, telephone number, department, and billing code. You can also include these fields in the accounting logs.

To configure new user data fields, follow these steps:

Step 1   Click **Interface Configuration**, and then click **User Data Configuration**.

The Configure User Defined Fields page appears. The checkboxes in the Display column indicate which fields are configured to appear in the Supplementary User Information section at the top of the User Setup page.

Step 2   Check a box in the Display column.

Step 3   In the corresponding Field Title box, type a title for the new field.

Step 4   To configure another field, repeat Step 2 and Step 3.

Step 5   When you have finished configuring new user data fields, click **Submit**.

Advanced Options

The Advanced Options page enables you to determine which advanced features Cisco Secure ACS displays. You can simplify the pages displayed in other areas of the Cisco Secure ACS HTML interface by hiding advanced features that you do not use.

To set advanced options for the Cisco Secure ACS HTML interface, follow these steps:

Step 1   Click **Interface Configuration**, and then click **Advanced Options**.

The Advanced Options table appears.

Step 2   Choose each option that you want displayed (enabled) in the Cisco Secure ACS HTML interface.

Caution	Disabling an advanced feature in the Interface Configuration section does not affect anything except the display of that feature in the HTML interface. Settings made while an advanced feature was displayed remain in effect when that advanced feature is no longer displayed. Further, the interface displays any advanced feature that has non-default settings, even if you have configured that advanced feature to be hidden. If you later disable the feature or delete its settings, Cisco Secure ACS hides the advanced feature. The only exception is the Network Device Groups feature. Regardless of whether Network Device Groups are in use, they are hidden when deselected on the Advanced Options page.

Step 3   When you have finished making selections, click **Submit**.

Cisco Secure ACS alters the contents of various sections of the HTML interface according to the selections you have made.

TACACS+ and RADIUS Options

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

Note	The Cisco Secure ACS HTML interface displays any protocol option that is enabled or has non-default values, even if you have configured that protocol option to be hidden. If you later disable the option or delete its value, and the protocol option was configured to be hidden, Cisco Secure ACS hides the protocol option. This behavior prevents Cisco Secure ACS from hiding active settings.

To configure the user interface for TACACS+ options, follow these steps:

Step 1   Click **Interface Configuration**, and then click **TACACS+ (Cisco IOS)**.

The TACACS+ (Cisco) page appears.

Step 2   In the TACACS+ Services table, check the box for each TACACS+ service you want displayed on the applicable setup page.

Step 3   To add new services and protocols, follow these steps:

— In the New Services section of the TACACS+ Services table, enter any Service or Protocol to be added.

Note   If you have configured Cisco Secure ACS to interact with device management applications for other Cisco products, such as a Management Center for Firewalls, Cisco Secure ACS may display new TACACS+ services as dictated by these device management applications. To ensure the proper functioning of Cisco Secure ACS, of device management applications with which Cisco Secure ACS interacts, and of the Cisco network devices managed by those applications, do not change or delete automatically generated TACACS+ service types.

— Check the appropriate box to choose the options that should be displayed for configuration either under User Setup, or Group Setup, or both.

Step 4   In the Advanced Configurations Options section, check the boxes of the display options you want to enable.

Step 5   When you have finished setting TACACS+ interface display options, click **Submit**.

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

It is unlikely that you would want to install every attribute available for every protocol. Displaying every option would make setting up a user or group cumbersome. To simplify setup, this section allows you to customize the attributes that are displayed. For a list of supported RADIUS AV pairs and accounting AV pairs, see "RADIUS Attributes" in the ACS user guide.

Depending on which AAA client or clients you have configured, the Interface Configuration page displays different RADIUS protocol configuration settings choices. The Interface Configuration page displays RADIUS IETF settings whenever any RADIUS AAA client is configured. The Interface Configuration page also displays additional settings for each vendor-specific RADIUS type. The settings that appear for various types of AAA client depend on what settings that type of device can employ.

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

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

Note   Your RADIUS network devices must support each IETF RADIUS attribute selected.

To set protocol configuration options for IETF RADIUS attributes, follow these steps:

Step 1   Click **Interface Configuration**, and then click **RADIUS (IETF)**.

The RADIUS (IETF) page appears.

Step 2   Check the corresponding box for each IETF RADIUS attribute that you want to appear as a configurable option on the User Setup or Group Setup page.

Note   Your RADIUS network devices must support each attribute selected.

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

Step 4   When you have finished choosing the attributes, click **Submit**.

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

Setting Protocol Configuration Options for Non-IETF RADIUS Attributes

This procedure enables you to hide or display various RADIUS vendor-specific attributes (VSAs) for configuration from the User Setup and Group Setup portions of the Cisco Secure ACS HTML interface.

To set protocol configuration options for a set of RADIUS VSAs, follow these steps:

Step 1   Click **Interface Configuration**.

Step 2   Click one of the RADIUS VSA set types displayed, for example, RADIUS (Ascend).

The page listing the selected set of available RADIUS VSAs appears.

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

Step 3   For each RADIUS VSA that you want to appear as a configurable option on the User Setup or Group Setup page, check the corresponding box.

Note   Your RADIUS network devices must support each attribute selected.

Step 4   Click **Submit**.

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

Summary

This topic summarizes the key points discussed in this lesson.

- The ACS HTML interface can be accessed either locally on the ACS server, or remotely if an administrator account is setup on the ACS server.

- Navigation of the ACS interface is similar to surfing the Internet.

- Customization of the HTML interface is done via interface configuration.

Module Summary

Upon completing this module, you should now be able to install and customize ACS. This ability includes being able to meet these objectives:

- Determine which ACS product is right for your network
- Install ACS
- Customize ACS

References

For additional information, refer to *Cisco Secure Access Control Server for Windows* at www.cisco.com/go/acs/.

Module 2

ACS Databases and Additional Server Interaction

Overview

When speaking of ACS, it is often overlooked that much of the power of ACS is in its ability to work with additional databases, such as other ACS databases or external user databases. This module discusses configurations of ACS for synchronizing databases with other ACS servers or external user databases, some import tools available, and service monitoring capabilities.

Module Objectives

Upon completion of this module, you will be able to work with additional databases and server interaction. This ability includes being able to meet these objectives:

- Learn how automatic service monitoring works
- Configure automatic service monitoring
- Understand how database synchronization works
- Configure database synchronization
- Obtain knowledge of import tools for large scale deployments
- Understand and configure LDAP databases
- Understand and configure ODBC databases

ACS 4.0 Primer (CACS v2.0)

System Configuration

Overview

ACS databases are an important component of the server. This lesson will teach you to manage these database options.

Objectives

Upon completing this lesson, you will be able to perform general system configuration. This ability includes being able to meet these objectives:

- Understand how automatic service monitoring works
- Configure automatic service monitoring
- Understand how database synchronization works
- Configure database synchronization
- Understand how to use import tools for large scale deployments

How Automatic Service Monitoring Works

ACS Active Service Management is an application-specific service monitoring tool that is tightly integrated with ACS. The two features that compose ACS Active Service Management are described in this section.

This section contains the following topics:

- System Monitoring
- Event Logging

System Monitoring

Cisco Secure ACS system monitoring enables you to determine how often Cisco Secure ACS tests its authentication and accounting processes, and to determine what automated actions it takes when the tests detect a failure of these processes. Cisco Secure ACS accomplishes system monitoring with the CSMon service.

System Monitoring Options

The following options are available for configuring system monitoring:

- **Test login process every *X* minutes:** Controls whether or not Cisco Secure ACS tests its login process. The value in the X box defines, in minutes, how frequently Cisco Secure ACS tests its login process. The default frequency is once per minute, which is also the most frequent testing interval possible.

   When this option is enabled, at the interval defined Cisco Secure ACS tests authentication and accounting. If the test fails, after four unsuccessful re-tries Cisco Secure ACS performs the action identified in the "If no successful authentications are recorded" list and logs the event.

- **If no successful authentications are recorded:** Specifies what action Cisco Secure ACS takes if it detects that its test login process failed. This list contains several built-in actions and reflects actions that you define. The items beginning with asterisks (*) are predefined actions.

   — ***Restart All:** Restart all Cisco Secure ACS services.

   — ***Restart RADIUS/TACACS+:** Restart only the RADIUS and TACACS+ services.

   — ***Reboot:** Reboot Cisco Secure ACS.

   — **Custom actions:** You can define other actions for Cisco Secure ACS to take upon failure of the login process. Cisco Secure ACS can execute a batch file or executable upon the failure of the login process. To make a batch or executable file available in the on failure list, place the file in the following directory:
   drive:*path*\CSMon\Scripts (where *drive* is the local drive on which you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory).

   — **Take No Action:** Leave Cisco Secure ACS operating as is.

- **Generate event when an attempt is made to log in to a disabled account:** Specifies whether Cisco Secure ACS generates a log entry when a user attempts to log in to your network using a disabled account.

- **Log all events to the NT Event log:** Specifies whether Cisco Secure ACS generates a Windows event log entry for each exception event.
- **Email notification of event:** Specifies whether Cisco Secure ACS sends an e-mail notification for each event.
    — **To:** The e-mail address to which notification e-mail is sent. For example, joeadmin@company.com.
    — **SMTP Mail Server:** The simple mail transfer protocol (SMTP) server that Cisco Secure ACS should use to send notification e-mail. You can identify the SMTP server either by its hostname or by its IP address.

Event Logging

The Event Logging feature enables you to configure whether Cisco Secure ACS logs events to the Windows event log and whether Cisco Secure ACS generates an e-mail when an event occurs. Cisco Secure ACS uses the System Monitoring feature to detect the events to be logged.

Configuring Automatic Service Monitoring

To setup Cisco Secure ACS System Monitoring, follow these steps:

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

Step 2   Click **ACS Service Management**. The ACS Active Service Management Setup page appears.

Step 3   To have Cisco Secure ACS test the login process, follow these steps:

1. Check the **Test login process every *X* minutes** box.

2. In the *X* box, enter the number of minutes (up to three characters) that should pass between each login process test.

3. From the **If no successful authentications are recorded** list, choose the action you want Cisco Secure ACS to take when the login test fails five successive times.

Step 4   To have Cisco Secure ACS generate a Windows event when a user attempts to log in to your network using a disabled account, check the **Generate event when an attempt is made to log in to a disabled account** box.

Step 5   If you are done setting up Cisco Secure ACS Service Management, click **Submit**.

Cisco Secure ACS implements the service management settings you made.

Setting Up Event Logging

To view the Windows event log, select **Start > Programs > Administrative Tools > Event Viewer**. For more information about the Windows event log or Event Viewer, refer to your Microsoft Windows documentation.

To set up Cisco Secure ACS event logging, follow these steps:

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

Step 2   Click **ACS Service Management**. The ACS Active Service Management Setup page appears.

Step 3   To have Cisco Secure ACS send all events to the Windows event log, choose **Log all events to the Windows Event log**.

Step 4   To have Cisco Secure ACS send an e-mail when an event occurs, follow these steps:

1. Check the **Email notification of event** box.

2. In the **To** box, type the e-mail address (up to 200 characters) to which Cisco Secure ACS should send event notification e-mail.

Note   Do not use an underscore in the e-mail addresses you type in this box.

---

3. In the SMTP Mail Server box, type the hostname (up to 200 characters) of the sending e-mail server.

Note	The SMTP mail server must be operational and must be available from the Cisco Secure ACS.

Step 5 When you are done setting up Cisco Secure ACS Service Management, click **Submit**.

Cisco Secure ACS implements the service management settings you made.

How Database Synchronization Works

ACS supports the use of an external ODBC database for the automation of your ACS configuration. Two components facilitate this process: CSDBsync, which is the process that actually performs the synchronization, and the accountActions table, which contains a set of rows that define actions CSDBSync is to perform in the Cisco Secure user database.

The synchronization with an external database allows you to configure the following, based on values contained in the External Database table:

- Users

- User groups

- Network configuration

- Custom RADIUS vendors and VSAs

For users, you can configure the following attributes:

- Adding a user

- Deleting a user

- Setting passwords

- Setting user group membership

- Setting max sessions parameters

- Setting network usage quota parameters

- Configuring command authorization

- Configuring network access restrictions

- Configuring time-of-day/day-of-week access restrictions

- Assigning IP addresses

- Specifying outbound RADIUS attribute values

- Specifying outbound TACACS+ attribute values

For user groups, you can configure the following parameters:

- Setting max sessions parameters

- Setting network usage quota parameters

- Configuring command authorization

- Configuring network access restrictions

- Configuring time-of-day/day-of-week access restrictions

- Specifying outbound RADIUS attribute values

- Specifying outbound TACACS+ attribute values

For network configuration, you can configure the following:

- Adding an AAA client
- Deleting an AAA client
- Setting AAA client configuration details
- Adding an AAA server
- Deleting an AAA server
- Setting AAA server configuration details
- Adding and configuring Proxy Distribution Table entries

For custom RADIUS vendors and VSAs, ACS allows you to create up to ten IETF-compliant RADIUS vendors, and all of the VSAs that you add for those servers must be sub-attributes of IETF RADIUS attribute number 26.

Components of Synchronization

When you perform database synchronization, two components work together, the CSDBsync process and the accountActions table. This section should help you better understand what role each component has in the synchronization process, and how the two together to facilitate synchronization.

CSDBsync is a service that ACS runs to perform automated user and group account management. This service works by using the ODBC DSN driver to access the accountActions table. The accountActions table holds information that is needed by CSDBsync.

The accountActions table is a table on the external ODBC server that contains a set of rows that define what actions CSDBSync performs in ACS.

The basic process of CSDBSync and the accountActions table working together is based on an action in the accountActions table. The most common actions are SET_VALUE and DELETE_VALUE. The SET_VALUE has an action code of 1 and the DELETE_VALUE has an action code of 2. CSDBSync reads the accountActions table for a configuration item, such as username, and the action code that goes with that item to determine if it is to add or delete that item from the ACS. Each item is then deleted from the RDBMS database.

Cisco recommends that for backup purposes, you create another table and mirror each transaction with CSDBSync to that table. Ensure that you back up this table frequently. Also, ensure that you perform frequent backups of the ACS database.

Configuring Database Synchronization

Before you perform synchronization, you need to complete a few tasks. These tasks enable the ACS to use CSDBSync to communicate with the accountActions table:

Step 1 Determine where you will create the accountActions table and the format you will use (For example, Access, CSV, Oracle 8, or SQL Server 6.5).

Step 2 Create the accountActions table on the third-party system.

Step 3 Create any stored procedures that might be necessary to populate the accountActions table. Refer to the user guide for more detailed information on these stored procedures.

The mechanism for maintaining your accountActions table is unique to your implementation. For information about the format and content of the accountActions table, see RDBMS Synchronization Import Definitions in the ACS user guide.

Step 4 Validate your third-party system to ensure that it updates the accountActions table properly. Rows generated in the accountActions table must be valid.

Step 5 Setup a system DSN on the ACS.

Step 6 Schedule RDBMS synchronization in ACS. These steps are discussed in the next section.

Step 7 Configure your external database to begin updating the accountActions table with the information that you want imported into the ACS user database.

Step 8 For troubleshooting, use the RDBMS Synchronization report in the Reports and Activity section. Additionally, you can monitor the CSDBSync service log.

RDBMS Synchronization Options

To enable RDBMS synchronization, go to the **Interface Configuration** section, and click the **Advanced Options** link. Once enabled, you will find an RDBMS Synchronization link in System Configuration. To begin configuring RDBMS Synchronization, click the **RDBMS Synchronization** link on the System Configuration page. Choose a DSN from the RDBMS Setup drop-list (this should already be configured). Also, type the username and password for the ODBC connection in the corresponding boxes.

Next, choose the synchronization options from the Synchronization Scheduling heading. Here, you can choose a manual synchronization, or schedule synchronization based on a time interval or by choosing timeslots from the time grid provided.

Finally, select the AAA server from the list of available servers on the left, and click -> (right-arrow button) to place them in the Partners column. This allows all partner device information to be synchronized.

Note that you can click the **Submit** button to schedule synchronization, or click the **Synchronize Now** button to force a manual synchronization.

This completes the configuration of synchronization. For more detailed information on synchronization, refer to the user guide provided with your ACS, as well as the vendor documentation for your ODBC RDBMS system.

Import Tools for Large-Scale Deployments

This topic describes Import Tools for Large-Scale Deployments.

Location of CSUtil.exe and Related Files

When you install Cisco Secure ACS in the default location, CSUtil.exe is located in the following directory: C:\Program Files\Cisco Secure ACS v*X.X*\Utils (where *X.X* is the version of your Cisco Secure ACS software). Regardless of where you install Cisco Secure ACS, CSUtil.exe is located in the Utils directory. Files generated by, or accessed by, CSUtil.exe are also located in the Utils directory.

CSUtil.exe Syntax

The syntax for the CSUtil.exe command is as follows:

CSUtil.exe [-q] [-c] [-d] [-g] [-i *filename*] **[[-p] -l** *filename*] **[-e** *-number*]

[-b *filename*] **[-r** *filename*] **[-f] [-n] [-u] [-x] [-y] [-listUDV] [-addUDV** *slot filename*]

[-delUDV slot] [-t -filepath *full filepath*] **[-passwd** *password*] **{-a | -g** *group number* |

-u *username* | **-f** *user list filepath*}] **[-addAVP** *filename*]

[-delAVP *vendor-ID application-ID attribute-ID*] **[-dumpAVP** *filename*]

Note	Most CSUtil.exe options require that you stop the CSAuth service. While the CSAuth service is stopped, Cisco Secure ACS does not authenticate users. To determine if an option requires that you stop CSAuth, refer to the detailed topics about the option. For a list of options and references to the detailed topics about each option, see CSUtil.exe Options at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae. htm#wp364488.

You can combine many of the options in a single use of CSUtil.exe. If you are new to using CSUtil.exe, we recommend performing only one option at a time, with the exception of those options, such as -p, that must be used in conjunction with other options.

Experienced CSUtil.exe users may find it useful to combine CSUtil.exe options, such as in the following example, which would first import AAA client configurations and then generate a dump of all Cisco Secure ACS internal data:

CSUtil.exe -i newnases.txt -d

CSUtil.exe Options

CSUtil.exe can perform several actions. The options, listed below in alphabetical order, are detailed in later sections of this chapter.

- **-b** – Backup system to a specified filename.

Note	For more information about performing a dump of the database, see Creating a Cisco Secure ACS Database Dump File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp417749.

- **-c** – Recalculate database CRC values.

- **-d** – Export all Cisco Secure ACS internal data to a file named `dump.txt`. Using this option requires that you stop the CSAuth service.

- **-e** – Decode internal Cisco Secure ACS error numbers to an ASCII text message.

- **-g** – Export group information to a file named `groups.txt`. Using this option requires that you stop the CSAuth service.

- **-i** – Import user or AAA client information from a file named `import.txt` or a specified file.

- **-l** – Load all Cisco Secure ACS internal data from a file named `dump.txt` or named file. Using this option requires that you stop the CSAuth service.

Note	For more information about this option, see Loading the Cisco Secure ACS Database from a Dump File at : www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp364902.

- **-n** – Create Cisco Secure user database and index. Using this option requires that you stop the CSAuth service.

- **-p** – Reset password aging counters during database load, to be used only in conjunction with the -l option.

- **-q** – Run CSUtil.exe without confirmation prompts.

- **-r** – Restore system from a specified backup filename.

- **-t** – Generate PAC files for EAP-FAST end-user clients.

- **-u** – Export user information, sorted by group membership, to a file named `users.txt`. Using this option requires that you stop the CSAuth service.

- **-x** – Display command-line syntax.

- **-y** – Dump Windows Registry configuration information to a file named `setup.txt`.

- **-addUDV** – Add a user-defined RADIUS vendor-specific attribute (VSA).

- **-delUDV** – Delete a user-defined RADIUS VSA.

- **-listUDV** – List all user-defined RADIUS VSAs currently defined in Cisco Secure ACS.

- **-addAVP** – Add or modify a posture validation attribute.

- **-delAVP** – Delete a posture validation attribute.

- **-dumpAVP** – Export all posture validation attributes.

Displaying Command-Line Syntax

CSUtil.exe displays command-line syntax for any one of the following reasons:

■ The -x option is included in the CSUtil.exe command.

■ No options are included with the CSUtil.exe command.

■ Incorrect syntax is used with the CSUtil.exe command.

Note	For more information about CSUtil.exe syntax, see CSUtil.exe Syntax at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp364500.

To display command-line syntax for CSUtil.exe, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Note	For more information about the location of CSUtil.exe, see Location of CSUtil.exe and Related Files at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp364488.

Step 2   Type **CSUtil.exe -x**. Press **Enter**. CSUtil.exe displays its command-line syntax.

Backing Up Cisco Secure ACS with CSUtil.exe

You can use the -b option to create a system backup of all Cisco Secure ACS internal data. The resulting backup file has the same data as the backup files produced by the ACS Backup feature found in the HTML interface.

Note	For more information about the ACS Backup feature, see Cisco Secure ACS Backup at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/sba.htm#wp222373.

Note	During the backup, all services are automatically stopped and restarted. No users are authenticated while the backup is occurring.

To backup Cisco Secure ACS with CSUtil.exe, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   Type **CSUtil.exe -b** *filename* (where *filename* is the name of the backup file). Press **Enter**. CSUtil.exe displays a confirmation prompt.

Step 3   To confirm that you want to perform a backup and to halt all Cisco Secure ACS services during the backup, type **Y** and press **Enter**.

CSUtil.exe generates a complete backup of all Cisco Secure ACS internal data, including user accounts and system configuration. This process may take a few minutes.

Note	CSUtil.exe displays the error message "Backup Failed" when it attempts to back up components of Cisco Secure ACS that are empty, such as when no administrator accounts exist. These apply only to components that are empty, not to the overall success or failure of the backup.

Restoring Cisco Secure ACS with CSUtil.exe

You can use the -r option to restore all Cisco Secure ACS internal data. The backup file from which you restore Cisco Secure ACS can be one generated by the CSUtil.exe -b option or by the ACS Backup feature in the HTML interface.

Cisco Secure ACS backup files contain two types of data:

- User and group data.
- System configuration.

You can restore either user and group data or system configuration, or both.

Note	During the restoration, all services are automatically stopped and restarted. No users are authenticated while the restoration is occurring.

To restore Cisco Secure ACS with CSUtil.exe, follow these steps:

Step 1 On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2 Perform one of the following:

— To restore all data (user and group data, and system configuration), type **CSUtil.exe -r all** *filename* (where *filename* is the name of the backup file). Press **Enter**.

— To restore only user and group data, type **CSUtil.exe -r users** *filename* (where *filename* is the name of the backup file). Press **Enter**.

— To restore only the system configuration, type **CSUtil.exe -r config** *filename* (where *filename* is the name of the backup file). Press **Enter**.

CSUtil.exe displays a confirmation prompt.

Step 3 To confirm that you want to perform a restoration and to halt all Cisco Secure ACS services during the restoration, type **Y** and press **Enter**.

CSUtil.exe restores the specified portions of your Cisco Secure ACS data. This process may take a few minutes.

Note	If the backup file is missing a database component, CSUtil.exe displays an error message. Such an error message applies only to the restoration of the missing component. The absence of a database component in a backup is usually intentional and indicates that the component was empty in Cisco Secure ACS at the time the backup was created.

Creating a Cisco Secure User Database

You can use the -n option to create a Cisco Secure user database.

Note   Using the -n option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

Caution   Using the -n option erases all user information in the Cisco Secure user database. Unless you have a current backup or dump of your Cisco Secure user database, all user accounts are lost when you use this option.

To create a Cisco Secure user database, follow these steps:

Step 1   If you have not performed a backup or dump of the Cisco Secure user database, do so now before proceeding.

Step 2   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 3   If the CSAuth service is running, type **net stop csauth** and press **Enter**. The CSAuth service stops.

Step 4   Type **CSUtil.exe -n** and press **Enter**. CSUtil.exe displays a confirmation prompt.

Step 5   To confirm that you want to initialize the Cisco Secure user database, type **Y** and press **Enter**. The Cisco Secure user database is initialized. This process may take a few minutes.

Step 6   To resume user authentication, type **net start csauth** and press **Enter**.

Creating a Cisco Secure ACS Database Dump File

You can use the -d option to dump all contents of the Cisco Secure user database into a text file. In addition to providing a thorough, eye-readable, and compressible backup of all Cisco Secure ACS internal data, a database dump can also be useful for the Cisco Technical Assistance Center (TAC) during troubleshooting.

Using the -l option, you can reload the Cisco Secure ACS internal data from a dump file created by the -d option.

Note   For more information about the -l option, see Loading the Cisco Secure ACS Database from a Dump File at
www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp364902.

Note   Using the -d option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To dump all Cisco Secure ACS internal data into a text file, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   If the CSAuth service is running, type **net stop csauth** and press **Enter**. The CSAuth service stops.

Step 3   Type **CSUtil.exe -d** and press **Enter**. CSUtil.exe displays a confirmation prompt.

Step 4   To confirm that you want to dump all Cisco Secure ACS internal data into dump.txt, type Y and press **Enter**. CSUtil.exe creates the dump.txt file. This process may take a few minutes.

Step 5   To resume user authentication, **type net start csauth** and press **Enter**.

Loading the Cisco Secure ACS Database from a Dump File

You can use the -l option to overwrite all Cisco Secure ACS internal data from a dump text file. This option replaces all the existing Cisco Secure ACS internal data with the data in the dump text file. In effect, the -l option initializes all Cisco Secure ACS internal data before loading it from the dump text file. Dump text files are created using the -d option. While the -d option only produces dump text files that are named `dump.txt`, the -l option allows for loading renamed dump files.

Note	For more information about creating dump text files, see Creating a Cisco Secure ACS Database Dump File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp417749.

You can use the -p option in conjunction with the -l option to reset password-aging counters.

Note	Using the -l option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To load all Cisco Secure ACS internal data from a text file, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   If the CSAuth service is running, type **net stop csauth** and press **Enter**. The CSAuth service stops.

Step 3   Type **CSUtil.exe -l** *filename* (where *filename* is the name of the dump file you want CSUtil.exe to use to load Cisco Secure ACS internal data). Press **Enter**. CSUtil.exe displays a confirmation prompt for overwriting all Cisco Secure ACS internal data with the data in the dump text file.

Note	Overwriting the database does not preserve any data; instead, after the overwrite procedure, the database contains only what is specified in the dump text file.

Step 4 To confirm that you want to replace all Cisco Secure ACS internal data, type **Y** and press **Enter**. CSUtil.exe initializes all Cisco Secure ACS internal data, and then loads Cisco Secure ACS with the information in the dump file specified. This process may take a few minutes.

Step 5 To resume user authentication, type **net start csauth** and press **Enter**.

Compacting the Cisco Secure User Database

Like many relational databases, the Cisco Secure user database handles the deletion of records by marking deleted records as deleted but not removing the records from the database. Over time, your Cisco Secure user database may be substantially larger than is required by the number of users it contains. To reduce the Cisco Secure user database size, you can compact it periodically.

Compacting the Cisco Secure user database consists of using three CSUtil.exe options in conjunction:

- **-d** – Export all Cisco Secure ACS internal data to a text file named `dump.txt`.
- **-n** – Create a Cisco Secure user database and index.
- **-l** – Load all Cisco Secure ACS internal data from a text file. If you do not specify the filename, CSUtil.exe uses the default file name `dump.txt`.

Additionally, if you want to automate this process, consider using the -q option to suppress the confirmation prompts that otherwise appear before CSUtil.exe performs the -n and -l options.

Note Compacting the Cisco Secure user database requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To compact the Cisco Secure user database, follow these steps:

Step 1 On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2 If the CSAuth service is running, type **net stop csauth** and press **Enter**. The CSAuth service stops.

Step 3 Type **CSUtil.exe -d -n –l**. Press **Enter**.

Tip If you include the -q option in the command, CSUtil.exe does not prompt you for confirmation of initializing or loading the database.

If you do not use the -q option, CSUtil.exe displays a confirmation prompt for initializing the database and then for loading the database.

Note For more information about the effects of the -n option, see Creating a Cisco Secure Internal Database at :
www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp364773.

Step 4   For each confirmation prompt that appears, type **Y** and press **Enter**.

CSUtil.exe dumps all Cisco Secure ACS internal data to `dump.txt`, initializes the Cisco Secure user database, and reloads all Cisco Secure ACS internal data from `dump.txt`. This process may take a few minutes.

Step 5   To resume user authentication, type **net start csauth** and press **Enter**.

User and AAA Client Import Option

The -i option enables you to update Cisco Secure ACS with data from a colon-delimited text file. You can also update AAA client definitions.

For user accounts, you can add users, change user information such as passwords, or delete users. For AAA client definitions, you can add or delete AAA clients.

This section contains the following topics:

- Importing User and AAA Client Information
- User and AAA Client Import File Format
- About User and AAA Client Import File Format
- ONLINE or OFFLINE Statement
- ADD Statements
- UPDATE Statements
- DELETE Statements
- ADD_NAS Statements
- DEL_NAS Statements
- Import File Example

Importing User and AAA Client Information

To import user or AAA client information, follow these steps:

Step 1   If you have not performed a backup or dump of Cisco Secure ACS, do so now before proceeding.

Step 2   Create an import text file.

Note   For more information about what an import text file can or must contain, see User and AAA Client Import File Format at :
www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp365198.

Step 3   Copy or move the import text file to the same directory as CSUtil.exe.

Step 4   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 5 Type **CSUtil.exe -i** *filename* (where *filename* is the name of the import text file you want CSUtil.exe to use to update Cisco Secure ACS). Press **Enter**. CSUtil.exe displays a confirmation prompt for updating the database.

Step 6 To confirm that you want to update Cisco Secure ACS with the information from the import text file specified, type **Y** and press **Enter**.

Cisco Secure ACS is updated with the information in the import text file specified. This process may take a few minutes.

If the import text file contained AAA client configuration data, CSUtil.exe warns you that you need to restart CSTacacs and CSRadius for these changes to take effect.

Step 7 To restart CSRadius, follow these steps:

1. Type **net stop csradius** and press **Enter**. The CSRadius service stops.

2. To start CSRadius, type **net start csradius** and press **Enter**.

Step 8 To restart CSTacacs, follow these steps:

1. Type **net stop cstacacs** and press **Enter**. The CSTacacs service stops.

2. To start CSTacacs, type **net start cstacacs** and press **Enter**.

User and AAA Client Import File Format

This section contains the following topics:

- About User and AAA Client Import File Format
- ONLINE or OFFLINE Statement
- ADD Statements
- UPDATE Statements
- DELETE Statements
- ADD_NAS Statements
- DEL_NAS Statements
- Import File Example

About User and AAA Client Import File Format

The import file can contain six different line types, as discussed in following topics. The first line of the import file must be one of the tokens defined in the ONLINE/OFFLINE Statement Tokens table.

Each line of a CSUtil.exe import file is a series of colon-separated tokens. Some of the tokens are followed by values. Values, like tokens, are colon-delimited. For tokens that require values, CSUtil.exe expects the value of the token to be in the colon-delimited field immediately following the token.

ONLINE or OFFLINE Statement

CSUtil.exe requires an ONLINE or OFFLINE token in an import text file. The file must begin with a line that contains only an ONLINE or OFFLINE token. The ONLINE and OFFLINE tokens are described in the ONLINE/OFFLINE Statement Tokens table below.

ONLINE/OFFLINE Statement Tokens			
Token	**Required**	**Value Required**	**Description**
ONLINE	Either ONLINE or OFFLINE must be present	—	The CSAuth service remains active while CSUtil.exe imports the text file. CSUtil.exe performance is slower when run in this mode, but Cisco Secure ACS continues to authenticate users during the import.
OFFLINE	Either ONLINE or OFFLINE must be present	—	The CSAuth service is stopped while CSUtil.exe imports the text file. Although CSUtil.exe performance is fastest in this mode, no users are authenticated during the import. If you need to import a large amount of user information quickly, consider using the OFFLINE token. While performing an import in the OFFLINE mode stops authentication during the import, the import is much faster. For example, importing 100,000 users in the OFFLINE mode takes less than one minute.

ADD Statements

ADD statements are optional. Only the ADD token and its value are required to add a user to Cisco Secure ACS. The valid tokens for ADD statements are listed in the table below.

Note   CSUtil.exe provides no means to specify a particular instance of an external user database type. If a user is to be authenticated by an external user database and Cisco Secure ACS has multiple instances of the specified database type, CSUtil.exe assigns the user to the first instance of that database type. For example, if Cisco Secure ACS has two LDAP external user databases configured, CSUtil.exe creates the user record and assigns the user to the LDAP database that was added to Cisco Secure ACS first.

ADD Statement Tokens			
Token	**Required**	**Value Required**	**Description**
ADD	Yes	username	Add user information to Cisco Secure ACS. If the username already exists, no information is changed.
PROFILE	No	group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name. If you do not use the PROFILE token or fail to provide a group number, the user is added to the default group.
CHAP	No	CHAP password	Require a CHAP password for authentication.

		ADD Statement Tokens	
Token	**Required**	**Value Required**	**Description**
CSDB	No	Password	Authenticate the username with the Cisco Secure user database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the Cisco Secure user database, using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows external user database.
EXT_NDS	No	—	Authenticate the username with a Novell NDS external user database.
EXT_SDI	No	—	Authenticate the username with an RSA external user database.
EXT_ODBC	No	—	Authenticate the username with an ODBC external user database.
EXT_LDAP	No	—	Authenticate the username with a generic LDAP external user database.
EXT_LEAP	No	—	Authenticate the username with a LEAP proxy RADIUS server external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following ADD statement would create an account with the username "John," assign it to Group 3, and specify that John should be authenticated by the Cisco Secure user database with the password "closedmondays":

ADD:John:PROFILE:3:CSDB:closedmondays

UPDATE Statements

UPDATE statements are optional. They make changes to existing user accounts. Only the UPDATE token and its value are required by CSUtil.exe, but if no other tokens are included, no changes are made to the user account. You can use the UPDATE statement to update the group a user is assigned to or to update which database Cisco Secure ACS uses to authenticate the user. The valid tokens for UPDATE statements are listed in the table on the next page.

UPDATE Statement Tokens			
Token	**Required**	**Value Required**	**Description**
UPDATE	Yes	Username	Update user information to Cisco Secure ACS.
PROFILE	No	Group number	Group number to which the user is assigned. This must be a number from 0 to 499, not a name. **Note**: If you do not specify a database token, such as CSDB or EXT_NT, updating a group assignment may erase a user's password.
CHAP	No	CHAP password	Require a CHAP password for authentication.
CSDB	No	Password	Authenticate the username with the Cisco Secure user database.
CSDB_UNIX	No	UNIX-encrypted password	Authenticate the username with the Cisco Secure user database, using a UNIX password format.
EXT_NT	No	—	Authenticate the username with a Windows external user database.
EXT_NDS	No	—	Authenticate the username with a Novell NDS external user database.
EXT_ODBC	No	—	Authenticate the username with an ODBC external user database.
EXT_LDAP	No	—	Authenticate the username with a generic LDAP external user database.
EXT_LEAP	No	—	Authenticate the username with a LEAP proxy RADIUS server external user database.
EXT_RADIUS	No	—	Authenticate the username with a RADIUS token server external user database.

For example, the following UPDATE statement causes CSUtil.exe to update the account with username "John," assign it to Group 50, specify that John should be authenticated by a UNIX-encrypted password, with a separate CHAP password "goodoldchap":

UPDATE:John:PROFILE:50:CSDB_UNIX:3Al3qf9:CHAP:goodoldchap

DELETE Statements

DELETE statements are optional. The DELETE token and its value are required to delete a user account from Cisco Secure ACS. The DELETE token is the only token in a DELETE statement.

UPDATE Statement Tokens			
Token	**Required**	**Value Required**	**Description**
DELETE	Yes	Username	The name of the user account that is to be deleted.

For example, the following DELETE statement causes CSUtil.exe to permanently remove the account with username "John" from the Cisco Secure user database: **DELETE:John**

ADD_NAS Statements

ADD_NAS statements are optional. The ADD_NAS, IP, KEY, and VENDOR tokens and their values are required to add an AAA client definition to Cisco Secure ACS. The valid tokens for ADD_NAS statements are listed below.

ADD_NAS Statement Tokens			
Token	**Required**	**Value Required**	**Description**
ADD_NAS	Yes	AAA client name	The name of the AAA client that is to be added.
IP	Yes	IP address	The IP address of the AAA client being added.
KEY	Yes	Shared secret	The shared secret for the AAA client.
VENDOR	Yes	See description	The authentication protocol the AAA client uses. For RADIUS, this includes the VSA. **Note**: The valid values are listed below. Quotation marks are required due to the spaces in the protocol names. ■ "TACACS+ (Cisco IOS)" ■ "RADIUS (Cisco Aironet)" ■ "RADIUS (Cisco BBSM)" ■ "RADIUS (Cisco IOS/PIX)" ■ "RADIUS (Cisco VPN 3000)" ■ "RADIUS (Cisco VPN 5000)" ■ "RADIUS (IETF)" ■ "RADIUS (Ascend)" ■ "RADIUS (Juniper)" ■ "RADIUS (Nortel)" ■ "RADIUS (iPass)"
NDG	No	NDG name	The name of the Network Device Group to which the AAA client is to be added.
SINGLE_CON	No	Y or N	For AAA clients using TACACS+ only, the value set for this TOKEN specifies whether the Single Connect TACACS+ AAA Client option is enabled.
KEEPALIVE	No	Y or N	For AAA clients using TACACS+ only, the value set for this token specifies whether the Log Update/Watchdog Packets from this Access Server option is enabled.

For example, the following ADD_NAS statement causes CSUtil.exe to add a AAA client with the name "SVR2-T+," using TACACS+ with the single connection and keep alive packet options enabled:

ADD_NAS:SVR2-T+:IP:*IP address***:KEY:***shared secret***:VENDOR:"TACACS+ (Cisco IOS)":NDG:"East**

Coast":SINGLE_CON:Y:KEEPALIVE:Y

Note   For more information, see Adding a AAA Client at::
www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/n.
htm#wp354890.

DEL_NAS Statements

DEL_NAS statements are optional. The DEL_NAS token is the only token in a DEL_NAS statement. DEL_NAS statements delete AAA client definitions from Cisco Secure ACS.

DEL_NAS Statement Tokens			
Token	**Required**	**Value Required**	**Description**
DEL_NAS	Yes	AAA client name	The name of the AAA client that is to be deleted.

For example, the following DEL_NAS statement causes CSUtil.exe to delete a AAA client with the name "SVR2-T+": **DEL_NAS:SVR2-T+**

Import File Example

The following is an example import text file:

OFFLINE

ADD:user01:CSDB:userpassword:PROFILE:1

ADD:user02:EXT_NT:PROFILE:2

ADD:chapuser:CSDB:hello:CHAP:chappw:PROFILE:3

ADD:mary:EXT_NT:CHAP:achappassword

ADD:joe:EXT_SDI

ADD:vanessa:CSDB:vanessaspassword

ADD:juan:CSDB_UNIX:unixpassword

UPDATE:foobar:PROFILE:10

DELETE:paul

ADD_NAS:SVR2-T+:IP:209.165.202.136:KEY:A87il032bzg:VENDOR:"TACACS+ (Cisco IOS)":NDG:"East Coast"

DEL_NAS:SVR16-RAD

Exporting User List to a Text File

You can use the -u option to export a list of all users in the Cisco Secure user database to a text file named `users.txt`. The `users.txt` file organizes users by group. Within each group, users are listed in the order that their user accounts were created in the Cisco Secure user database. For example, if accounts were created for Pat, Dana, and Lloyd, in that order, `users.txt` lists them in that order as well, rather than alphabetically.

Note	Using the -u option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To export user information from the Cisco Secure user database into a text file, follow these steps:

Step 1 On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2 If the CSAuth service is running, type **net stop csauth** and press **Enter**. The CSAuth service stops.

Step 3 Type **CSUtil.exe -u** and press **Enter**. CSUtil.exe exports information for all users in the Cisco Secure user database to a file named `users.txt`.

Step 4 To resume user authentication, type **net start csauth** and press **Enter**.

Exporting Group Information to a Text File

You can use the -g option to export group configuration data, including device command sets, from the Cisco Secure user database to a text file named `groups.txt`. The `groups.txt` file is useful primarily for debugging purposes while working with the TAC.

Note	Using the -g option requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

To export group information from the Cisco Secure user database to a text file, follow these steps:

Step 1 On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2 If the CSAuth service is running, type **net stop csauth** and press **Enter**. The CSAuth service stops.

Step 3 Type **CSUtil.exe -g** and press **Enter**. CSUtil.exe exports information for all groups in the Cisco Secure user database to a file named `groups.txt`.

Step 4 To resume user authentication, type **net start csauth** and press **Enter**.

Exporting Registry Information to a Text File

You can use the -y option to export Windows Registry information for Cisco Secure ACS. CSUtil.exe exports the Registry information to a file named `setup.txt`. The `setup.txt` file is primarily useful for debugging purposes while working with the TAC.

To export Registry information from Cisco Secure ACS to a text file, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   Type **CSUtil.exe -y** and press **Enter**.

CSUtil.exe exports Windows Registry information for Cisco Secure ACS to a file named `setup.txt`.

Decoding Error Numbers

You can use the -e option to decode error numbers found in Cisco Secure ACS service logs. These are error codes internal to Cisco Secure ACS. For example, the CSRadius log could contain a message similar to the following:

```
CSRadius/Logs/RDS.log:RDS 05/22/2001 10:09:02 E 2152 4756 Error -
1087 authenticating geddy
- no NAS response sent
```

In this example, the error code number that you could use CSUtil.exe to decode is "-1087":

```
C:\Program Files\Cisco Secure ACS vx.x\Utils: CSUtil.exe -e -1087
CSUtil v3.0(1.14), Copyright 1997-2001, Cisco Systems Inc
Code -1087 : External database reported error during
authentication
```

Note   The -e option applies to Cisco Secure ACS internal error codes only, not to Windows error codes sometimes captured in Cisco Secure ACS logs, such as when Windows authentication fails.

Note   For more information about Cisco Secure ACS service logs, see *Service Logs* at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/r.htm#wp551732.

To decode an error number from a Cisco Secure ACS service log, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   Type **CSUtil.exe -e –*number*** (where *number* is the error number found in the Cisco Secure ACS service log). Press **Enter**.

Note   The hyphen (-) before *number* is required.

CSUtil.exe displays the text message equivalent to the error number specified.

Recalculating CRC Values

The -c option is for use by the TAC. Its purpose is to resolve CRC (cyclical redundancy check) value conflicts between files manually copied into your Cisco Secure ACS directories and the values recorded in the Windows Registry.

Note Do not use the -c option unless a Cisco representative requests that you do.

User-Defined RADIUS Vendors and VSA Sets

This section provides information and procedures about user-defined RADIUS vendors and VSAs.

This section contains the following topics:

- About User-Defined RADIUS Vendors and VSA Sets
- Adding a Custom RADIUS Vendor and VSA Set
- Deleting a Custom RADIUS Vendor and VSA Set
- Listing Custom RADIUS Vendors
- Exporting Custom RADIUS Vendor and VSA Sets
- RADIUS Vendor/VSA Import File

About User-Defined RADIUS Vendors and VSA Sets

In addition to supporting a set of predefined RADIUS vendors and vendor-specific attributes (VSAs), Cisco Secure ACS supports RADIUS vendors and VSAs that you define. We recommend that you use RDBMS Synchronization to add and configure custom RADIUS vendors; however, you can use CSUtil.exe to accomplish the same custom RADIUS vendor and VSA configurations that you can accomplish using RDBMS Synchronization. Custom RADIUS vendor and VSA configuration created by either of these two features—RDBMS Synchronization or CSUtil.exe—can be modified by the other feature. Choosing one feature for configuring custom RADIUS vendors and VSAs does not preclude using the other feature.

Note For more information about RDMBS Synchronization, see RDBMS Synchronization at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/sad.htm#wp756877.

Vendors you add must be IETF-compliant; therefore, all VSAs that you add must be sub-attributes of IETF RADIUS attribute number 26. You can define up to ten custom RADIUS vendors, numbered 0 (zero) through 9. CSUtil.exe allows only one instance of any given vendor, as defined by the unique vendor IETF ID number and by the vendor name.

Note If you intend to replicate user-defined RADIUS vendor and VSA configurations, user-defined RADIUS vendor and VSA definitions to be replicated must be identical on the primary and secondary Cisco Secure ACS servers, including the RADIUS vendor slots that the user-defined RADIUS vendors occupy.

Adding a Custom RADIUS Vendor and VSA Set

You can use the -addUDV option to add up to ten custom RADIUS vendors and VSA sets to Cisco Secure ACS. Each RADIUS vendor and VSA set is added to one of ten possible user-defined RADIUS vendor slots.

| Note | While CSUtil.exe adds a custom RADIUS vendor and VSA set to Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated during this process. |

Before You Begin

■ Define a custom RADIUS vendor and VSA set in a RADIUS vendor/VSA import file.

| Note | For more information, see RADIUS Vendor/VSA Import File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp365780. |

■ Determine the RADIUS vendor slot to which you want to add the new RADIUS vendor and VSAs.

| Note | For more information, see Listing Custom RADIUS Vendors at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp365715. |

■ Make sure that regedit is not running. If regedit is running on the Cisco Secure ACS Windows server, it can prevent Registry updates required for adding a custom RADIUS vendor and VSA set.

To add a custom RADIUS VSA to Cisco Secure ACS, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   Type:
CSUtil.exe -addUDV *slot-number*
filename
Press **Enter**.

Slot-number is an unused Cisco Secure ACS RADIUS vendor slot and *filename* is the name of a RADIUS vendor/VSA import file. The *filename* can include a relative or absolute path to the RADIUS vendor/VSA import file. For example, to add the RADIUS vendor defined in d:\acs\myvsa.ini to slot 5, the command would be:

CSUtil.exe -addUDV 5 d:\acs\myvsa.ini

CSUtil.exe displays a confirmation prompt.

Step 3   To confirm that you want to add the RADIUS vendor and halt all Cisco Secure ACS services during the process, type **Y** and press **Enter**.

CSUtil.exe halts Cisco Secure ACS services, parses the vendor/VSA input file, and adds the new RADIUS vendor and VSAs to Cisco Secure ACS. This process may take a few minutes. After it is complete, CSUtil.exe restarts Cisco Secure ACS services.

Note	We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the Utils directory, where CSUtil.exe is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

Deleting a Custom RADIUS Vendor and VSA Set

You can use the -delUDV option to delete a custom RADIUS vendor from Cisco Secure ACS.

Note	While CSUtil.exe deletes a custom RADIUS vendor from Cisco Secure ACS, all Cisco Secure ACS services are automatically stopped and restarted. No users are authenticated while this process is occurring.

Before You Begin

Verify that, in the Network Configuration section of the Cisco Secure ACS HTML interface, no AAA client uses the RADIUS vendor.

Note	For more information about configuring AAA clients, see AAA Client Configuration at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/n.htm#wp342084.

Verify that your RADIUS accounting log does not contain attributes from the RADIUS vendor you want to delete.

Note	For more information about configuring your RADIUS accounting log, see Accounting Logs at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/r.htm#wp550598.

To delete a custom RADIUS vendor and VSA set from Cisco Secure ACS, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   Type **CSUtil.exe -delUDV** *slot-number* (where *slot-number* is the slot containing the RADIUS vendor that you want to delete). Press **Enter**.

CSUtil.exe displays a confirmation prompt.

Step 3   To confirm that you want to halt all Cisco Secure ACS services while deleting the custom RADIUS vendor and VSAs, type **Y** and press **Enter**. CSUtil.exe displays a second confirmation prompt.

Step 4   To confirm that you want to delete the RADIUS vendor, type **Y** and press **Enter**.

CSUtil.exe halts Cisco Secure ACS services, deletes the specified RADIUS vendor from Cisco Secure ACS. This process may take a few minutes. After it is complete, CSUtil.exe restarts Cisco Secure ACS services.

Listing Custom RADIUS Vendors

You can use the -listUDV option to determine what custom RADIUS vendors are defined in Cisco Secure ACS. This option also enables you to determine which of the ten possible custom RADIUS vendor slots are in use and which RADIUS vendor occupies each used slot.

To list all custom RADIUS vendors defined in Cisco Secure ACS, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   Type **CSUtil.exe -listUDV**. Press **Enter**.

CSUtil.exe lists each user-defined RADIUS vendor slot in slot number order. CSUtil.exe lists slots that do not contain a custom RADIUS vendor as "Unassigned." An unassigned slot is empty. You can add a custom RADIUS vendor to any slot listed as "Unassigned."

Exporting Custom RADIUS Vendor and VSA Sets

You can export all custom RADIUS vendors and VSA sets to files. Each vendor and VSA set is saved to a separate file. The files created by this option are in the same format as RADIUS vendor/VSA import files. This option is particularly useful if you need to modify a custom RADIUS vendor and VSA set and you have misplaced the original file used to import the set.

| Note | Exporting a custom RADIUS vendor and VSA set does not remove the vendor and VSA set from Cisco Secure ACS. |

Cisco Secure ACS places all exported vendor/VSA files in a subdirectory of the directory containing CSUtil.exe. The subdirectory is named System UDVs.

Each exported vendor/VSA file is named UDV_*n*.ini, where *n* is the slot number currently occupied by the custom RADIUS vendor and VSA set. For example, if vendor Widget occupies slot 4, the exported file created by CSUtil.exe is UDV_4.ini.

To export custom RADIUS vendor and VSA sets to files, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   Type **CSUtil.exe -dumpUDV**. Press **Enter**.

For each custom RADIUS vendor and VSA set currently configured in Cisco Secure ACS, CSUtil.exe writes a file in the System UDVs subdirectory.

RADIUS Vendor/VSA Import File

To import a custom RADIUS vendor and VSA set into Cisco Secure ACS, you must define the RADIUS vendor and VSA set in an import file. This section details the format and content of RADIUS VSA import files.

We recommend that you archive RADIUS vendor/VSA import files. During upgrades, the Utils directory, where CSUtil.exe is located, is replaced, including all its contents. Backing up RADIUS vendor/VSA import files ensures that you can recover your custom RADIUS vendors and VSAs after reinstallation or upgrading to a later release.

This section contains the following topics:

- About the RADIUS Vendor/VSA Import File
- Vendor and VSA Set Definition
- Attribute Definition
- Enumeration Definition
- Example RADIUS Vendor/VSA Import File

About the RADIUS Vendor/VSA Import File

RADIUS Vendor/VSA import files use a Windows .ini file format. Each RADIUS vendor/VSA import file comprises three types of sections, detailed in the following table. Each section comprises a section header and a set of keys and values. The order of the sections in the RADIUS vendor/VSA import file is irrelevant.

RADIUS VSA Import File Section Types			
Section	Required	Number	Description
Vendor and VSA set definition	Yes	1	Defines the RADIUS vendor and VSA set. For more information, see Vendor and VSA Set Definition at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp365827.
Attribute definition	Yes	1 to 255	Defines a single attribute of the VSA set. For more information, see Attribute Definition at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp365843.

RADIUS VSA Import File Section Types			
Section	**Required**	**Number**	**Description**
Enumeration	No	0 to 255	Defines enumerations for attributes with integer data types. For more information, see Enumeration Definition at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp431105.

Vendor and VSA Set Definition

Each RADIUS vendor/VSA import file must have one vendor and VSA set section. The section header must be "[User Defined Vendor]." The following table lists valid keys for the vendor and VSA set section.

Vendor and VSA Set Keys			
Keys	**Required**	**Value Required**	**Description**
Name	Yes	Vendor name	The name of the RADIUS vendor.
IETF Code	Yes	An integer	The IETF-assigned vendor number for this vendor.
VSA *n* (where *n* is the VSA number)	Yes – you can define 1 to 255 VSAs	Attribute name	The name of a VSA. For each VSA named here, the file must contain a corresponding attribute definition section.

Note	Attribute names must be unique within the RADIUS vendor/VSA import file and within the set of all RADIUS attributes in Cisco Secure ACS. To facilitate this, we recommend that you prefix the vendor name to each attribute name, such as "widget-encryption" for an encryption-related attribute for the vendor Widget. This also makes accounting logs easier to understand.

For example, the following vendor and VSA set section defines the vendor "Widget," whose IETF-assigned vendor number is 9999. Vendor Widget has 4 VSAs (thus requiring 4 attribute definition sections):

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
```

Attribute Definition

Each RADIUS vendor/VSA import file must have one attribute definition section for each attribute defined in the vendor and VSA set section. The section header of each attribute definition section must match the attribute name defined for that attribute in the vendor and VSA set section. The following table lists the valid keys for an attribute definition section.

Attribute Definition Keys			
Keys	**Required**	**Value Required**	**Description**
Type	Yes	See Description	The data type of the attribute. It must be one of the following: ■ STRING ■ INTEGER ■ IPADDR If the attribute is an integer, the Enums key is valid.
Profile	Yes	See Description	The attribute profile defines if the attribute is used for authorization or accounting (or both). At least one of the following two values must be present in the Profile key definition: ■ **IN** – The attribute is used for accounting. After you add the attribute to Cisco Secure ACS, you can configure your RADIUS accounting log to record the new attribute. For more information about RADIUS accounting logs, see Accounting Logs at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/r.htm#wp550598. ■ **OUT** – The attribute is used for authorization. In addition, you can use the value "MULTI" to allow several instances of the attribute per RADIUS message. Combinations are valid. For example: Profile=MULTI OUT or Profile=IN OUT
Enums	No (only valid when the TYPE value is INTEGER)	Enumerations section name	The name of the enumeration section.

Note   Several attributes can reference the same enumeration section. For more information, see Enumeration Definition at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp431105.

For example, the following attribute definition section defines the widget-encryption VSA, which is an integer used for authorization, and for which enumerations exist in the Encryption-Types enumeration section:

```
[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types
```

Enumeration Definition

Enumeration definitions enable you to associate a text-based name for each valid numeric value of an integer-type attribute. In the Group Setup and User Setup sections of the Cisco Secure ACS HTML interface, the text values you define appear in lists associated with the attributes that use the enumerations. Enumeration definition sections are required only if an attribute definition section references them. Only attributes that are integer-type attributes can reference an enumeration definition section.

The section header of each enumeration definition section must match the value of an Enums key that references it. An enumeration definition section can be referenced by more than one Enums key, thus allowing for reuse of common enumeration definitions. An enumeration definition section can have up to 1000 keys. This table lists the valid keys for an enumeration definition section.

Enumerations Definition Keys			
Keys	**Required**	**Value Required**	**Description**
n (See description.)	Yes	String	For each valid integer value of the corresponding attribute, an enumerations section must have one key. Each key defines a string value associated with an integer value. Cisco Secure ACS uses these string values in the HTML interface. For example, if 0 through 4 are valid integer values for a given attribute, its enumeration definition would contain the following: 0=*value0* 1=*value1* 2=*value2* 3=*value3* 4=*value4*

For example, the following enumerations definition section defines the Encryption-Types enumeration, which associates the string value 56-bit with the integer 0 and the string value 128-bit with the integer 1:

```
[Encryption-Types]
0=56-bit
1=128-bit
```

Example RADIUS Vendor/VSA Import File

The example RADIUS vendor/VSA import file, below, defines the vendor Widget, whose IETF number is 9999. The vendor Widget has five VSAs. Of those attributes, four are for authorization and one is for accounting. Only one attribute can have multiple instances in a single RADIUS message. Two attributes have enumerations for their valid integer values and they share the same enumeration definition section.

```
[User Defined Vendor]
Name=Widget
IETF Code=9999
VSA 1=widget-encryption
VSA 2=widget-admin-interface
VSA 3=widget-group
VSA 4=widget-admin-encryption
VSA 5=widget-remote-address

[widget-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-admin-interface]
Type=IPADDR
Profile=OUT

[widget-group]
Type=STRING
Profile=MULTI OUT

[widget-admin-encryption]
Type=INTEGER
Profile=OUT
Enums=Encryption-Types

[widget-remote-address]
Type=STRING
Profile=IN

[Encryption-Types]
0=56-bit
1=128-bit
2=256-bit
```

PAC File Generation

You can use the -t option to generate PAC files for use with EAP-FAST clients.

Note   For more information about PACs and EAP-FAST, see EAP-FAST Authentication at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/sau.htm#wp326311.

This section contains the following topics:

- PAC File Options and Examples
- Generating PAC Files

PAC File Options and Examples

When you use the -t option generate PAC files with CSUtil.exe, you have the following additional options.

- **User specification options** – While you can choose which user specification option you want to use, you **must** choose one of the four options for specifying which users you want PAC files for; otherwise, CSUtil.exe displays an error message because no users are specified. User specification options are as follows:

  — **-a** – CSUtil.exe generates a PAC file for each user in the Cisco Secure user database. For example, if you have 3278 users in the Cisco Secure user database and ran **CSUtil.exe -t -a**, CSUtil.exe would generate 3278 PAC files, one for each user.

Note　Using the -a option restarts the CSAuth service. No users are authenticated while CSAuth is unavailable.

  — **-g** *N* – CSUtil.exe generates a PAC file for each user in the user group specified by number (*N*). Cisco Secure ACS has 500 groups, numbered from 0 (zero) to 499. For example, if group 7 has 43 users and you ran **CSUtil.exe -t -g 7**, CSUtil.exe would generate 43 PAC files, one for each user who is a member of group 7.

Note　Using the -g option restarts the CSAuth service. No users are authenticated while CSAuth is unavailable.

  — **-u** *username* – CSUtil.exe generates a PAC file for the user specified by name (*username*). For example, if you ran **CSUtil.exe -t -u seaniemop**, CSUtil.exe would generate a single PAC file, named `seaniemop.pac`.

Tip　You can also specify a domain-qualified username, using the format *DOMAIN\username*. For example, if you specify `ENIGINEERING\augustin`, Cisco Secure ACS generates a PAC file name `ENGINEERING_augustin.pac`.

  — **-f** *list* – CSUtil.exe generates a PAC file for each username contained in the file specified, where *list* represents the full path and filename of the list of usernames.

  Lists of usernames should contain one username per line with no additional spaces or other characters.

  For example, if list.txt in d:\temp\pacs contains the following usernames:

  - seaniemop

  - jwiedman

  - echamberlain

  and you ran CSUtil.exe -t -f d:\temp\pacs\list.txt, CSUtil.exe generates three PAC files: `seaniemop.pac`, `jwiedman.pac`, and `echamberlain.pac`.

Tip　You can also specify domain-qualified usernames, using the format *DOMAIN\username*. For example, if you specify `ENIGINEERING\augustin`, Cisco Secure ACS generates a PAC file name `ENGINEERING_augustin.pac`.

— **-passwd** *password* – CSUtil.exe uses the password specified, rather than the default password, to protect the PAC files it generates. The password you specify is required when the PACs it protects are loaded into an EAP-FAST end-user client.

Note   We recommend that you use a password you devise rather than the default password.

PAC passwords are alphanumeric, between four and 128 characters long, and case-sensitive. While CSUtil.exe does not enforce strong password rules, we recommend that you use a strong password, that is, your PAC password should:

- Be very long.

- Contain uppercase and lowercase letters.

- Contain numbers in addition to letters.

- Contain no common words or names.

Generating PAC Files

Note   If you use the -a or -g option during PAC file generation, CSUtil.exe restarts the CSAuth service. No users are authenticated while CSAuth is unavailable.

Note   For more information about PACs, see About PACs at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/sau.htm#wp326451.

To generate PAC files, follow these steps:

Step 1   Use the discussion in PAC File Options and Examples at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp431168, to determine the following:

— Which users you want to generate PAC files for. If you want to use a list of users, create it now.

— What password you want to use to protect the PAC files you generate. If necessary, create a password. We recommend passwords that are long, use a combination of uppercase and lowercase letters, and include numbers.

— The full path to the directory you want the PAC files to be created in. If necessary, create the directory.

Step 2   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 3   Type **CSUtil.exe -t** *additional arguments* (where *additional arguments* represents at least one option for specifying for which users to generate PAC files). You can also use the options to specify filepath and password. Press **Enter**.

CSUtil.exe generates the PAC files for each user specified. The PAC files are named with the username plus a ".pac" file extension. For example, a PAC file for the username `seaniemop` would be `seaniemop.pac` and a PAC file for the domain-qualified username `ENGINEERING\augustin` would be `ENGINEERING_augustin.pac`.

If you specified a filepath, the PAC files are saved where you specified. You can distribute the PAC files to the applicable end-user clients.

Posture Validation Attributes

You can use CSUtil.exe to export, add, and delete posture validation attributes, which are essential to Network Admission Control (NAC).

Note   For more information about NAC, see Network Admission Control at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/nac.htm#wp24045.

This section contains the following topics:

- Posture Validation Attribute Definition File
- Exporting Posture Validation Attribute Definitions
- Importing Posture Validation Attribute Definitions
- Deleting a Posture Validation Attribute Definition
- Default Posture Validation Attribute Definition File

Posture Validation Attribute Definition File

A posture validation attribute definition file is a text file that contains one or more posture validation attribute definitions. Each definition consists of a definition header and several values, described below.

Note   For an example of the contents of a posture validation attribute definition file, see Default Posture Validation Attribute Definition File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp431258.

With the exception of the attribute definition header, each attribute definition value must be formatted as follows: *name=value* (where *name* is the value name and *value* is a string or integer, as specified in the list below).

Tip   Use a semi-colon to identify lines that are comments.

Here is an example of a posture validation attribute definition, including a comment after the attribute definition:

```
[attr#0]
vendor-id=9
vendor-name=Cisco
application-id=1
application-name=PA
attribute-id=00001
attribute-name=Application-Posture-Token
attribute-profile=out
attribute-type=unsigned integer
```

```
; attribute 1 is reserved for the APT
```

A posture validation attribute is uniquely defined by the combination of its vendor ID, application ID, and attribute ID. The following list provides details of these values and of each line required in an attribute definition:

- **[attr#*n*]** – Attribute definition header, where *n* is a unique, sequential integer, beginning with zero. CSUtil.exe uses the definition header to distinguish the beginning of a new attribute definition. Each attribute definition *must* begin with a line containing the definition header. The first attribute definition in the file *must* have the header `[attr#0]`, the second attribute definition in a file must have the header `[attr#1]`, and so on. A break in the numbering causes CSUtil.exe to ignore attribute definitions at the break and beyond. For example, in a file with ten attribute definitions, if the fifth attribute is defined as `[attr#5]` instead of `[attr#4]`, CSUtil.exe ignores the attribute defined as `[attr#5]` and the remaining five attributes following it.

Tip   The value of *n* is irrelevant to any of the ID values in the attribute definition file. For example, the 28th definition in a file must have the header `[attr#27]`, but this does not limit or otherwise define valid values for vendor-id, application-id, attribute-id. Neither does it limit or define the number of posture validation attributes supported by Cisco Secure ACS.

- **vendor-id** – An unsigned integer, the vendor number is of the vendor associated with the posture validation attribute. The vendor number should be the number assigned to the vendor in the IANA Assigned Numbers RFC. For example, vendor ID 9 corresponds to Cisco Systems, Inc.

    Vendor IDs have one or more applications associated with them, identified by the application-id value.

- **vendor-name** – A string: the vendor name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, any attribute definition with a vendor ID of 9 could have a vendor name "Cisco."

Note   The vendor name cannot differ for each attribute that shares the same vendor ID. For example, you cannot add an attribute with a vendor-id of 9 if the vendor-name is not "Cisco."

- **application-id** – An unsigned integer: the application ID uniquely identifies the vendor application associated with the posture validation attribute. For example, if the vendor ID is 9 and the application ID is 1, the posture validation attribute is associated with the Cisco application with an ID of 1, which is the Cisco Trust Agent (CTA) (also known as a posture agent [PA]).

- **application-name** – A string: the application name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, if the vendor ID is 9 and the application ID is 1, the application name would be "PA," an abbreviation of posture agent, which is another term for CTA.

Note   The application name cannot differ for each attribute that shares the same vendor ID and application ID pair. For example, you cannot add an attribute with a vendor-id of 9 and application ID of 1 if the application-name is not "PA."

- **attribute-id** – An unsigned integer in the range of 1 to 65535: the attribute ID uniquely identifies the posture validation attribute for the vendor ID and application ID specified.

Note	For each application, attributes 1 and 2 are reserved. If you add attributes that imply a new application, CSUtil.exe automatically creates attribute 1 as Application-Posture-Token and attribute 2 as System-Posture-Token.

- **attribute-name** – A string: the attribute name appears in the Cisco Secure ACS HTML interface and logs for the associated posture validation attribute. For example, if the vendor ID is 9, the application ID is 1, and the attribute ID is 1, the attribute name is "Application-Posture-Token."

- **attribute-profile** – A string: the attribute profile specifies whether Cisco Secure ACS can send the attribute in a posture validation response, can receive the attribute in a posture validation request, or can both send and receive the attribute during posture validation. Valid values for attribute-profile are:

  — **in** – Cisco Secure ACS accepts the attribute in posture validation requests and can log the attribute, and you can use it in local policy rule definitions. Attributes with an "in" attribute-profile are also known as inbound attributes.

  — **out** – Cisco Secure ACS can send the attribute in posture validation responses but you cannot use it in local policy rule definitions. Attributes with an "out" attribute-profile are also known as outbound attributes. The only outbound attributes that you can configure Cisco Secure ACS to log are the attributes for Application Posture Tokens and System Posture Tokens; however, these are system-defined attributes that you cannot modify.

  — **in out** – Cisco Secure ACS both accepts the attribute in posture validation requests and can send the attribute in posture validation responses. Attributes with an "in out" attribute-profile are also known as both inbound and outbound attributes.

- **attribute-type** – A string: the attribute type specifies the kind of data that are valid in the associated attribute. For attributes whose attribute-profile is `in` or `in out`, the attribute-type determines the types of operators available for defining local policy rules that use the attribute. An example of an inbound attribute is the ServicePacks attribute sent by CTA. An example of an outbound attribute is the System-Posture-Token attribute, sent to CTA.

  Valid values of attribute-type are:

  — boolean

  — string

  — integer

  — unsigned integer

  — ipaddr

  — date

  — version

  — octet-array

Note	For more information about attribute data types, see NAC Attribute Data Types at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/nac.htm#wp84199.

Exporting Posture Validation Attribute Definitions

The -dumpAVP option exports the current posture validation attributes to an attribute definition file.

Note	For an explanation of the contents of a posture validation attribute definition file, see Posture Validation Attribute Definition File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp431258.

Note	For an example of an attribute definition file, see Default Posture Validation Attribute Definition File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp431453.

To export posture validation attributes, follow these steps:

Step 1 On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2 Type **CSUtil.exe -dumpavp** *filename* (where *filename* is the name of the file in which you want CSUtil.exe to write all attribute definitions). Press **Enter**.

Tip	When you specify *filename*, you can prefix the filename with a relative or absolute path. For example, `CSUtil.exe -dumpavp c:\temp\allavp.txt` writes the file allavp.txt in c:\temp.

Step 3 If you are prompted to confirm overwriting a file with the same path and name that you specified in Step 2, do one of the following:

— To overwrite the file, type **Y** and press **Enter**.

Tip	To force CSUtil.exe to overwrite an existing file, use the -q option: **CSUtil.exe -q -dumpavp** *filename*.

— To preserve the file, type **N**, press **Enter**, and return to Step 2.

CSUtil.exe writes all posture validation attribute definitions in the file specified. To view the contents of the file, use the text editor of your choice.

Importing Posture Validation Attribute Definitions

The -addAVP option imports posture validation attribute definitions from an attribute definition file into Cisco Secure ACS.

Before You Begin

Because completing this procedure requires restarting the CSAuth service, which temporarily suspends authentication services, consider performing this procedure when demand for Cisco Secure ACS services is low.

Use the steps in Exporting Posture Validation Attribute Definitions to create a backup of posture validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of current posture validation attributes.

To import posture validation attributes, follow these steps:

Step 1   Use the discussion in Posture Validation Attribute Definition File to create a properly formatted attribute definition file. Place the file either in the directory containing CSUtil.exe or a directory accessible from the computer running Cisco Secure ACS.

Step 2   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 3   Type **CSUtil.exe -addavp** *filename* (where *filename* is the name of the file in which you want CSUtil.exe to write all attribute definitions). Press **Enter**.

Tip   When you specify *filename*, you can prefix the filename with a relative or absolute path. For example, `CSUtil.exe -addavp c:\temp\addavp.txt` writes the file addavp.txt in c:\temp.

CSUtil.exe adds or modifies the attributes specified in the file. An example of a successful addition of nine posture validation attributes follows:

```
C:.../Utils 21: csutil -addavp myavp.txt
CSUtil v3.3(1.6), Copyright 1997-2001, Cisco Systems Inc
Attribute 9876:1:11 (Calliope) added to registry
Attribute 9876:1:3 (Clio) added to registry
Attribute 9876:1:4 (Erato) added to registry
Attribute 9876:1:5 (Euterpe) added to registry
Attribute 9876:1:6 (Melpomene) added to registry
Attribute 9876:1:7 (Polyhymnia) added to registry
Attribute 9876:1:8 (Terpsichore) added to registry
Attribute 9876:1:9 (Thalia) added to registry
Attribute 9876:1:10 (Urania) added to registry

AVPs from 'myavp.txt' were successfully added
```

Step 4   If you are ready to make the imported attribute definitions take effect, restart the CSAuth and CSAdmin services.

Caution   While CSAuth is stopped, no users are authenticated.

To restart the CSAuth, CSLog, and CSAdmin services, enter the following commands at the command prompt, allowing the computer time to perform each command:

net stop csauth

net start csauth

net stop cslog

net start cslog

net stop csadmin

net start csadmin

Cisco Secure ACS begins using the imported posture validation attributes. Attributes that have an attribute type of `in` or `in out` are available in the HTML interface when you define local policy rules.

Deleting a Posture Validation Attribute Definition

The -delAVP option deletes a single posture validation attribute from Cisco Secure ACS.

Before You Begin

Because completing this procedure requires restarting the CSAuth service, which temporarily suspends authentication services, consider performing this procedure when demand for Cisco Secure ACS services is low.

Use the steps in Exporting Posture Validation Attribute Definitions, to create a backup of posture validation attribute definitions. You can also use the exported attribute definition file to double-check the vendor ID, application ID, and attribute ID of the posture validation attribute you want to delete.

To delete posture validation attributes, follow these steps:

Step 1   On the computer running Cisco Secure ACS, open a Windows command prompt and change directories to the directory containing CSUtil.exe.

Step 2   Type:

> **CSUtil.exe -delavp** *vendor-ID*
>
> *application-ID*
>
> *attribute-ID*

CSUtil.exe prompts you to confirm the attribute deletion.

Step 3   Examine the confirmation prompt and then do one of the following:

— If you are certain you want to delete the attribute identified by the confirmation prompt, type **Y** and press **Enter**.

Tip   You can use the -q option to suppress the confirmation prompt.

— If you do not want to delete the attribute identified by the confirmation prompt, type N, press Enter, and return to Step 2.

CSUtil.exe deletes from its internal database the posture validation attribute you specified. In the following example, CSUtil.exe deleted an attribute with a vendor ID of 9876, an application ID of 1, and an attribute ID of 1.

```
CSUtil v3.3, Copyright 1997-2004, Cisco Systems Inc
Are you sure you want to delete vendor 9876; application 1;
attribute 1? (y/n)
Y

Vendor 9876; application 1; attribute 1 was successfully deleted
```

Step 4   If you are ready to make the attribute deletion take effect, restart the CSAuth and CSAdmin services.

Caution   While CSAuth is stopped, no users are authenticated.

To restart the CSAuth, CSLog, and CSAdmin services, enter the following commands at the command prompt, allowing the computer time to perform each command:

net stop csauth

net start csauth

net stop cslog

net start cslog

net stop csadmin

net start csadmin

Deleted posture validation attributes are no longer available in Cisco Secure ACS.

Default Posture Validation Attribute Definition File

Example D-2 in the *User Guide for Cisco Secure ACS for Windows Server Version 4.0* provides the definitions for the posture validation attributes that Cisco provides with Cisco Secure ACS. If you need to reset the default attributes to their original definitions, you can copy the example to create a posture validation attribute definition file. See the References below for the URL of the example.

Summary

You should now be able to perform general system configuration. This ability includes being able to:

■ Understand how automatic service monitoring works

■ Configure automatic service monitoring

■ Understand how database synchronization works

■ Configure database synchronization

■ Understand how to use import tools for large scale deployments

References

For additional information, refer to the following resources:

■ Creating a Cisco Secure ACS Database Dump File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp417749.

■ Loading the Cisco Secure ACS Database from a Dump File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp364902.

■ Posture Validation Attribute Definition File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp431258.

■ Default Posture Validation Attribute Definition File at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp431453.

■ Location of CSUtil.exe and Related Files at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/ae.htm#wp364488.

Lesson 2

LDAP and ODBC User Authentication Support

Overview

Cisco Secure ACS for Windows 2000 and NT servers enables users to authenticate against external databases in preference to their internal databases. This allows a Cisco Secure ACS installation to "back end" into a variety of authentication sources, including Windows NT/2000, Novell Directory Services (NDS), Lightweight Directory Access Protocol (LDAP), various token-card servers, and Open Database Connectivity (ODBC) databases.

Objectives

Upon completing this lesson, you will be able to configure ODBC and LDAB database configurations. This ability includes being able to meet these objectives:

■   Understand and configure Cisco Secure ACS to use LDAP databases

■   Understand and configure Cisco Secure ACS to use ODBC databases

LDAP Databases

This topic describes how to configure ACS to use LDAP databases.

The Cisco Secure ACS can be configured to try other external user databases in case an authentication attempt fails against its internal list of users. You configure the external user databases you would like ACS to use in the Unknown User Policy, which is located in the external databases section of ACS. The external databases are attempted sequentially, in the configured order. Upon a successful authentication, the user is added to the Cisco Secure ACS internal database but marked for authentication by the appropriate database. For subsequent authentication attempts, ACS will try the supplied credentials against the previously successful external database.

One of the external databases that ACS supports is Generic LDAP, using standard LDAP to authenticate the users. This topic describes how to configure the Generic LDAP authenticator in Cisco Secure ACS.

LDAP Concepts

This section outlines a minimal set of LDAP concepts necessary for configuration derivation. If you are knowledgeable in LDAP you might want to skip this section.

LDAP Entries and Attributes

The objects or concepts that are represented in the LDAP information model are contained in entries. These can represent users, groups, printers, and so forth. Each entry is constructed entirely from a list of attributes. Each attribute has a type, and one or more values.
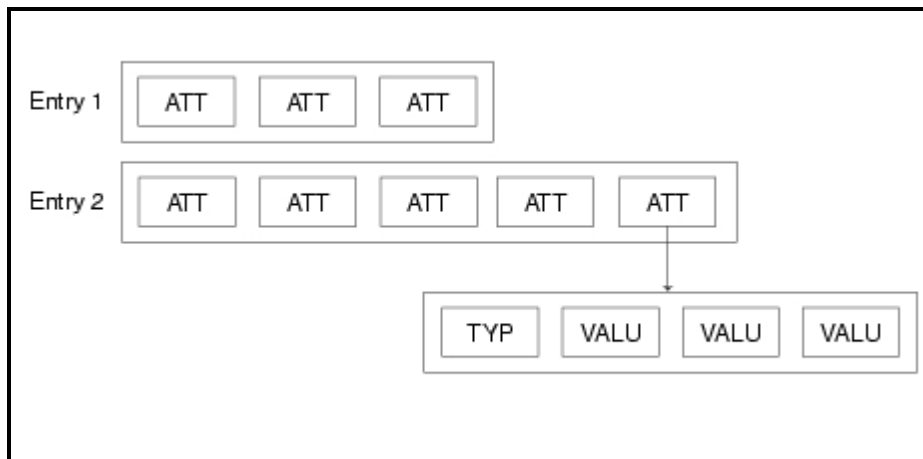
The directory server handles the special attributes objectClass, DistinguishedName, and passwords differently.

Each entry in the LDAP directory has an objectClass attribute. The LDAP directory server uses this attribute to determine the entry types (an entry can be of more than one type). The entry types, in turn, define which attributes are required and which are optional. This information, often embedded elsewhere in the directory, is generally referred to as the *schema*.
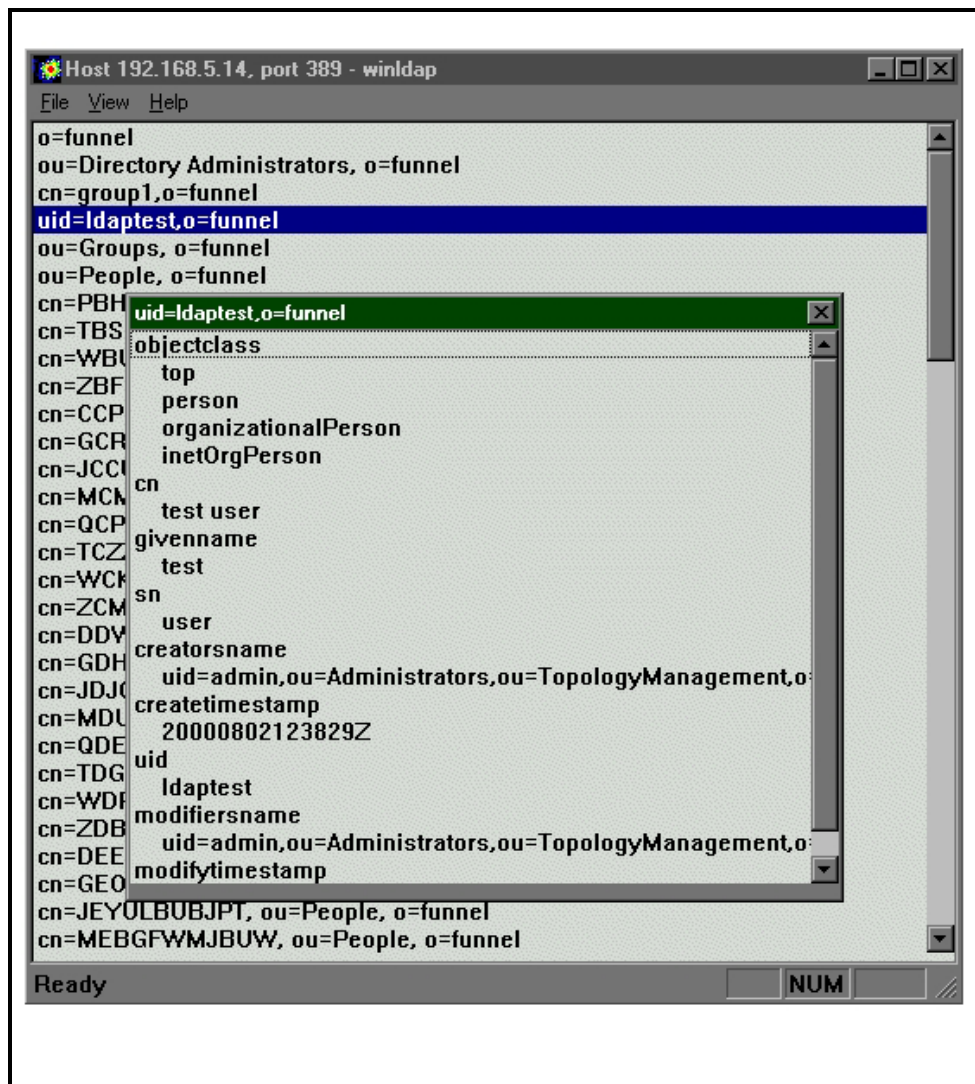
This is an example of the results when you examine a real entry in an LDAP server using a browser from the Netscape LDAP Software Development Kit (SDK). Most of the attributes are single values, but the objectClass attribute contains four values.

One important attribute not shown in the example is the "Distinguished Name" or *dn*. The dn uniquely identifies the entry among all entries in the directory. In fact, the dn is not always stored as a single attribute, but can be synthesized, at least partly, from other attributes. For instance, in the example screenshot, the uid attribute is used as part of the dn.

The dn can be constructed under a generous set of rules, and this permits great flexibility for the directory layout. Normally, however, a tree structure is imposed using a hierarchy of component elements within the dn. These elements are called Relative Distinguished Names and are formatted as a little endian set of attributes. For example:

dn = uid = Fred, ou = QA Department, ou = Access Products, o = cisco

Attributes containing passwords are normally hidden for security reasons. These are covered in more detail in the next section, LDAP Binding.

LDAP Binding

You typically configure LDAP directory servers so that the passwords are not exposed. However, to validate that the credentials or a user are correct, you can use a bind to authenticate a user against the directory. For more information on using a bind refer to ldap documentation. This mechanism, which you use to validate Cisco Secure ACS users, is effectively a logon to the directory.

Simple LDAP Search Filters

Knowledge of search filters is useful in understanding the configuration information required to correctly set up the Cisco Secure ACS. You use a search filter to specify which records are returned by the LDAP directory server. In the case of the Cisco Secure ACS, the search filter can be represented as a string whose format is defined in RFC 1960. The credentials of the user are not stored internally. The Cisco Secure ACS uses a restricted subset of this RFC.

Search filters are composed of attribute match requirements. For example, to construct a search filter to return all of the entries in a directory that contain an attribute called *uid* with one value equal to *testuser,* the filter would be: `(uid = testuser)`.

Filters can be logically conjoined; so to add a further qualification to the above filter that the objectClass of the entries to be returned is "Person," we have:

        `(&(uid = ldaptest)(objectClass = Person))`
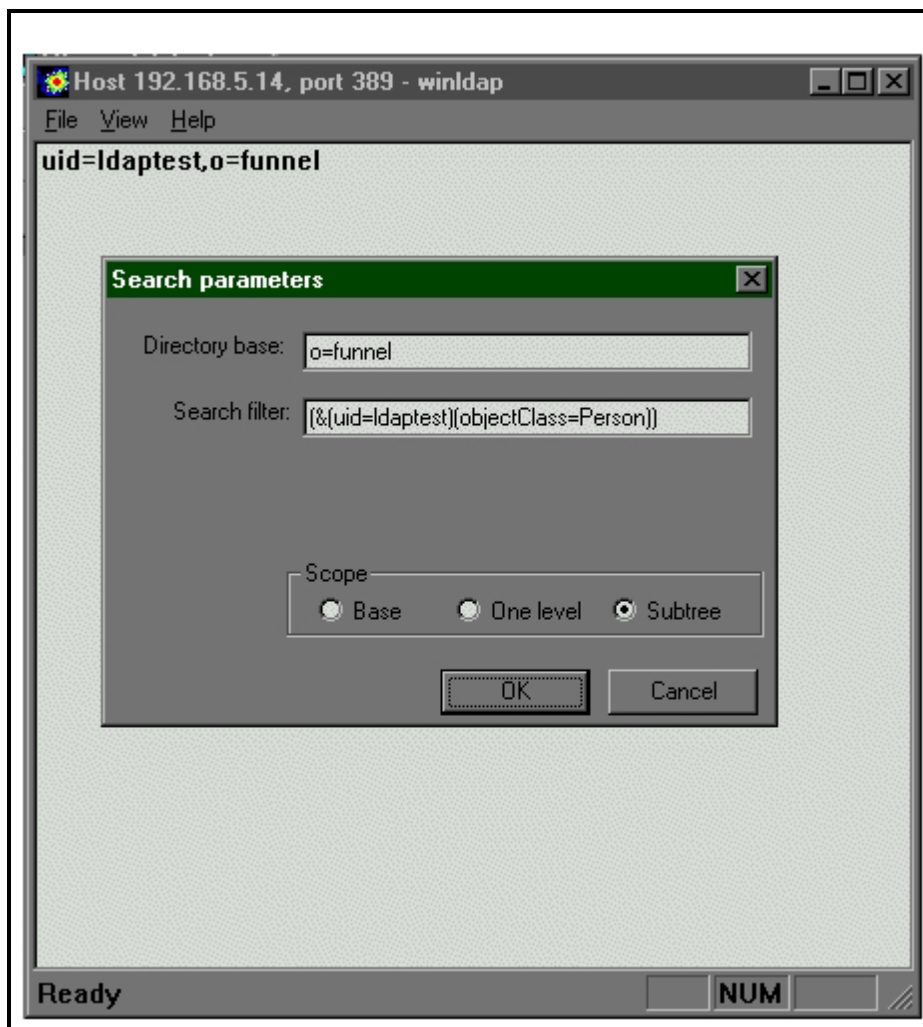
The example above shows the results of applying the search filter against a test directory.

LDAP Configuration

This section describes how the values required by the Cisco Secure ACS LDAP Database Configuration page are derived from the particular details of the target LDAP server. The configuration has been broken into two sections: information about the server and information about the schema.

LDAP Directory Server Information and Connection

The first two fields on the LDAP Database configuration page in External Databases, Hostname and Port, specify where the LDAP requests are sent. In the Hostname text box, type either the IP address or the DNS-resolvable hostname of the LDAP server. In the port box, type the TCP port to which the LDAP server listens.

LDAP Version

The Cisco Secure ACS negotiates with the LDAP server for a supported version. If this box is not checked, ACS does not try to negotiate using LDAP version 3, and will fall back to a previous version. By default, this box is checked.

Security Settings

LDAP communicates in plain text between the ACS server and the LDAP directory. You can configure this connection to use a Secure Socket Layer (SSL) if a certificate has been obtained. If the Security box is checked, you must provide the path to a certificate database. For further details on setting up SSL, see the Setting Up SSL topic in this module.

Administrator Credentials

To provide the authority necessary when obtaining group mapping information, you must provide authentication for an administrative entry that has permissions to search and retrieve the list of groups under a specified group subtree. You must fully qualify the admin dn. You can obtain an admin user who has permissions over the standard directory namespace for a Netscape directory from the Netscape console by clicking the **Users and Groups** tab, then clicking the **Directory** button in the field Bind DN. For a default installation, this is normally:

```
uid = admin, ou = Administrators, ou = TopologyManagement, o =
NetscapeRoot
```

This entry is space-sensitive.

Subtrees

There are two locations used as the root of the hierarchy for searching for users and groups, respectively. You must fully specify these locations in conventional distinguished name format. These locations are configured when the LDAP directory server is set up. Often these are left at the root level of the directory, that is: `o = cisco`.

Retrieving the Groups for a Specified Subtree Root

This search uses a filter (described in the Simple LDAP Search Filters section). This filter specifies that objects only return if their objectclass indicates that they are a group:

```
(objectclass = groupObjectClass)
```

For example, using the default Netscape schema where (groupObjectClass = GroupOfUniqueNames) and (objectClass = GroupOfUniqueNames), the value of the groupObjectClass field in the GUI must be equal to the value of the objectClass attribute in the target directory server that uniquely characterizes this entry as a group on the ldap server.

Logon

This search enables you to find users when given a login ID. It is performed during authentication so that you can perform a bind to validate the credentials, without the user needing to supply their complete, fully qualified name. The filter used for this search is as follows:

```
(&(objectclass = userObjectClass)( userObjectType = <<username>>))
```

For example, when authenticating user *testuser* and using the default Netscape schema, where userObjectType = *uid* and userObjectClass = *Person*, these values are substituted into the filter. In this scenario, the following filter would be constructed for this search:

```
(&(objectclass = Person)( uid = testuser))
```

Consequently, the value of the userObjectClass field in the GUI must be equal to the value of the objectClass attribute in the target directory server, which uniquely characterizes this entry as a user. Furthermore, the value of userObjectType must be the name of attribute whose value is the login name for the user object.

Retrieving Groups for a User

This search is performed after authentication to find groups that contain a membership attribute equal to the user being authenticated. The syntax of the filter is:

```
(&(objectclass = groupObjectClass)( groupAttribute = <<username>>))
```

For example, when authenticating user *testuser* and using the default Netscape schema, where GroupObjectClass = *GroupOfUniqueNames* and GroupAttribute = *UniqueMember*, these values are substituted into the filter. In this scenario, the following filter would be constructed for this search:

```
(&(objectclass = GroupOfUniqueNames)( UniqueMember = testuser))
```

The value of the userObjectClass field in the GUI is described above. The GroupAttribute name must be the name of the attribute in a group that contains the list of members of the group as its values.

Summary

This section has shown how the values put into the Cisco Secure ACS fit into LDAP searches. In summary:

Summary Table

Subhead	Subhead
UserObjectType	The name of the attribute in a user entry object, whose value is the login name for that user object.
UserObjectClass	The value of the objectClass attribute in the target Directory Server that uniquely characterizes this entry as a user.
GroupObjectType	The name of attribute in a group entry object whose value is the name for that group object.
GroupObjectClass	The value of the objectClass attribute in the target Directory Server that uniquely characterizes this entry as a group.
Group Attribute Name	The name of the attribute in a group that contains the list of members of the group as its values.

Setting Up SSL

This section describes how to set up Secure Socket Layer (SSL) when using the Netscape LDAP Directory Server and Certificate Management Server (CMS). This assumes that the LDAP Directory Server has already been set up for SSL using a certificate from the CMS. You can obtain externally-verified certificates and use those instead.

Fundamentally, this method uses a Netscape browser pointed at a specific SSL port on the directory server to obtain the certificate and install it in the certificate database (cert7.db).

Step 1   Enter the IP address or fully qualified domain name of the certificate server where the CA certificate resides.

Step 2   Make a request for a personal certificate.

Step 3   Enter the IP address or fully qualified domain name of the certificate server using port 444 to get a manual enrollment form. Fill in the details, and then send off the request.

Step 4   On the certificate server, verify this certificate request.

Step 5   On the intended SSL client, point the browser back to the certificate server on the agent port (this is installation-dependent, but the test CMS used port 8100). This imports the newly verified personal certificate.

Step 6   Point the browser back at the LDAP SSL port, and accept the certificate. Locate the certificate database file (cert7.db) used by the browser, and enter the full path (including filename) into the Certificate Database Path field in the Cisco Secure ACS GUI.

The LDAP Browser

The screenshots in this primer are from the sample browser in the Netscape LDAP Software Developer's Kit for Windows. The LDAP browser is a useful tool for validating that the

schema information is correct for the directory server to be used. The schema entries can be substituted into search filters.

For example, assuming that the groupObjectClass has been determined to be *GroupOfUniqueNames,* you can construct the search filter to mirror the search filter actually used in the Cisco Secure ACS (objectclass = GroupOfUniqueNames). The directory base is, in this case, the *Group Directory Subtree* value selected for ACS in the GUI.
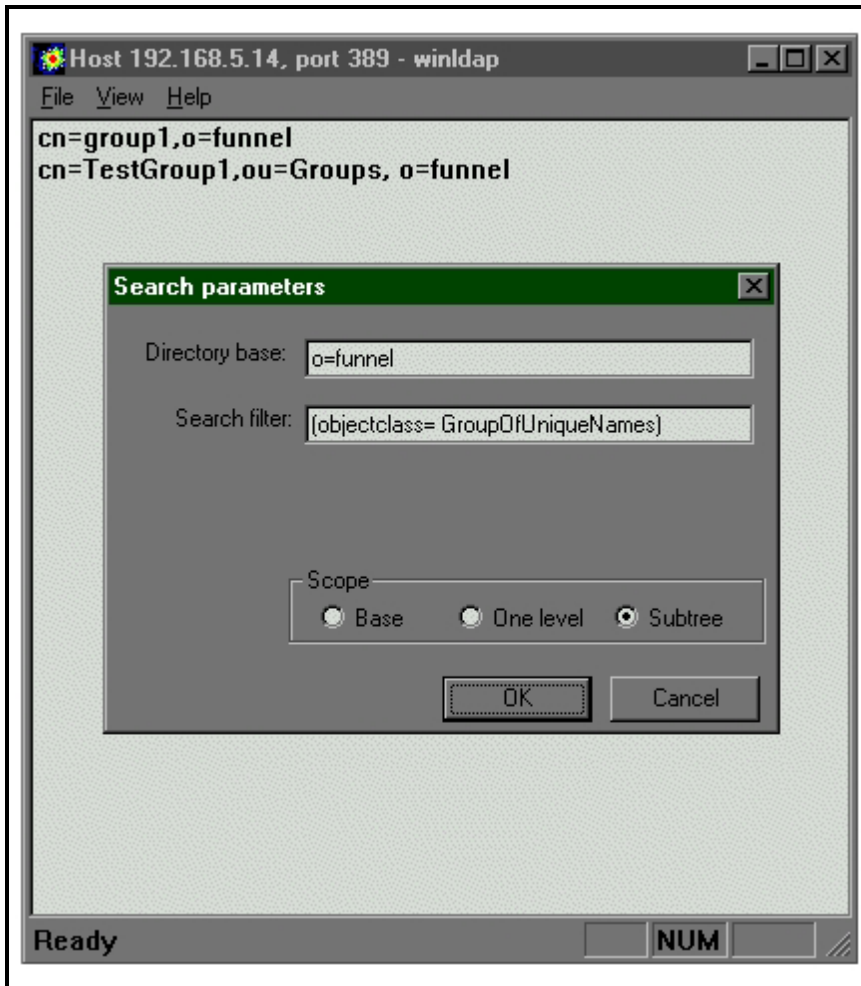
The scope for searches within the Cisco Secure ACS is always set at *Subtree* (i.e. a recursive search).

ODBC Databases

The ODBC external authenticator allows ACS to integrate with your RDBMS user database by defining the interface to a stored SQL procedure. This procedure, implemented by you, returns basic authentication pass/fail data back to the Cisco Secure ACS. Cisco Systems provides the template or "stub" procedure, but only you can complete it because the procedure must interact with one or more systems within your organization.

In addition to authenticating the user, the SQL procedure might return the number of the Cisco Secure ACS group to which the user is assigned. Cisco Secure ACS then applies the authorization and profile data of this group to the user before the requested service is granted.

Cisco Secure ACS uses a System Data Source Name (System DSN) configured locally in the ODBC32 Control Panel applet to access the stored SQL procedure.

Authentication Protocols Supported

Cisco Secure ACS supports the following authentication protocols via ODBC external authentication:

- PAP

- CHAP

- MSCHAP/MPPE

- ARAP

There are configuration implications between the PAP and CHAP/ARAP protocols.

Cisco Secure ACS Group Mapping

ODBC authentication has basic support for the assignment of a Cisco Secure ACS group. The SQL procedure may optionally return a group number that corresponds to a group within the Cisco Secure ACS configuration. By default Cisco Secure ACS groups are named Default Group, Group 1, Group 2, and so on, where the Default Group is numeric group 0.

Cisco Secure ACS Software Versions

Cisco Secure ACS version 2.3(1) was the first version to support ODBC authentication. This feature did not significantly change in Cisco Secure ACS 2.4(1), except for the addition of Oracle support. In Cisco Secure ACS 2.5(1) and later, the MSCHAP authentication protocol supports MPPE.

Supported Database Vendors

Although several standards govern the use of SQL, the following two different methods return data from a stored SQL procedure:

- Recordset, as used by Microsoft SQL Server and Access

- Output Parameters, as used by Oracle

The Cisco Secure ACS configuration (detailed in later sections) must be set appropriately for the RDBMS being used. For RDBMSs other than Microsoft SQL Server, Microsoft Access, or Oracle, refer to the RDBMS documentation to find out which method is used.

RDBMS/ODBC Configuration

The first step in ODBC configuration is to create the stored procedure within the RDBMS.

Depending on the authentication protocols required, one or two procedures may be required. For basic PAP authentication, the Cisco Secure ACS uses the PAP SQL procedure where the username and password are passed to the procedure for authentication. The default name for the PAP SQL procedure is *CSNTAuthUserPAP*. For CHAP, MSCHAP and ARAP, the ACS has to receive from the procedure a copy of the user's clear text password to perform authentication. The default name for the CHAP/MSCHAP/ARAP SQL procedure is *CSNTExtractClearTextPw*

Variable types used in the SQL procedures may have one or more matching SQL types; hence, assume the following:

- **Integer***:* SQL_INTEGER
- **String***:* SQL_CHAR and/or SQL_VARCHAR

The two procedures are defined in the following sections.

SQL Procedure Definitions:CSNTAuthUserPAP

Procedure Inputs

The procedure *CSNTAuthUserPAP* will take the following named input parameters:

- **CSNTusername:** String, 0–64 characters
- **CSNTpassword:** String, 0–255 characters

Note   The parameter names are for guidance only and may be changed; however, the order may not—the username must precede the password parameter.

Note   Passwords supplied via the RADIUS protocol are 0 - 128 characters.

Procedure Results

Depending on the procedure type (recordset- or parameter-based), the SQL procedure returns the following named values as either a single row or a set of named output parameters:

CSNTAuthUserPAP Procedure Results

Value	Description
CSNTresult	Integer.
CSNTgroup	Integer, ACS group number for Authorization. 0xFFFFFFFF (-1) used to assign default. Values outside the 0-499 range are converted to the default.
CSNTacctInfo	String, 0-15 characters, 3rd-party defined string added to subsequent accounting log file entries.
CSNTerrorString	String, 0-255 characters, 3rd-party defined string written to the ACS service log file on error.

The fields *CSNTgroup* and *CSNTacctInfo* are processed on a successful authentication only. Similarly, CSNTerrorString is logged only after a failure, where result >= 4.

SQL Procedure Definitions: CSNTExtractClearTextPw

Procedure Inputs

The procedure *CSNTExtractClearTextPw* takes the following named parameter:

CSNTusername: String, 0–64 characters

Procedure Results

Depending on the procedure type (recordset or parameter-based), the SQL procedure returns the following named values as either a single row or a set of named output parameters:

CSNTExtractClearTextPw Procedure Results

Subhead	Subhead
CSNTresult	Integer, see Procedure Result Codes below.
CSNTgroup	Integer, ACS group number for Authorization. 0xFFFFFFFF (-1) used to assign default. Values outside the 0-499 range will be converted to the default.
CSNTacctInfo	String, 0-15 characters, 3rd-party defined string added to subsequent accounting log file entries.
CSNTerrorString	String, 0-255 characters, 3rd-party defined string written to the ACS service log file on error.
CSNTpassword	String, 0-255 characters, password for use by ACS for (MS)CHAP/ARAP authentication.

The fields *CSNTgroup* and *CSNTacctInfo* are processed on a successful authentication only. Similarly, *CSNTerrorString* is logged only after a failure, where result >= 4 (see Procedure Result Codes).

Procedure Result Codes

One of the following result codes should be returned in the *CSNTresult* field.

- **0** (zero)**:** Authentication successful
- **1:** Username unknown
- **2:** Supplied password invalid
- **3:** Unknown username or password invalid
- **4+:** Internal procedure error – authentication not processed

Write your SQL procedures so that they decide among error code 1, 2, or 3 to indicate a failure, depending on how much information is to be included in the failed authentication log files.

A return code of 4 (or higher) results in an authentication error event. Result codes in this range can be returned to indicate that it was not possible to process the authentication because of some fault condition. Such errors do not increment per-user failed attempt counters. Also, error codes are returned to the NAS so that it can distinguish between errors and failures and (if configured) fail over to a backup Cisco Secure ACS or alternate AAA server.

RDBMS Login for ACS

After you have implemented the SQL procedures in the RDBMS, access should be granted to the procedures that is sufficient to allow the Cisco Secure ACS to run them via the System DSN created in the following section. This is typically done by creating a login account for use by the Cisco Secure ACS. The account will require execution rights on these procedures and may need other rights/permissions, depending on what actions the procedures perform. The account name and password are entered in the Cisco Secure ACS during its configuration process.

ODBC DSN

The Cisco Secure ACS communicates with the RDBMS using an ODBC driver running on the same server as the Cisco Secure ACS. With Windows 2000, this method is an integral part of the operating system; however, with Windows NT 4.0, it is not. The Cisco Secure ACS installer program automatically detects whether the ODBC driver is present. If the driver is not present, the installer displays an error message and you must exit the installation, install the ODBC driver, and restart the Cisco Secure ACS installation.

In Windows NT 4.0, the ODBC32 Data Source Administrator can be found in Control Panel. In Windows 2000, the ODBC32 Data Source Administrator is found on the Administrative Tools menu.
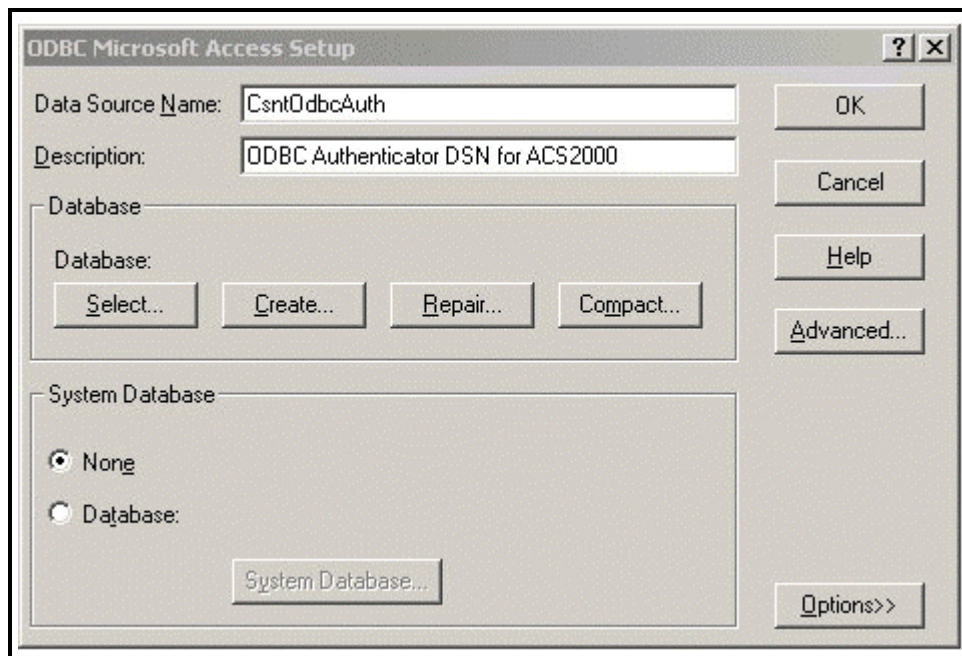
The ODBC DSN Administrator window has several tabs, including User DSN and System DSN. Because the Cisco Secure ACS runs as an NT service, it is important to create the DSN under the System DSN tab. The DSN specifies the RDBMS vendor (and hence which ODBC driver) and how to reach the database. For Microsoft Access, this is the location of the .mdb database file. For Microsoft SQL Server or Oracle, it may include the name/IP address of the computer on which the database resides. Detailed discussion about the configuration options is beyond the scope of this paper. For more information, please refer to your RDBMS documentation.

When configuring the Cisco Secure ACS, select the DSN name that is chosen during creation of the System DSN.

External User Databases

CiscoSecure ODBC Authentication Configuration.

ODBC Configuration	
System DSN:	CiscoSecure DBSync ▾
DSN Username:	acs2000
DSN Password:	***************
DSN Connection Retries:	3
ODBC Worker Threads:	1
DSN Procedure Type:	Returns Recordset ▾
☑ **Support PAP authentication**	
PAP SQL Procedure:	CSNTAuthUserPap
☐ **Support CHAP/MS-CHAP/ARAP authentication**	
CHAP SQL Procedure:	CSNTExtractUserClearTextPw
☐ **Support EAP-TLS authentication**	
EAP SQL Procedure:	CSNTFindUser

Submit   Cancel

ACS Configuration- Create External DB Config

The first step in configuring the Cisco Secure ACS is to create an instance of the ODBC external authenticator. From the ACS GUI home page navigation, choose the **External User Database** button, click the **Database Configuration** link**,** and then click **External ODBC Database**. If no configuration exists, click **Create New Configuration***,* type a configuration name in the text box, and click **Submit**. After you create the configuration, or if a configuration already exists, click **Configure**.

On the ODBC External Database Configuration page, choose the System DSN from the list. This should be the same System DSN configured previously in the ODBC32 Control Panel applet. If the correct DSN does not appear on the list, then it is likely that the DSN was created as a User DSN instead of System DSN.

Next, enter the RDBMS account name and password into the DSN Username and DSN Password fields, respectively. These are the credentials created for the Cisco Secure ACS within the RDBMS that allow the Cisco Secure ACS to run the stored procedures via the System DSN.

The Connection Retries and ODBC Worker Threads boxes should be left at their default values unless there are connectivity or performance issues. The Connection Retries value specifies

how many times the Cisco Secure ACS tries to connect to an ODBC data source upon failure. The ODBC Worker Threads value can be increased to create a set of pooled connections to the RDBMS; however, this can only be increased from the default if the ODBC driver in use is "thread safe." For example, the Microsoft Access ODBC is not thread safe, and the Cisco Secure ACS may become unstable if more than a single thread is used. Microsoft SQL Server and Oracle ODBC drivers are thread safe. For other ODBC drivers, refer to documentation supplied with the driver.

The DSN Procedure Type defines whether the RDBMS returns recordset or parameter data from SQL procedures. If your database is Microsoft SQL Server or Access choose **Returns Recordset**. If your database is an Oracle database, choose **Returns Parameters** from the drop-list.

Lastly, use the check-boxes to specify the authentication protocols to support, and then enter the SQL procedure name for each. The default procedure names appear in the procedure name text boxes; however, you can use any procedure name that matches the name of the procedure implemented in the RDBMS. At least one procedure must be implemented: PAP or CHAP/MS-CHAP/ARAP. If, for example, the PAP procedure is not implemented, the "Support PAP authentications" box should remain unchecked. Any PAP authentications will automatically fail with the message "Auth type not supported by External DB" logged in the Failed Attempts report.

When the ODBC External Database Configuration page is submitted, the Cisco Secure ACS attempts to connect to the DSN to check connectivity, but it does not check to ensure that the procedures specified in the procedure name text boxes exist in the RDBMS.

Default Group Mapping

If the SQL procedures are not coded to return a group assignment (or if they return an illegal value), the user is assigned to the default group for the ODBC External Database. From the Cisco Secure ACS home page navigation, choose the **External User Databases** button, click **Database Group Mappings**, then click **External ODBC Database**. Finally, select the group to which the user is mapped. This value defaults to Default Group—that is, numeric group 0.

Set Unknown User Policy

After you configure the ODBC External Database, enable the Unknown User Policy in the same way as for any other external user databases. By default, the Cisco Secure ACS rejects any user that is not defined locally to its internal database. After Unknown User Policy is enabled, it defines which external databases are contacted and in which order. In the example below, only ODBC authentication has been selected from the list of available databases. Databases are not listed on this page until a configuration has been created.

Add CSNTaccInfo to Reporting Logs

The procedure result field/parameter *CSNTacctInfo* can be used to include a string in some of the various reports generated by the Cisco Secure ACS, such as RADIUS and TACACS+ accounting CSV reports. The field can contain up to fifteen characters, and is intended to enable the RDBMS to include a short client-defined sequence of characters into reports such as a billing code or a user's department.

If the SQL procedures return a value that is to be included in a Cisco Secure ACS report, the report configuration must be changed from the default to include this field. To add the *CSNTacctInfo* to RADIUS accounting, from the Cisco Secure ACS home page navigation, choose the **System Configuration** button, then click **Logging**. Next, choose either **CSV RADIUS Accounting** or **ODBC RADIUS Accounting**, depending on which is desired. Under Select Columns To Log, scroll through the left window until the attribute *ExtDB Info* is visible. This is the attribute to which *CSNTacctInfo* is mapped. Choose the attribute, and then click the right-arrow to add this attribute to the report. Then, press the **Submit** button to save the new configuration.

Testing and Troubleshooting the Configuration

There are three main aspects to achieving a working system:

1. Cisco Secure ACS/ODBC configuration

2. RDBMS SQL procedure interface

3. Customer-specific authentication SQL code

By using the stub procedures the testing aspects 1 and 2 are simplified because the stub procedures allow these to be tested in isolation of aspect 3. These basic "just say 'yes'" procedures enable testing of the Cisco Secure ACS configuration, the ODBC DSN, and the SQL procedure within the RDBMS without requiring that the procedures have been finished. You must write the final version of the procedures such that the appropriate databases, tables, columns, and rows are accessed to return the required data to the Cisco Secure ACS.

After successful authentications have been achieved using a basic procedure, the stub can be replaced by the real authentication SQL code and aspect 3 can be tested.

Failed Attempts Report

Most authentication failures result from the user incorrectly entering the credentials when connecting to the NAS. Such failed attempts are logged to the Cisco Secure ACS *Failed Attempts* report. Entries in this report have a *Message-Type* of *Authen Failed* and a failure code set to one of the values below.

Failure Codes for Failed Attempts Report

Code	Description
Auth type not supported by External DB	Example: PAP request made when only CHAP has been configured.
External DB user unknown	SQL procedure returned user unknown.
External DB user invalid or bad password	SQL procedure returned user unknown or bad password.
External DB CHAP password invalid	CHAP authentication failed.
External DB MSCHAP password invalid	MSCHAP authentication failed.
External DB ARAP password invalid	ARAP authentication failed.
External DB not operational	ODBC connection is down. Refer to the CSAuth service log file for more detail.
External DB reports error condition	An unknown error has occurred. Refer to the CSAuth service log file for more detail.

Debugging the Cisco Secure ACS Service Log Files

During the initial testing period, it is useful to enable maximum logging within the Cisco Secure ACS. To do this, from the Cisco Secure ACS home page navigation, choose the **System Configuration** button**,** and then click **Service Control**. Under Services Log File Configuration*,* set the **Level of Detail** option to Full*,* and then click **Restart**. This results in each Cisco Secure ACS service writing full diagnostic traces to its respective log file.

The service log file of most interest when you are debugging ODBC authentication is the CSAuth log. This is the central authentication service within the Cisco Secure ACS and is responsible for interaction with the external ODBC database also. If the Cisco Secure ACS was installed to its default location, the CSAuth logs are located in the following path:

> \Program Files\CiscoSecure ACS v4.x\CSAuth\Logs

The active file is named `auth.log`. Previous logs are named according to their creation dates (e.g. `auth 2000-12-12.log`). Entries in the log are time stamped and relate to several Cisco Secure ACS features. To locate entries that are relevant to ODBC authentication, open the file with a text editor such as Notepad and search for instances of the string "External DB [ODBCAuthDll.dll]".

Successful PAP authentication Example

```
Attempting authentication for Unknown User 'testuser'

External DB [ODBCAuthDll.dll]: Authen PAP start for user
[testuser]

External DB [ODBCAuthDll.dll]: Authentication OK for user
[testuser]
```

If the group assignment field is out of range, the user will still authenticate; however, the default group will be used for authorization—which may lead to unexpected results. In which case the log would show the following:

```
External DB [ODBCAuthDll.dll]: Invalid group [654] for user
[testuser], assigning default
```

Failed PAP Authentication Example

```
Attempting authentication for Unknown User 'testuser'

External DB [ODBCAuthDll.dll]: Authen PAP start for user
[testuser]

External DB [ODBCAuthDll.dll]: Authen failed for user
[testuser] (-1065)
```

UnConfigured Protocol Authentication Attempt

If a particular protocol has not been configured (for example, PAP), any attempt to authenticate will result in the following failure:

```
Attempting authentication for Unknown User 'testuser'

External DB [ODBCAuthDll.dll]: Authen PAP start for user
[testuser]

External DB [ODBCAuthDll.dll]: PAP authentication not
configured
```

ODBC/DSN Problem

If there are problems with either the DSN or the ODBC connection, look for messages such as the following:

```
External DB [ODBCAuthDll.dll]: CAuthenDb::Open—Data source
name not found and no default driver specified

External DB [ODBCAuthDll.dll]: Failed to open DSN 'CiscoSecure
ODBCAuth'

External DB [ODBCAuthDll.dll]: Error during authentication,
closing DSN connection
```

RDBMS Reported Error

If an SQL procedure indicates an RDBMS/internal procedure error (with a return code of 4+ and an error string), the following would be logged:

```
Attempting authentication for Unknown User 'testuser'

External DB [ODBCAuthDll.dll]: Authen PAP start for user
[testuser]

External DB [ODBCAuthDll.dll]: Authen error for user
[testuser] <returned string>
```

Example SQL Procedures

CSNTAuthUserPAP

The examples given are stubs that return a hard-coded data-set for a successful authentication.

SQL Server

```
CREATE PROCEDURE CSNTAuthUser

@username varchar(64), @password varchar(255)
AS
      SELECT 0,1,"account info","No Error"
GO
```

Oracle

```
create or replace procedure CSNTAuthUserPap
 username             IN  varchar2,
 password             IN  varchar2,
 CSNTresult           OUT int,
 CSNTgroup            OUT varchar2,
 CSNTaccInfo              OUT varchar2,
 CSNTErrorString      OUT varchar2
)
as
begin
  CSNTresult          := 0;
  CSNTgroup           := 1;
```

```
                    CSNTaccInfo            :='account info';

                    CSNTErrorString        :='No Error';

                end;
```

MS-Access

```
create a procedure CSNTAuthUserPap

SELECT tabUsers.CSNTresult, tabUsers.CSNTgroup,
tabUsers.CSNTacctInfo, tabUsers.CSNTerrorString

FROM tabUser

WHERE (((tabUsers.CSNTusername)=[@CSNTusername]) AND
((tabUsers.CSNTpassword)=[@CSNTpassword]))
```

CSNTExtractClearTextPw

The examples given in this section are stubs that return a hard-coded data-set for a successful authentication.

SQL Server

```
CREATE PROCEDURE CSNTExtractUserClearTextPw

@username varchar(64)

AS

        SELECT 0,1,"account info","No Error","MyChapPassword"

GO
```

Oracle

```
create or replace procedure CSNTExtractUserClearTextPw

(

 username               IN  varchar2,

 CSNTresult             OUT int,

 CSNTgroup              OUT varchar2,

 CSNTaccInfo                 OUT varchar2,

 CSNTErrorString        OUT varchar2,

 CSNTPassword                OUT varchar2

)

as

begin

  CSNTresult            := 0;

  CSNTgroup             := 1;

  CSNTaccInfo           :='account info';

  CSNTErrorString       :='No Error';

  CSNTPassword          :='MyChapPassword';

end;
```

Summary

This topic summarizes the key points discussed in this lesson.

- Configuration of LDAP databases is performed in External Database configuration.

- ACS can also be used in conjunction with SQL databases. This lesson covered the configuration required to do so.

Module Summary

ACS databases are an important component of the server. This lesson taught you to manage these database options. Cisco Secure ACS for Windows 2000 and NT servers also enables users to authenticate against external databases in preference to their internal databases. This allows a Cisco Secure ACS installation to "back end" onto a variety of authentication sources, including Windows NT/2000, Novell Directory Services (NDS), Lightweight Directory Access Protocol (LDAP), various token-card servers, and ODBC databases.

ACS Authentication and NAD Interactions

Overview

One of the major functions of ACS is its ability to support multiple authentication types. In addition, ACS has extensive flexibility by using the Shared Profile Components feature. In this lesson, you will learn how to work with these configurations as well as how to view different reports and activity.

Module Objectives

Upon completion of this module, you will be able to work with multiple authentication types, configure the different options in the Shared Profile Components configuration menu, as well as view reports and activity. This ability includes being able to meet these objectives:

- Configure 802.1x

- Configure EAP-TLS

- Configure PEAP

- Configure LEAP

- Configure EAP-FAST

- Configure EAP-MD5

- Configure CHAP, PAP, and MSCHAP

- Understand how downloadable ACLs work

- Configure downloadable ACLs

- Understand and configure device command authorization

- Understand and configure network access restrictions

- Restrict access point device login to the access point only

- View Reports and Activity

Lesson 1

Authentication Types

Overview

Authentication is an important part of ACS. In this lesson, you will learn how to enable a number of authentication types in ACS.

Objectives
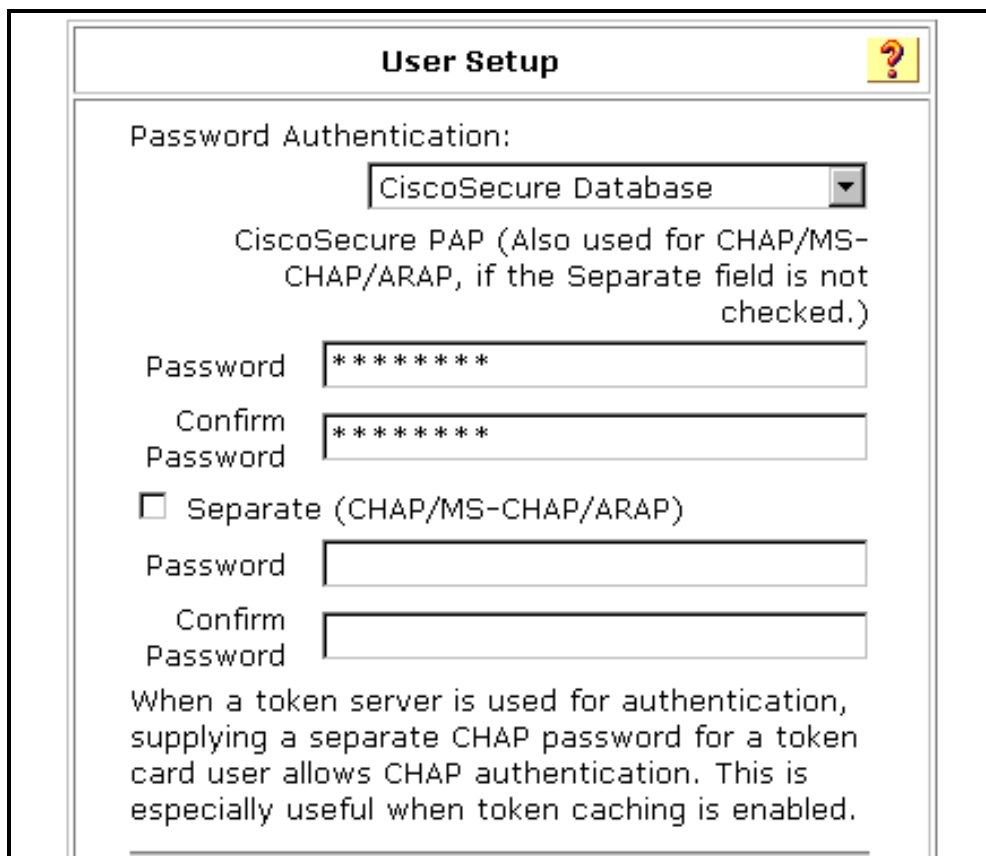
Upon completing this lesson, you will be able to configure multiple authentication types. This ability includes being able to meet these objectives:

- Configure 802.1x
- Configure EAP-TLS
- Configure PEAP
- Configure LEAP
- Configure EAP-FAST
- Configure EAP-MD5
- Configure CHAP, PAP, and MSCHAP

Configuring 802.1x

When a device performing 802.1x authentication sees an end-user on a port, it forces the port into an unauthorized state so only 802.1x traffic is forwarded. Traffic such as Dynamic Host Configuration Protocol (DHCP), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Simple Message Transfer Protocol (SMTP), and Post Office Protocol 3 (POP3) is blocked. The client can send an EAP-Start message, although client initiation is not required. The 802.1x device replies with an EAP-Request Identity message back to the client to obtain the identity of the client. The EAP-Response packet from the client contains the identity of the client and is forwarded to the authentication server.

The authentication server—in this case, ACS—is configured to authenticate clients with a specific authentication algorithm, and credential verification takes place. The result is an ACCEPT or REJECT packet from the authentication server to the device that requests authentication of a client. Upon receipt of the ACCEPT packet, the port to which the client connects transitions to an authorized state and traffic is forwarded.

Configuring ACS for 802.1x authentication

To configure ACS for 802.1x authentication, follow these steps:

Step 1 To add and configure users, click **User Setup** from the ACS main navigation bar and define the user name and password.

Step 2 On the User Setup page, define the Internet Engineering Task Force (IETF) attributes 64 and 65.

Make sure that the Tag is set to one because the Catalyst ignores any tag other than 1. To assign a user to a specific VLAN, you must also define attribute 81 with a VLAN name. Do not use a VLAN number. The value for 064 should be set to VLAN and the value for 065 should be set to 802.

User Setup

IETF RADIUS Attributes

☑ [064] Tunnel-Type
    Tag 1 ▾ Value VLAN ▾
    Tag 2 ▾ Value ▾

☑ [065] Tunnel-Medium-Type
    Tag 1 ▾ Value 802 ▾
    Tag 2 ▾ Value ▾

☐ [066] Tunnel-Client-Endpoint
    Tag 1 ▾ Value
    Tag 2 ▾ Value

☐ [067] Tunnel-Server-Endpoint
    Tag 1 ▾ Value
    Tag 2 ▾ Value

☐ [069] Tunnel-Password
    Tag 1 ▾ Value
    Tag 2 ▾ Value

☑ [081] Tunnel-Private-Group-ID
    Tag 1 ▾ Value big-access1
    Tag 2 ▾ Value

[Submit] [Delete] [Cancel]

Note   For more information on these IETF attributes, refer to RFC 2868: RADIUS Attributes for Tunnel Protocol Support.

Note   In the initial configuration of the ACS server, IETF RADIUS attributes can fail to display. To enable IETF attributes in user configuration screens, choose **Interface configuration > RADIUS (IETF)**, then check attributes **64**, **65**, and **81** in the User and Group columns.

If you do not define IETF attribute 81 and the port is a switch port in access mode, the port will belong to the access VLAN defined on the port. If you have defined attribute 81 for dynamic VLAN assignment and the port is a switch port in access mode, you must issue the command **aaa authorization network default group radius** in global configuration mode on the switch. This command assigns the port to the VLAN that the RADIUS server provides. Otherwise, 802.1x moves the port to the `AUTHORIZED` state after authentication of the user; but the port remains in the default VLAN of the port and connectivity can fail. If you have defined attribute 81 but you have configured the port as a routed port, denial of access occurs and this error message displays:

%DOT1X-SP-5-ERR_VLAN_NOT_ASSIGNABLE:

RADIUS attempted to assign a VLAN to Dot1x port GigabitEthernet2/15 whose VLAN cannot be assigned.

Configuring the PC Client to Use 802.1x Authentication

This example is specific to the Windows XP Extensible Authentication Protocol (EAP) over LAN (EAPOL) client:

Step 1   Choose **Start > Control Panel > Network Connections**, then right-click your Local Area Connection and choose Properties.

Step 2   On the General tab, check **Show icon in notification area [taskbar] when connected**.

Step 3   On the Authentication tab, check **Enable IEEE 802.1x authentication for this network**.

Step 4 Set the EAP type to MD5-Challenge, as shown in this example:
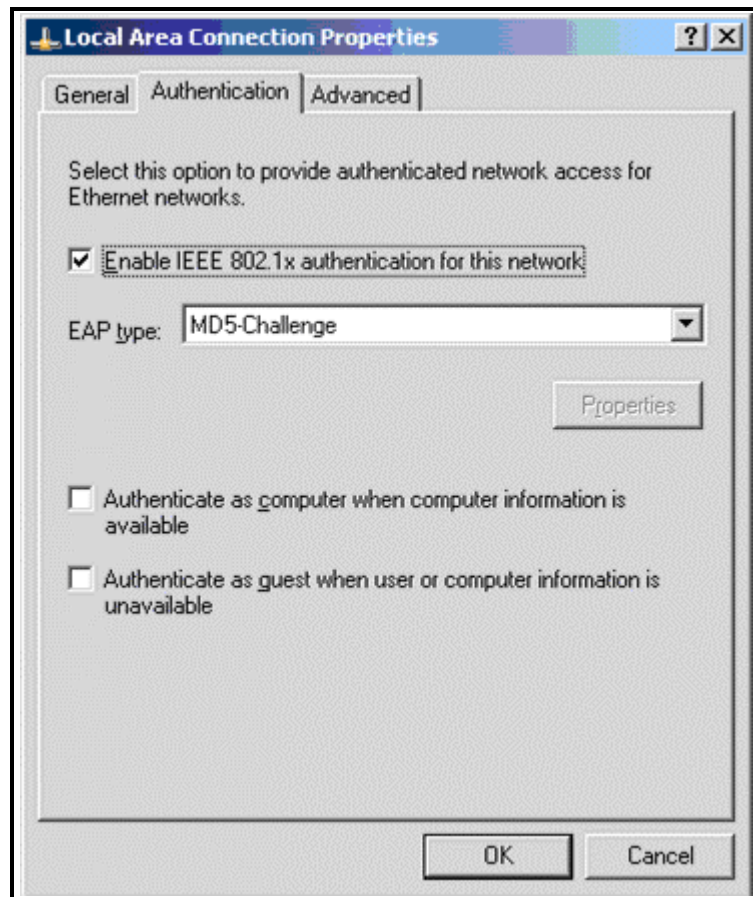
Verify the 802.1x Operation

To verify 802.1x operation, follow these steps:

Step 1 If you have correctly completed the configuration, the client presents the following dialog bubble, prompting you to enter a user name and password. Click the bubble.
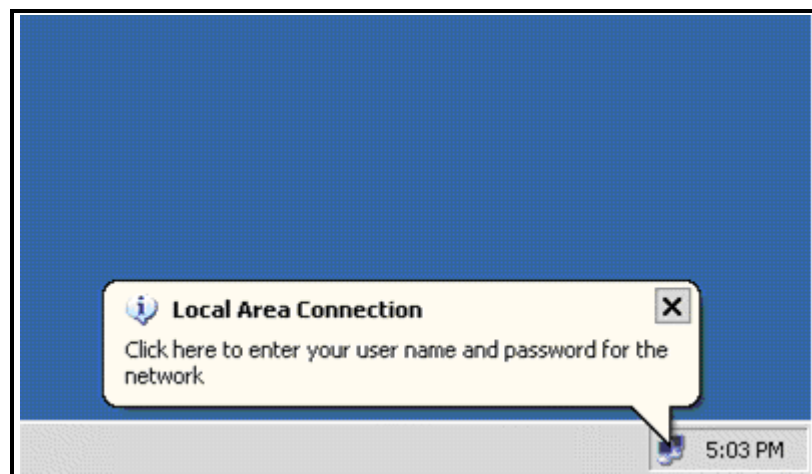
Step 2 In the authentication window that appears, enter the user name and password.
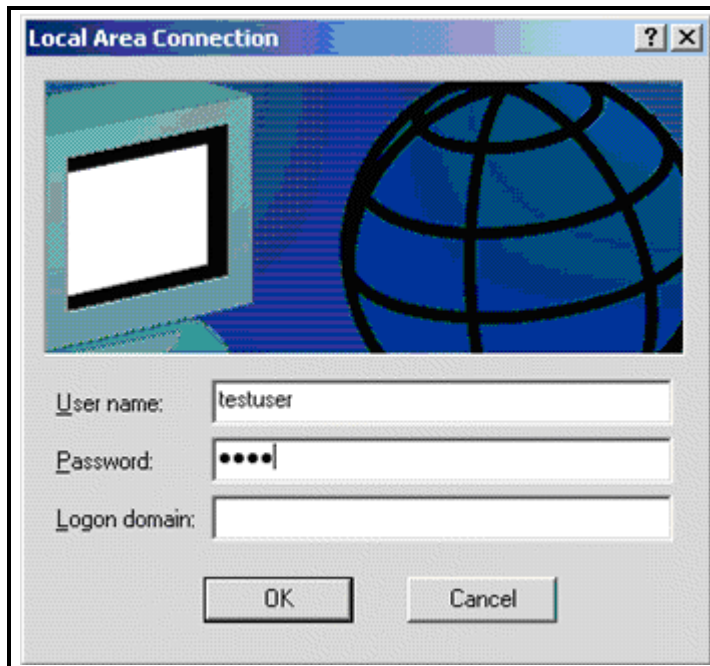
Step 3   If no error messages appear, verify connectivity with the usual methods, such as by accessing network resources and using the **ping** utility.

If the following error message appears, verify that the correct user name and password have been supplied.
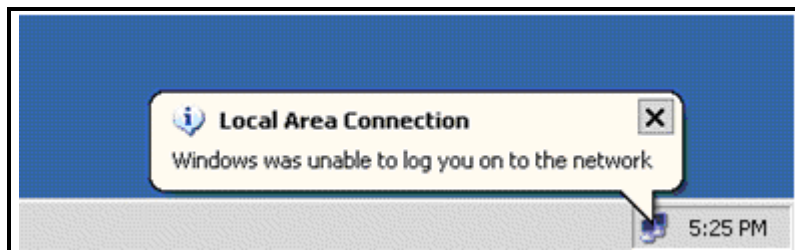
Step 4   If the user name and password appear to be correct, check the 802.1x port state on the device authenticating the host.

Configuring EAP-TLS

Both EAP-TLS and Protected Extensible Authentication Protocol (PEAP) build and use a TLS/Secure Socket Layer (SSL) tunnel. EAP-TLS uses mutual authentication in which both the ACS (authentication, authorization, and accounting [AAA]) server and clients have certificates and prove their identities to each other. PEAP, however, uses only server-side authentication; only the server has a certificate and proves its identity to the client.

Configuration Requirements

- ACS
- CA Server

Major Configuration Steps

- Obtain a Certificate for the ACS Server (not detailed in this lesson)
- Configure ACS to Use a Certificate From Storage
- Restart the Service and Configure EAP-TLS Settings on the ACS
- Configure the AAA Client for Desired Settings
- Configure the External User Database

Configuring MS Certificate Machine Auto Enrollment

Follow these steps to configure ACS to use the certificate in storage.

Step 1 Open a web browser and enter http://ACS-ip-address:2002/ in the address bar to access the ACS. From the ACS main navigation bar, click **System Configuration**, and then click **ACS Certificate Setup**.

Step 2 From the ACS Certificate Setup page, click **Install ACS Certificate**.

Step 3 Choose the **Use certificate from storage** radio button. In the Certificate CN text box, enter the name of the certificate that you assigned when you enrolled with the CA server. Click the **Submit** button.

Step 4 When the configuration is complete, you will see a confirmation message indicating that the configuration of the ACS server has been changed.

Note You do not need to restart the ACS at this time.

System Configuration

Edit

Install ACS Certificate

Installed Certificate Information	?
Issued to:	ACS-1
Issued by:	ACS-1
Valid from:	November 04 2005 at 14:52:06
Valid to:	November 04 2006 at 14:52:06
Validity:	OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

[Install New Certificate] [Cancel]

[? Back to Help]

Specifying Additional Certificate Authorities That the ACS Should Trust

The ACS will automatically trust the CA that issued its own certificate. If the client certificates are issued by additional CAs, then you need to complete the following steps.

Step 1 Click **System Configuration** on the ACS main navigation bar, and then click **ACS Certificate Setup**.

Step 2 Click **ACS Certificate Authority Setup** to add CAs to the list of trusted certificates. In the field for CA certificate file, enter the location of the certificate, and then click **Submit**.

System Configuration

Edit

ACS Certification Authority Setup

CA Operations	?

Add new CA certificate to local certificate storage

CA certificate file [   ]

? Back to Help

[Submit] [Cancel]

Step 3   Click **Edit Certificate Trust List**. Check all of the CAs that the ACS should trust, and remove the check from all of the CAs that the ACS should not trust. Click **Submit**.

Restarting the ACS Service and Configure EAP-TLS Settings on the ACS

Follow the steps below to restart the service and configure EAP-TLS settings.

Step 1   Click **System Configuration** on the ACS main navigation bar, and then click **Service Control**.

Step 2   Click **Restart** to restart the ACS service.

Step 3   To configure EAP-TLS settings, click **System Configuration**, and then click **Global Authentication Setup**.

Step 4   Check **Allow EAP-TLS**, and then check one or more of the certificate comparisons. When you are finished, click **Submit**.

System Configuration

Edit

Global Authentication Setup

EAP Configuration	?

PEAP
- ☐ Allow EAP-MSCHAPv2
- ☐ Allow EAP-GTC
- ☐ Allow Posture Validation

Cisco client initial message: [   ]

PEAP session timeout (minutes): [120]

Enable Fast Reconnect: ☑

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS
- ☑ Allow EAP-TLS

Select one or more of the following options:
- ☑ Certificate SAN comparison
- ☑ Certificate CN comparison
- ☑ Certificate Binary comparison

EAP-TLS session timeout (minutes): [120]

LEAP
- ☑ Allow LEAP (For Aironet only)

EAP-MD5
- ☑ Allow EAP-MD5

AP EAP request timeout (seconds): [20]

MS-CHAP Configuration	?

- ☑ Allow MS-CHAP Version 1 Authentication
- ☑ Allow MS-CHAP Version 2 Authentication

? Back to Help

[Submit] [Submit + Restart] [Cancel]

Specifying and Configuring the Access Point as a AAA Client

Follow these steps to configure the access point (AP) as an AAA client.

Step 1 Click **Network Configuration** from the ACS main navigation bar. In the AAA Clients section, click **Add Entry**.

Step 2 Type the hostname of the access point in the AAA Client Hostname text box and type the IP address of the access point in the AAA Client IP Address text box. Type a shared secret key for the ACS and the access point in the Key text box. Choose **RADIUS (Cisco Aironet)** from the Authenticate Using drop-list. When you are finished, click **Submit**.

Configuring the External User Databases

Follow these steps to configure the external user databases.

Step 1   Click **External User Databases** from the ACS main navigation bar, and then click **Database Configuration**. Click **Windows Database**.

Note   If there is no Windows database already defined, click **Create New Configuration** and then click **Submit**.

Step 2   Click **Configure**. Under Configure Domain List, move the SEC-SYD domain from Available Domains to Domain List.
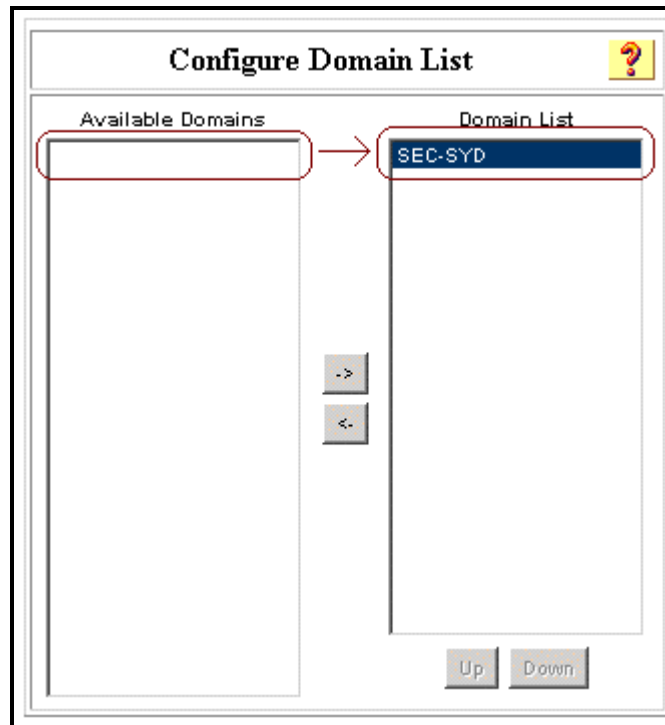
Step 3 To enable machine authentication, check the option **Permit EAP-TLS machine authentication** under Windows EAP Settings. *Do not* change the machine authentication name prefix. Microsoft currently uses "/host" (the default value) to distinguish between user and machine authentication. If you wish, you can enable domain stripping by checking the EAP-TLS Strip Domain Name box. When you are finished, click **Submit**.
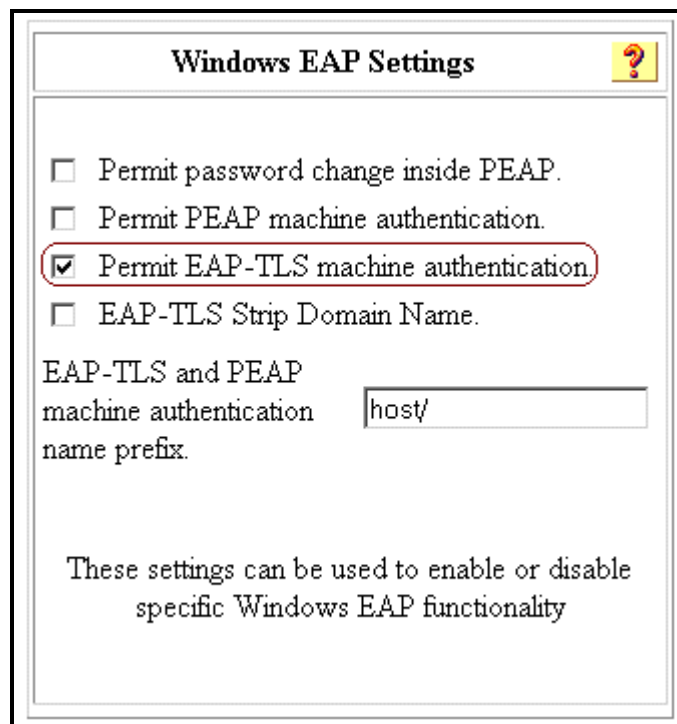
Step 4 From the ACS main navigation bar, click **External User Databases**, and then click **Unknown User Policy**. Choose the **Check the following external user databases** radio button, then click the right-arrow button (->) to move Windows Database

from the External Databases list to the Selected Databases list. When you are finished, click **Submit**.

Restarting the Service

When you have finished configuring the ACS, follow these steps to restart the ACS services.

Step 1 Click **System Configuration**, and then click **Service Control**.

Step 2 Click **Restart**.

Configuring PEAP

Both PEAP and EAP-TLS build and use a TLS/Secure Socket Layer (SSL) tunnel. However, PEAP uses server-side authentication only; only the server has a certificate and proves its identity to the client. EAP-TLS, on the other hand, uses mutual authentication in which both the ACS (authentication, authorization, and accounting [AAA]) server and clients have certificates and prove their identities to each other.

PEAP is convenient because clients do not require certificates. EAP-TLS is useful for authenticating headless devices, because certificates require no user interaction.

Configuring PEAP in ACS

The configuration of PEAP in ACS is similar to the configuration of EAP. Follow these steps to restart the service and configure PEAP settings.

Step 1　From the ACS main navigation bar, click **System Configuration** and then click **Service Control**.

Step 2　Click **Restart** to restart the service.

Step 3　To configure PEAP settings, from the ACS main navigation bar, click **System Configuration**, and then click **Global Authentication Setup**.

Step 4　Check the two PEAP settings listed below, and leave all other settings at their default. You can also specify additional settings, such as Enable Fast Reconnect. When you are finished, click **Submit**.

— Allow EAP-MSCHAPv2

— Allow MS-CHAP Version 2 Authentication

System Configuration

Edit

Global Authentication Setup

EAP Configuration	❓

PEAP
- ☑ Allow EAP-MSCHAPv2
- ☑ Allow EAP-GTC

Cisco client initial message: [   ]

PEAP session timeout (minutes): [120]

Enable Fast Reconnect: ☑

EAP-TLS
- ☐ Allow EAP-TLS

Select one or more of the following options:

Configuring LEAP

This section covers basic configurations of Cisco LEAP on the ACS server, for use with an AP and various clients, including non-root bridges, workgroup bridges, and AP repeaters.

Adding the AP to the ACS server

Step 1   From the ACS main navigation bar, click **Network Configuration**.

Step 2   Click **Add Entry**.

Step 3   Configure the DNS name of the AP, the IP address of the AP, the RADIUS shared secret, and the Authentication method, as shown in the example.

Step 4   Choose **RADIUS (Cisco Aironet)** in the Authenticate Using drop-list.

Step 5   To complete, click **Submit+Restart**.

Configuring the WEP Key Session Timeout

802.1x specifies a re-authentication option. The Cisco LEAP algorithm utilizes this option to expire the current WEP session key for the user and issue a new WEP session key. It is important to note that, although re-authentication is an option, it is disabled by default. The following is the configuration to enable the 802.1X WEP Key timeout.

Note	To determine the timeout value to use, please refer to the WEP timeout document at www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch8.htm#wp1047518

Step 1 From the ACS main navigation bar, click **Group Setup** as shown in the example.

Step 2 Choose the group for which you want to modify the WEP Key/Session timeout. In most cases, the Default group is the one you will want to modify.

Step 3 Click **Edit Settings**.

Step 4 Scroll down to the **IETF RADIUS ATTRIBUTES** section.

Step 5 For WEP key timeout, check the **[027]Session -Timeout** box and configure the timeout value in seconds, as in the second figure below.

Step 6 Click **Submit+Restart** to finish.
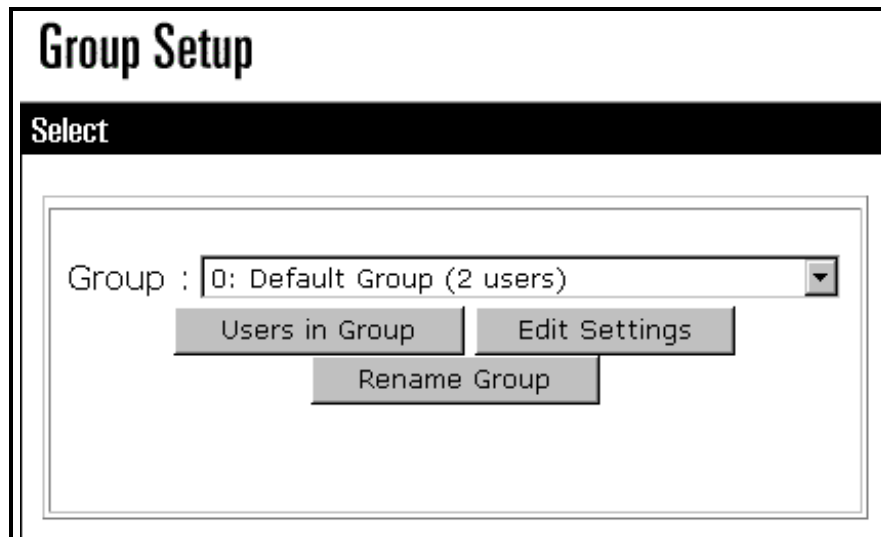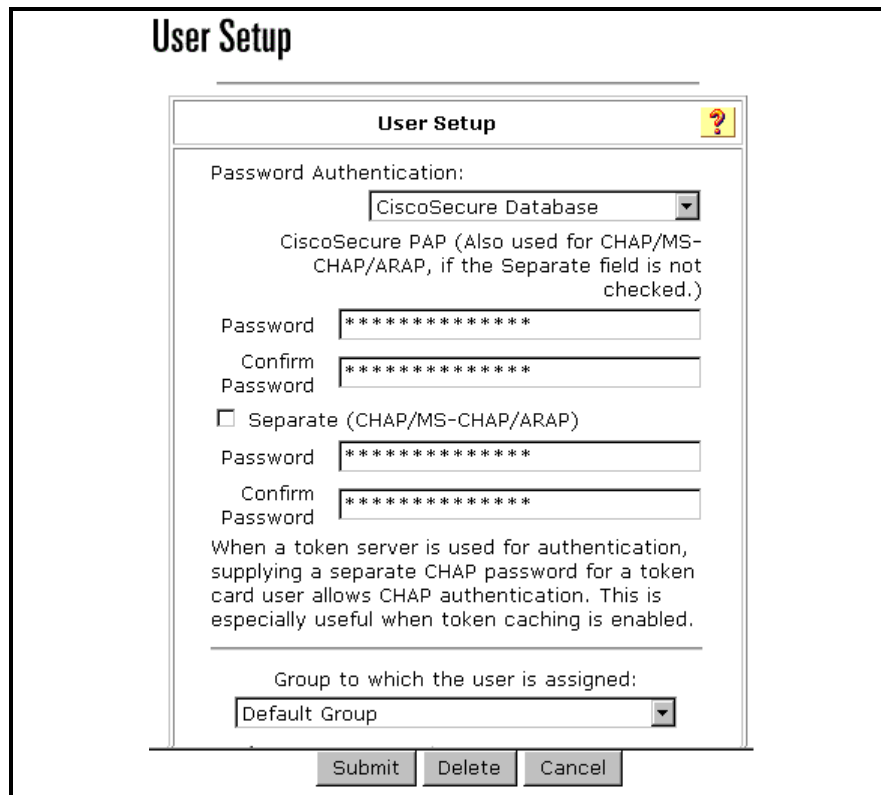
Enabling EAP-Cisco (Cisco LEAP) on the Root Bridge or AP

Step 1   Browse to the AP or Wireless Bridge.

Step 2   From the Summary Status page, click **Setup**.

Step 3   From the Service menu, choose **Security**.

Step 4   Click **Authentication Server**.

Step 5   From the 802.1X Protocol Version drop-list, select the version of 802.1x you want to run on the AP. Please note that Draft 7 is no longer supported.

Step 6   Enter the IP address of the ACS in the Server Name/IP text box.

Step 7   Verify that the Server Type drop-list is set to **RADIUS**.

Step 8   Enter **1645** in the Port text box. This is the correct IP port number to use with the ACS.

Step 9   In the Shared Secret text box, enter the value that is used on the ACS.

Step 10   Check the EAP Authentication check box.

Step 11   Modify the Timeout text box if needed. This is the timeout value for an ACS to respond to an authentication request. If the ACS does not respond to the authentication request within this timeframe, the AP will round robin the request to the next ACS that is configured. The AP supports up to four RADIUS servers or ACSs.

Step 12   Click **OK** when finished.

Adding a MAC address to the ACS

The ACS can authenticate MAC addresses sent from an AP. A properly configured AP will attempt to authenticate a MAC address using Secure-PAP authentication with the ACS. The MAC addresses are entered into the ACS as users, with the username and password being the MAC address.

Step 1   From the ACS main navigation bar, click **User Setup**.

Step 2   In the User text box, type the MAC address of the user's PC. Do not use dashes, periods, or any other delimiters.

Step 3   In the **CiscoSecure-PAP** text box, type the MAC address.

Step 4   Check the **Separate (CHAP/MS-CHAP)** box.

Step 5   Enter a strong password in the **CHAP/MS-CHAP** text box. This should not match the MAC address.

Step 6   Click **Submit**.

Configuring MAC Authentication on the Root Bridge or AP

There are two modes available for MAC authentication:

- **MAC authentication only:** This mode allows for MAC address authentication as a means of augmenting Open, Shared Key, or Network-EAP authentication.

- **MAC authentication to coexist with EAP authentication:** This mode allows for MAC address authentication or EAP (non-Network-EAP) to authenticate the device or user. The AP will first attempt MAC authentication and, if that fails, attempt EAP authentication for Open and Shared Key clients.

Configuring EAP-FAST

This topic describes EAP-FAST in ACS.

How EAP-FAST Works

EAP-FAST comprises three basic phases:

- **Phase 0 (optional):** the Protected Access Credential (PAC) is initially distributed to the client.

- **Phase 1:** a secure tunnel is established using the PAC.

- **Phase 2:** the client is authenticated via the secure tunnel.

The initial "Phase 0" or auto-provisioning (also called in-band provisioning) component of EAP-FAST permits the secure distribution of the user PAC to each client. With some other authentication protocols, it is necessary to establish a network connection or manually install a file in order to distribute credentials to the user. Phase 0 in EAP-FAST permits a user PAC to be distributed to the client during an encrypted session after the credentials of the user are authenticated. This user authentication uses a challenge-handshake protocol to authenticate the client and to validate the server response. This authentication mechanism guards against potential interception and re-forwarding of provisioning requests for the purpose of intercepting a user PAC.

Phase 0 is optional in EAP-FAST. PAC files may also be manually generated at the PAC server and distributed manually to client devices (this is referred to as *manual* or *out-of-band provisioning*). Because auto provisioning uses MSCHAPv2 protocol, it may be necessary to use manual provisioning if you use a non-Microsoft format database such as LDAP, which does not support MSCHAPv2 credentials.

Note that the end result of Phase 0 is PAC distribution, not client authentication. After successful PAC distribution, the server issues an authentication failure to the access point and the user is disassociated from the network. Then the client re-initiates an EAP-FAST authentication with the network using the newly provisioned PAC and the credentials of the user.

After the optional Phase 0, the actual EAP-FAST authentication starts with Phase 1. In the Phase 1 EAP-FAST authentication transaction, a secure tunnel is established between the user and the EAP-FAST-capable RADIUS server using the PAC credential of the user with the TLS protocol.

During the initial authentication request, the server sends its Authority ID (A-ID). The client selects the correct PAC from its storage by correlating the provided A-ID with the saved PACs and the respective PAC-Info fields.

Note   The client sends only the PAC opaque to the server, not the PAC key. The server decrypts the PAC opaque using its master key. As the server and client now share the PAC key, the PAC key is used to create the unique transport layer security (TLS) tunnel for this client's authentication.

After the TLS tunnel is established using the PAC, the user authentication credentials are passed securely using the EAP-GTC (Generic Token Card) protocol within the encrypted tunnel to the RADIUS server (Phase 2).

Note	The client response is cryptographically bound to the EAP authentication success message. This prevents a Man-In-The-Middle (MITM) attack in which the attacker (client) attempts to provide a false response to the server in order to obtain the session key.

After successful Phase 2 authentication of the client to the EAP-FAST server, a RADIUS access-accept message is passed to the access point (along with the master session key). An EAP success message is generated at the access point (as with other EAP authentication protocols). Upon receipt of the EAP-success packet, the client derives the session key using a complimentary algorithm used at the server to generate the session key passed to the access point. This key permits the client and access point to establish a unique session key using the defined encryption mechanism (WPA authenticated key management, CCKM, or standard 802.11 WEP keying).

Configuring the Access Control Server

This section describes how to configure ACS for EAP-FAST with in-band PAC provisioning using Windows Active Directory as the external database.

Adding an Access Point as an AAA Client in ACS

Follow these steps to add an access point as an AAA client in ACS:

Step 1 From the ACS main navigation bar, click **Network Configuration**.

Step 2 Click **Add Entry**. The AAA Client Setup for AP page appears.

Step 3 Enter the access point name, IP address, and key (shared secret you entered on the access point).

Step 4   From the Authenticate Using drop-list, choose **RADIUS (Cisco Aironet)**, which also includes RADIUS IETF attributes.

Note   If Network Device Groups (NDGs) are enabled, first select the appropriate NDG and add the access point to it. For details about NDGs, see the "Network Device Group Configuration" section of the User Guide for CiscoSecure ACS for Windows Server at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/user/n. htm#wp342699

Step 5   Click the **Submit and Restart** button.

Configuring ACS to Query External Databases

Follow these steps to configure the ACS server to query an external database:

Step 1   From the ACS main navigation bar, choose **External User Databases > Database Configuration > Windows Database > Configure**. The User Databases page appears.
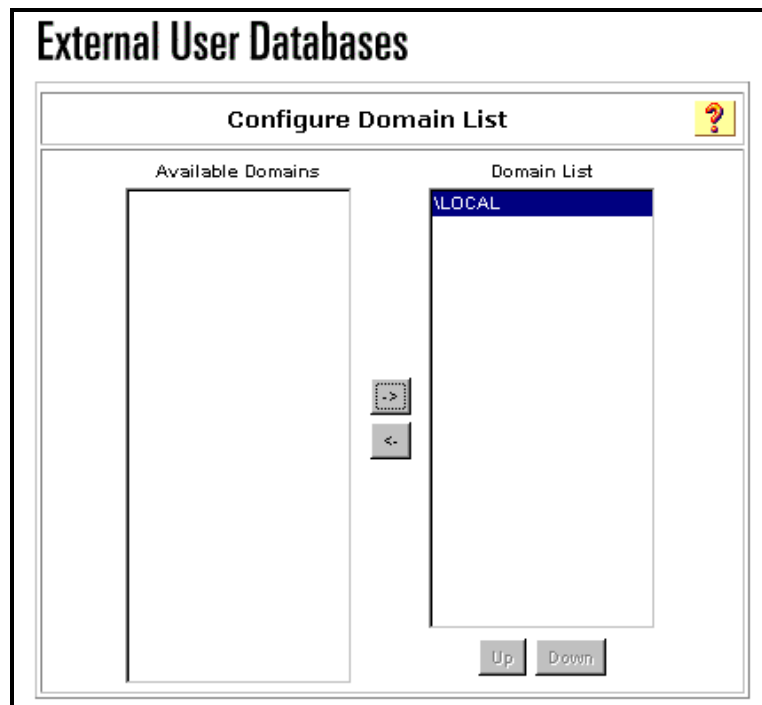
Step 2   Under Configure Domain List, move items from Available Domains to Domain List.

Step 3   Under Windows EAP settings, verify that the Permit password change inside PEAP or EAP-FAST box is checked.

Step 4   Click **Submit**.

Note   You can also enable the dial-in permission feature for EAP-FAST under the Windows User Database Configuration. However, the MS-CHAP settings for password changes on this ACS configuration page are applicable only to non-EAP MS-CHAP authentication. To enable password change in conjunction with EAP-FAST, you must use the configuration under Windows EAP Settings.

External User Databases

These settings can be used to enable or disable password changes using the MS-CHAP version 1 or version 2 protocols.

Windows EAP Settings

☑ Permit password change inside PEAP or EAP-FAST.
☐ Permit PEAP machine authentication.
☐ Permit EAP-TLS machine authentication.
☐ EAP-TLS Strip Domain Name.

EAP-TLS and PEAP machine authentication name prefix: host/

These settings can be used to enable or disable specific Windows EAP functionality

Step 5   Choose **Unknown User Policy** from the External User Databases page.

Step 6   Choose **Check the following external user databases**.

Step 7   Move **Windows Database** from the External Databases list to the Selected Databases list.

Step 8   Click **Submit**.

Note   From this point, ACS looks for the user in the Windows database. If not found in the ACS local database, the user is placed in the ACS default group. Consult the ACS documentation for more details about database group mappings.

Note   Because the ACS software queries the Active Directory to verify user credentials, you may need to configure additional access rights in Windows. For details see the *Installation Guide for CiscoSecure ACS for Windows Server* at www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs40/install/postinst.htm#wp1041202
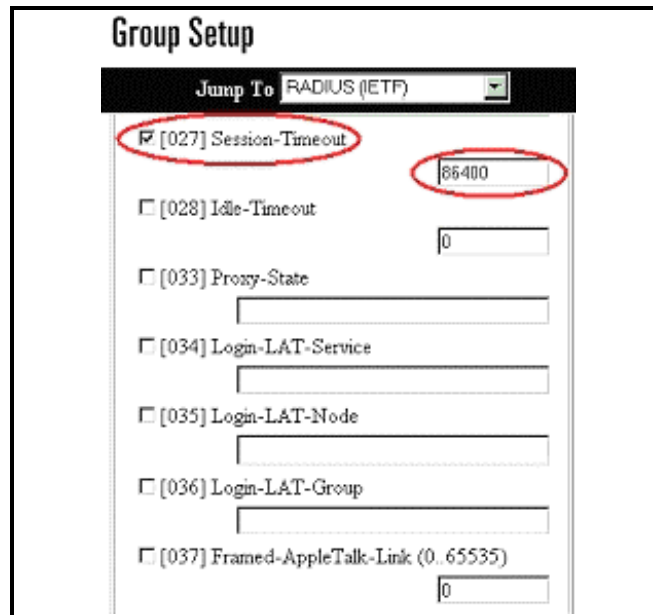
Configuring Group Settings on ACS

Follow these steps to configure group settings on the ACS server:

Step 1   From the ACS main navigation bar, choose **Group Setup > Default Group** and click **Edit Settings**. The Configure Unknown User Policy page appears.

Step 2   Choose the **Check the following external user databases** radio button.

Step 3   From the ACS main navigation bar, click **Group Setup**. The Group Setup page appears.
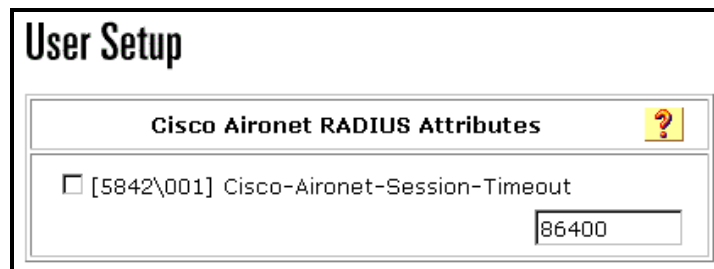
Step 4   Scroll down to RADIUS IETF attributes and check the **[027] Session-Timeout** box. Set the Timeout to **86400** seconds.

Step 5   Click **Submit** + **Restart**.

You may also need to set the session timeout per user using the Aironet RADIUS session timeout, if per user (or per group) attributes are configured on ACS.

Enabling EAP-FAST Support on ACS

Follow these steps to enable EAP-FAST support on the ACS server:

Step 1   From the ACS main navigation menu, choose **System Configuration > Global Authentication Setup**.

System Configuration
Edit

Global Authentication Setup

EAP Configuration

PEAP
☐ Allow EAP-MSCHAPv2
☐ Allow EAP-GTC
Cisco client initial message:
PEAP session timeout (minutes): 120
Enable Fast Reconnect: ☑

EAP-FAST
☑ Allow EAP-FAST
Master key TTL: 1 months
Retired master key TTL: 3 months
PAC TTL: 1 weeks
Client initial message: Welcome !!!
Authority ID Info: Swiss-TAC-ACS
Allow in-band PAC provisioning ☑
Reset to Master ☐

Step 2   Check the **Allow EAP-FAST** box.

Step 3   Set the Master key time-to-live (TTL), Retired master key, and PAC TTL as follows:

—   **Master key TTL:** 1 month

—   **Retired master key TTL:** 3 months

—   **PAC TTL:** 1 week

Step 4   Enter a message to be sent to the users who authenticate with an EAP-FAST client.

Note   The initial display message appears if the end user client supports its display. The current EAP-FAST supplicant implementation in ACU version 6.3 does not support this option.

Step 5   Enter the descriptive text in the Authority ID Info field. This text is also shows on the client where you can select the PAC authority used with a certain profile.

Step 6   Check the **Allow in-band PAC provisioning** box.

Step 7   Choose **EAP-FAST Master Server**.

Step 8   Click **Submit** + **Restart**.

Note   For a basic reference, see EAP-FAST Protocol Overview at
www.cisco.com/en/US/products/hw/wireless/ps430/prod_configuration_guide09186a008046dc81.html.

Configuring EAP-MD5

To accomplish the configuration of EAP-MD5, you must configure global authentication. This section details this configuration.

Global Authentication Setup

Use this procedure to select and configure how Cisco Secure ACS handles extended options for authentication. In particular, you use this procedure to allow either EAP-MD5 or EAP-TLS, and to allow MS-CHAP Version 1, MS-CHAP Version 2, or both.

To configure authentication options, follow these steps:

Step 1   On the ACS main navigation bar, click **System Configuration**.

Step 2   Click **Global Authentication Setup**.

Step 3   In the EAP Configuration table, select one of the following options:

— Allow EAP-MD5-Challenge

— Allow EAP-TLS (requires server certificate)

Step 4   In the MS-CHAP Configuration table, select each version of MS-CHAP that you want to allow for Cisco Secure ACS. Your choices are the following:

— Allow MS-CHAP Version 1 Authentication

— Allow MS-CHAP Version 2 Authentication

Step 5   Click **Submit + Restart**.

Configuring Legacy Authentication Protocols

This section provides you with a brief introduction to configuring ACS to use CHAP, PAP, and MSCHAP for authentication.

Global Authentication Setup

Use this procedure to select and configure how Cisco Secure ACS handles extended options for authentication. In particular, you use this procedure to allow either EAP-MD5 or EAP-TLS, and to allow either MS-CHAP Version 1 or MS-CHAP Version 2, or both.

To configure authentication options, follow these steps:

Step 1   On the ACS main navigation bar, click **System Configuration**.

Step 2   Click **Global Authentication Setup**.

Step 3   In the EAP Configuration table, select one of the following options:

— Allow EAP-MD5-Challenge

— Allow EAP-TLS (requires server certificate)

Step 4   In the MS-CHAP Configuration table, select each version of MS-CHAP that you want to allow for Cisco Secure ACS. Your choices are the following:

— Allow MS-CHAP Version 1 Authentication

— Allow MS-CHAP Version 2 Authentication

Step 5   Click **Submit + Restart**.

Setting a Separate CHAP/MS-CHAP/ARAP Password in User Configuration

Setting a separate CHAP/MS-CHAP/ARAP password adds more security to Cisco Secure ACS authentication. However, you must have a AAA client configured to support the separate password.

To allow the user to authenticate using a CHAP, MS-CHAP, or ARAP password, instead of the PAP password in the CiscoSecure user database, follow these steps:

Step 1   Add a basic user account

Step 2   Check the **Separate CHAP/MS-CHAP/ARAP** box in the User Setup table.

Step 3   Specify the CHAP/MS-CHAP/ARAP password to be used by entering it in each of the second set of Password/Confirm boxes under the Separate (CHAP/MS-CHAP/ARAP) checkbox.

Note   The Password and Confirm Password boxes are only required for authentication by the Cisco Secure ACS database. Additionally, if a user is assigned to a Voice over IP (VoIP) (null password) group, and the optional password is also included in the user profile, the password is not used until the user is re-mapped to a non-VoIP group.

Step 4 Do one of the following:

— If you are finished configuring the user account options, click **Submit** to record the options.

— To continue to specify the user account options, perform other procedures in this chapter, as applicable.

Summary

This topic summarizes the key points discussed in this lesson.

- You learned how to configure 802.1x.

- You learned how to configure EAP-TLS.

- You learned how to configure PEAP.

- You learned how to configure LEAP.

- You learned how to configure EAP-FAST.

- You learned how to configure EAP-MD5.

- You learned how to configure CHAP, PAP, and MSCHAP.

Understanding and Configuring Shared Profile Components

Overview

In Access Control Server (ACS), Shared Profile components can consist of downloadable IP access control lists (ACLs), Network Access Restrictions (NARs), and command authorization sets for both shell commands and PIX shell commands. Because of their complexity, these configurations sometimes prove to be difficult to configure and maintain. This lesson provides a more extended look into the configuration and management of these components.

Objectives

Upon completing this lesson, you will be able to understand and configure Shared Profile Components. This ability includes being able to meet these objectives:

- Understand how downloadable ACLs work
- Configure downloadable ACLs
- Understand and configure device command authorization
- Understand and configure network access restrictions
- Configure restricted access point device login to the access point only

Understanding Downloadable ACLs

This topic describes Downloadable ACLs.

Downloadable ACLs

Cisco.com

Web
FTP
172.26.26.50

1. The HTTP request to 172.26.26.50 is intercepted by the PIX Firewall.
2. Authentication request to AAA server.
3. Authentication response containing ACL name from AAA server.
4. The PIX Firewall checks to see if the user's ACL is already present.
5. Request from the PIX Firewall to the AAA server for the user's ACL.
6. The ACL is sent to the PIX Firewall.
7. The HTTP request is forwarded to 172.26.26.50

192.168.0.0

PIX
Firewall

10.0.0.0

AAA server
172.16.0.4

Student PC
10.0.0.11

The basic principle behind downloadable ACLs is that they are access lists that you configure on the server instead of the PIX. This provides the benefit of a single point of configuration when you need to make changes to the ACL. Additionally, with downloadable ACL's you only need to configure the ACL once, on one device, and you can then apply the same ACL on numerous devices. With authentication configured, when a user establishes a connection and authenticates against the ACS, the PIX downloads the ACL and applies it to the uauth of the user. A uauth is the authentication information of a user as it is stored in the PIX Firewall cache. This access list functions just like a regular access list.

Developing the ACL

Prior to configuring Downloadable ACLs, you should have some idea of how you are going to apply the ACL. Below are some considerations to take into account when creating your access-list.

- In an access list, the source IP address comes before the destination IP address.

- The PIX Firewall does not use wildcard masks; instead, a standard subnet mask is used in the access list.

- The two options that an access list can perform are Permit and Deny.

- Examples of protocols that you can define are Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP), Encapsulating Security Payload (ESP), Generic Routing Encapsulation (GRE), or the keyword Any. You could also use an IP protocol number instead.

- Beyond protocols, you can place port numbers or services in the access list. Some examples of port numbers are 23 (Telnet), 80 (HTTP), 443 (SSL [Secure Sockets Layer]), 500 (Internet Security Association Key Management Protocol [ISAKMP] and 25 (SMTP [Simple Mail Transport Protocol]).

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

Configuring Downloadable ACLs

This topic describes how to create a Downloadable ACL.

Adding a Downloadable IP ACL

Before you begin, you should have already configured any Network Access Filters (NAFs) that you intend to use in your downloadable IP ACL.

To add a downloadable IP ACL, follow these steps:

Step 1   In the ACS main navigation bar, choose **Shared Profile Components**.

Step 2   Click **Downloadable IP ACLs**, and then click **Add**.

Step 3   In the Name box, type the name of the new IP ACL.

Note	The name of an IP ACL may contain up to 27 characters. The name must not contain spaces or any of the following characters: - [ ] / \ " < > —

Step 4   In the Description box, type a description of the new IP ACL.

Step 5   To add ACL content to the new IP ACL, click **Add**.

Step 6   In the Name box, type the name of the new ACL content.

Note	The name of ACL content can contain up to 27 characters. The name must not contain spaces or any of the following characters: - [ ] / \ " < > —

Step 7   In the ACL Definitions box, type the new ACL definition.

Step 8   To save the ACL content, click **Submit**.

Step 9   To associate an NAF to the ACL content, select an NAF from the Network Access Filtering box to the right of the new ACL content. If you do not assign an NAF, Cisco Secure ACS associates the ACL content to all network devices, which is the default.

Step 10   Repeat Step 5 through Step 9 until you have completely specified the new IP ACL.

Step 11   To set the order of the ACL contents, choose the radio button for an ACL definition and then click Up or Down to reposition it in the list.

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

Step 12   To save the IP ACL, click **Submit**.

Cisco Secure ACS enters the new IP ACL, which takes effect immediately. For example, if the IP ACL is for use with PIX Firewalls, it is available to be sent to any PIX Firewall that is attempting authentication of a user who has that downloadable IP ACL assigned to his or her user or group profile.

Understanding Device Command Authorization Sets

Command authorization sets create a central depository for command authorization. The capability of command authorization is available in most Cisco routers and Cisco PIX Firewalls at the local level. This section discusses how to move command authorization to the ACS. The ACS provides command authorization sets that you configure in the Group Setup section, as well as via the Shared Profile Components section. While the functionality of command authorization is the same in both areas, the benefit of configuring command authorization sets within Shared Profile Components is that you can configure the entire command set at once without continuously having to submit each command before configuring the next. Another benefit to configuring command authorization sets within Shared Profile Components is that you can configure multiple levels of command sets and apply them at either the group or the user-profile level.

PIX Command Authorization Sets require that the TACACS+ command authorization request identify the service as "pixshell." Verify that this service has been implemented in the version of PIX operating system your firewalls use; if it has not been implemented, use Shell Command Authorization Sets to perform command authorization for PIXs. As of PIX OS version 6.3, pixshell has not been implemented.

For command authorization sets that support Cisco device-management applications such as the Management Center for Firewalls in VMS, the benefits of using command authorization sets are similar. You can enforce authorization of various privileges in a device-management application by applying command authorization sets to Cisco Secure ACS groups that contain users of the device-management application. The Cisco Secure ACS groups can correspond to different roles within the device-management application and you can apply different command authorization sets to each group, as applicable.

Cisco Secure ACS has three sequential stages of command authorization filtering. Each command authorization request is evaluated in the following order:

Step 1 **Command Match:** Cisco Secure ACS determines whether the command being processed matches a command listed in the command authorization set. If no matching command is found, command authorization is determined by the Unmatched Commands setting, which is either permit or deny. Otherwise, if the command is matched, evaluation continues.

Step 2   **Argument Match:** Cisco Secure ACS determines whether the command arguments presented match the command arguments listed in the command authorization set.

— If any argument is unmatched, command authorization is determined by whether the Permit Unmatched Args option is enabled. If unmatched arguments are permitted, the command is authorized and evaluation ends; otherwise, the command is not authorized and evaluation ends.

— If all arguments are matched, evaluation continues.

Step 3   **Argument Policy:** After determining that the arguments in the command being evaluated match the arguments listed in the command authorization set, Cisco Secure ACS determines whether each command argument is explicitly permitted. If all arguments are explicitly permitted, Cisco Secure ACS grants command authorization. Cisco Secure ACS denies command authorization to any arguments that are not permitted.

Configuring Device Command Authorization Sets

To add a command authorization set, follow these steps:

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

Step 2   Choose one of the applicable command authorization set types from those listed, and then click **Add**.

Step 3   In the Name box, type a name for the command authorization set.

Note	The set name can contain up to 27 characters. Names cannot contain the characters #, ?, ", *, >, or <. Leading and trailing spaces are not allowed.

Step 4   In the Description box, type a description of the command authorization set.

If Cisco Secure ACS displays an expandable checklist tree below the Name and Description boxes, use the checklist tree to specify the actions permitted by the command authorization set. To do so, follow these steps:

Step 1   To expand a checklist node, click the plus (+) symbol to its left.

Step 2   To enable an action, check its check. For example, to enable a Device View action, check the View box under the Device checklist node.

Step 3   To enable other actions in this command authorization set, repeat Step 1 and Step 2, as needed.

If Cisco Secure ACS displays additional boxes below the Name and Description boxes, use the boxes to specify the commands and arguments permitted or denied by the command authorization set. To do so, follow these steps:

Step 1   To specify how Cisco Secure ACS should handle unmatched commands, choose either the Permit or Deny option, as applicable.

Note	The default setting is Deny.

Step 2   In the box just above the Add Command button, type a command that is to be part of the set.

Caution	Enter the full command word; if you use command abbreviations, authorization control may not function.

Note	Enter only the command portion of the command/argument string here. Arguments are added only after the command is listed. For example, with the command/argument string "show run" you would type only the command show.

Step 3   Click **Add Command**.

Step 4 To add an argument to a command, in the command list box, select the command and then enter the argument in the box to the right of the command in the format **<permit | deny> <argument>**.

Step 5 To allow arguments, which you have not listed, to be effective with this command, check the Permit Unmatched Args box.

Step 6 To add other commands to this command authorization set, repeat these steps.

Step 7 To save the command authorization set, click **Submit**.

Understanding Network Access Restrictions

Network access restrictions (NARs) provide authorization conditions that have to be met before a user can gain access to the network. Cisco Secure ACS applies these conditions using information from attributes sent by authentication, authorization, and accounting (AAA) clients. Although you may set up NARs in several ways, they are all based on matching attribute information sent by an AAA client. Therefore, you must understand the format and content of the attributes that your AAA clients send if you want to employ NARs effectively.

In setting up a NAR, you must choose whether the filter operates positively or negatively. That is, you must specify in the NAR whether to permit or deny access from AAA clients that send information that matches the information stored in the NAR. However, if a NAR encounters insufficient information to operate, it defaults to denying access.

NAR Permit and Deny Conditions

	Match	No Match	Insufficient Information
Permit	Access granted	Access denied	Access denied
Deny	Access denied	Access granted	Access denied

Cisco Secure ACS supports two basic types of NARs:

- IP-based restrictions in which the originating request relates to an existing IP address

- Non-IP-based filters for all other cases in which automatic number identification (ANI) may be used

IP-based restrictions are based on one of the following attribute fields, depending on the protocol that the AAA client uses:

- If you are using TACACS+, the rem_addr field is used.

- If you are using RADIUS IETF, the calling-station-id (attribute 31) and called-station-id (attribute 30) fields are used.

More information about NAR field interpretation is provided in the TACACS+ and RADIUS sections later in this document.

AAA clients that do not provide sufficient IP-address information (for example, some types of firewalls) do not support all NAR functions.

A *non-IP*-based NAR is a list of permitted or denied "calling" or "point of access" locations that you can use to restrict an AAA client when an IP-based connection *is not* established. The non-IP-based NAR generally uses the calling line ID (CLID) number and the Digital Number Identification Service (DNIS) number (see the figures below).

However, by entering an IP address instead of the CLID, you may use the non-IP-based filter even when the AAA client does not use a Cisco IOS® Software release that supports CLI or DNIS. In another exception to entering a CLI, you may enter a MAC address to permit or deny access when you are using a Cisco Aironet® AAA client. Likewise, you could enter the Cisco Aironet access point MAC address instead of the DNIS number. The format that you specify in

the CLI box — CLI, IP address, or MAC address — must match the format of what you receive from your AAA client. You can determine this format from your RADIUS accounting log.

When specifying a NAR, you may use an asterisk (*) as a wildcard for any value, or as part of any value, to establish a range. All of the values and conditions in a NAR specification must be met for the NAR to restrict access. In other words, the values are "ANDed."

User Interface Snapshot of IP-Based Access Restriction

User Interface Snapshot of DNIS/CLI Access Restriction

NAR Types

You may define a NAR for, and apply it to, a specific user or user group. For more information about this approach, see "Setting Network Access Restrictions for a User" or "Setting Network Access Restrictions for a User Group" in the Cisco Secures ACS online documentation. This NAR definition method will be referred to in this document as existing NAR definitions. However, in the Shared Profile Components section of Cisco Secure ACS, you may create and name a shared NAR without directly citing any user or user group. You give the shared NAR a name that can be referenced in other parts of the Cisco Secure ACS HTML interface. Then, when you set up users or user groups, you may select none, one, or multiple shared restrictions to be applied. When you specify the application of multiple shared NARs to a user or user group, choose one of two access criteria: either "All selected filters must permit" or "Any one selected filter must permit."

The following tables describe the result of the NAR evaluation process when using Shared Profile Component (SPC). The first table describes the result when one or more SPC NARs return, "Access granted." The second table describes the result when one or more SPC NAR return "Access denied".

SPC NAR Conditions when Specific Filter Reports "Access Granted" Results

SPC NAR Conditions when Specific Filter Reports "Access Granted" Results

	Match All (Default Is Success)	Match Any (Default Is Failure)
Permit filter reports Access granted (matched at least one entry)	Need to evaluate next filter	Success
Deny filter reports Access granted (did not match all entries)	Failure	Need to evaluate next filter

SPC NAR Conditions when Specific Filter Reports "Access Denied" Results

	Match All (Default Is Success)	Match Any (Default Is Failure)
Permit filter reports Access granted (did not match all entries)	Failure	Need to evaluate next filter
Deny filter reports Access granted (match at least one entry)	Need to evaluate next filter	Success

Shared access restrictions are stored in the CiscoSecure user database. You can use the Cisco Secure ACS backup and restore features. You can also replicate the shared access restrictions with other configurations, to a secondary Cisco Secure ACS.

NAR Priority Algorithm

Cisco Secure ACS uses a priority algorithm for cases in which multiple NAR definitions (existing, SPC NARs, and both user and group definitions) exist for a certain user. The following figure describes how the priority algorithm operates.

NAR Priority Algorithm
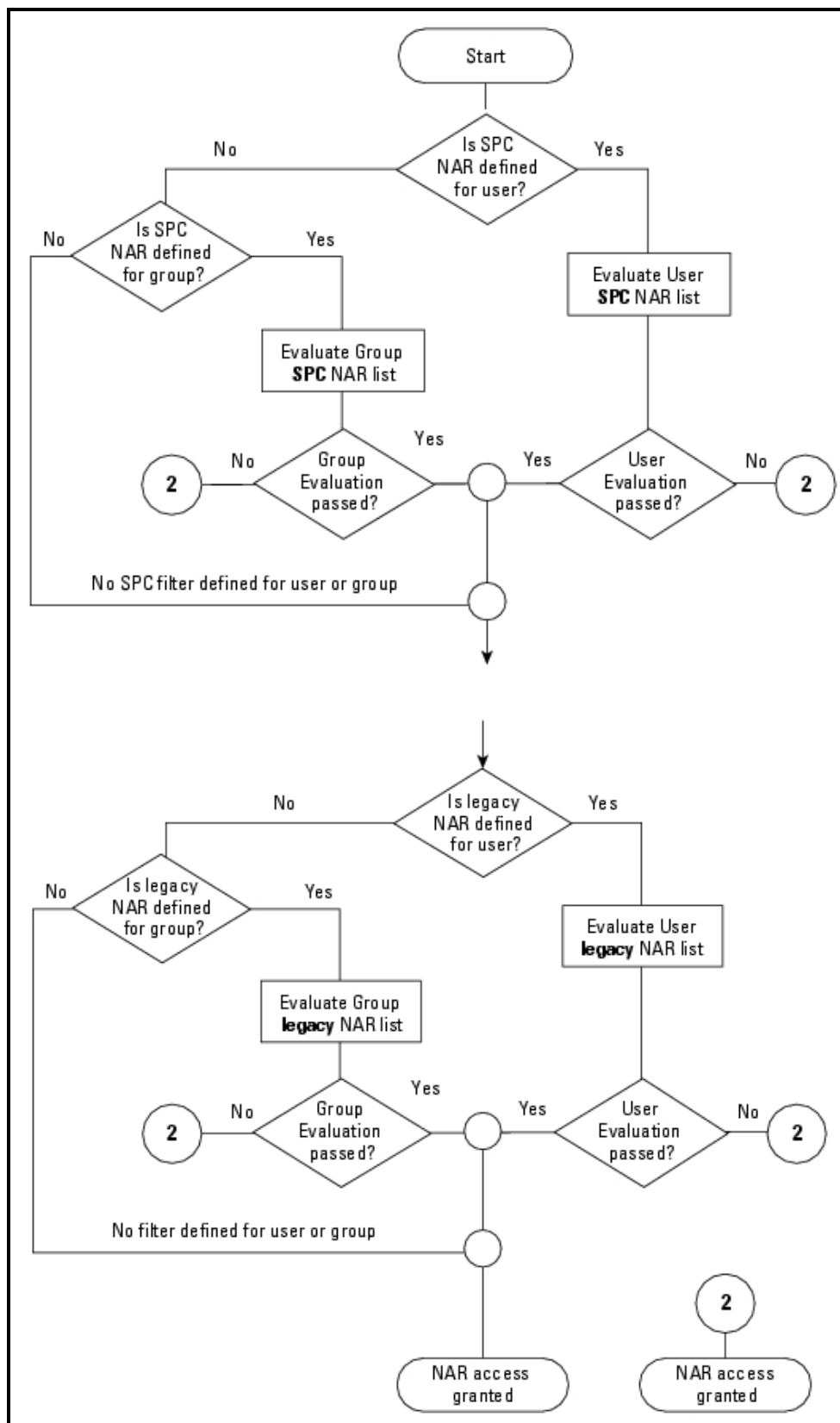
Logging and Debugging Information

You can use failed-attempts reports or passed-authentications reports to understand why access was or was not granted to a certain user. Usually, the caller ID, network access server (NAS) port, and NAS IP address fields are available and can be used to debug the session.

When the reason for acceptance or denial is unclear, you can add the Filter Information field to these reports (both to failed attempts and passed authentications). This field will provide additional data only when using SPC NARs. (All existing NARs can be easily replaced with SPC NARs.) When you use existing NARs, this field will show the first message (No Filter Activated) regardless of the results.

The following table describes all available messages in the Filter-Information-field.

Explanation of Messages in Filter Information Field

Messages for SPC NARs in Filter-Information-Field	Success/Failure	Description
No Filters activated	Success	The Shared Network Access Restrictions was not activated for this user/group (this message does not indicate that NAR SPC NAR definition is also not activated)
No Access Filters Passed	Failure	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "any one selected NAR results in permit," but none of the NAR filters in the list matched.
All Access Filters Passed	Success	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "all selected NARs result in permit," and all NAR filters in the list matched.
No Filters Selected	Success	The Shared Network Access Restrictions function was activated for this user or group, but the filter list is empty.
Failed to evaluate *<filter name> <filter entry>*	Failure	Evaluation of filter entry *<filter entry>* in filter *<filter name>* failed.
Access Filter *<filter name>* from *<id>* permitted on Filter Line: *<filter entry>*. This is sufficient to satisfy an "Any Selected" SPC NAR configuration.	Success	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "any one selected NAR results in permit," where the filter entry *<filter entry>* matched in filter *<filter name>* for user/group *<id>* (and the filter policy is permit). These conditions cause the entire evaluation to pass.
Access Filter < *filter name>* from *<id>* did not fail any criteria. This is sufficient to satisfy an "Any Selected" SPC NAR config.	Success	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "any one selected NAR results in permit," where the filter entries matched in filter *<filter name>* for user/group *<id>* (and the filter policy is deny). These conditions cause the entire evaluation to pass.
Access Filter *<filter name>* from *<id>* denied on Filter Line: *<line>*. This is sufficient to reject an "All Selected" SPC NAR config	Failure	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "all selected NARs result in permit," where filter entry *<filter entry>* matched in filter *<filter name>* for user/group *<id>* (and the filter policy is deny). These conditions cause the entire evaluation to fail.
Access Filter *<filter name>* from *<id>* did not permit any criteria. This is sufficient to reject an "All Selected'" SPC NAR config.	Failure	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "all selected NARs result in permit," where none of the filter entries matched in filter *<filter name>* for user/group *<id>* (and the filter policy is permit). These conditions cause the entire evaluation to fail.
Access Filter *<filter name>* from *<id>* denied Because of lack of required attributes. This is sufficient to reject an "All Selected" SPC NAR config.	Failure	The Shared Network Access Restrictions function was activated for this user or group. The matching policy is that "all selected NARs result in permit," where some of the attributes were missing when matching filter *<filter name>* for user/group *<id>*. These conditions cause the entire evaluation to fail.

Note	The success/failure result is relevant only to the SPC NAR evaluation process. It is possible that if both existing NAR and SPC NAR are used simultaneously, a NAR success message can appear in a failed-attempts report, in which the user passed evaluation for SPC NAR but was denied based on an existing NAR. (The latter determines the result as described in the priority algorithm.)

Filter Selection for TACACS+ Protocol

A TACACS+ session can be checked against IP-based NARs or DNIS/CLI-based NARs. Depending on the user session information, Cisco Secure ACS chooses:

- IP-based NAR when the rem_addr field in the TACACS+ start packet body contains a valid IP address
- DNIS/CLI-based NAR in all other cases

NAR Field Interpretation for TACACS+ Protocol

The following tables describe how Cisco Secure ACS utilizes the different NAR fields when using TACACS+.

IP-Based NAR

NAR Field	TACACS+ fields used when evaluating
AAA client	NAS IP address (taken from the source address in the socket between Cisco Secure ACS and the TACACS+ client)
Port	Taken from port field in the TACACS+ start packet body
Address	Taken from the rem_addr field in TACACS+ start packet body

DNIS/CLI-Based NAR

NAR entry	TACACS+ fields used when evaluating
AAA client	NAS IP address (taken from the source address in the socket between Cisco Secure ACS and the TACACS+ client)
Port	Taken from port field in the TACACS+ start packet body
CLI	Taken from the rem_addr field in TACACS+ start packet body
DNIS	Taken from the rem_addr field in TACACS+ start packet body. In cases in which the rem_addr data begins with "/" the DNIS field will contain the rem_addr data without the "/" character

Filter Selection for RADIUS Protocol

A RADIUS session can be checked against IP-based NARs or DNIS/CLI-based NARs. Depending on the user session information, Cisco Secure ACS chooses:

- IP-based NAR when the calling-station-id (RADIUS attribute 31) contains a valid IP address
- DNIS/CLI-based NAR in all other cases

NAR Field Interpretation for RADIUS Protocol

The following tables describe how Cisco Secure ACS utilizes the different NAR fields when using RADIUS protocol.

IP-Based NAR

NAR Field	Radius fields used when evaluating
AAA client	NAS-IP-Address (RADIUS attribute 4) or, if NAS-IP-Address does not exist, NAS-Identifier (RADIUS attribute 32)
Port	NAS-Port (RADIUS attribute 5) or, if NAS-Port does not exist, NAS-Port-Id (RADIUS attribute 87)
Address	Calling-Station-Id (RADIUS attribute 31)

DNIS/CLI-Based NAR

NAR Entry	Radius fields used when evaluating
AAA client	NAS-IP-Address (RADIUS attribute 4) or, if NAS-IP-Address does not exist, NAS-Identifier (RADIUS attribute 32)
Port	NAS-Port (RADIUS attribute 5) or, if NAS-Port does not exist, NAS-Port-Id (RADIUS attribute 87)
CLI	Calling-Station-Id (RADIUS attribute 31)
DNIS	Called-Station-Id (RADIUS attribute 30)

References

RFC2865 – RADIUS protocol

RFC2869 – RADIUS protocol extensions

List of RADIUS attributes – www.iana.org/assignments/radius-types

Configuring Network Access Restrictions

You can create a shared NAR that contains many access restrictions. Although the Cisco Secure ACS HTML interface does not enforce limits to the number of access restrictions in a shared NAR or to the length of each access restriction, there are limits that you must adhere to, as follows:

- The combination of fields for each line item cannot exceed 1024 characters.

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

Before defining a NAR, you must establish the elements you intend to use in the NAR. This means that you must specify all NAFs and network device groups (NDGs), and define all relevant AAA clients before making them part of the NAR definition.

To add a shared NAR, follow these steps:

Step 1   In the ACS main navigation bar, choose **Shared Profile Components**.

Step 2   Click **Network Access Restrictions**, and then click **Add**.

Step 3   In the Name box, type a name for the new shared NAR.

Note   The name can contain up to 31 characters. Leading and trailing spaces are not allowed. Names cannot contain the four characters [,], ',' (i.e. comma), or /.

Step 4   In the Description box, type a description of the new shared NAR.

Step 5   If you want to permit or deny access based on IP addressing, follow these steps:

- Check the Define IP-based access descriptions box.

- To specify whether you are listing addresses that are permitted or denied, from the Table Defines list, choose the applicable value.

Step 6   To specify the clients that this NAR applies to, choose one of the following values from the AAA Client list:

- The name of the NDG

- The name of the NAF

- The name of the particular AAA client

- All AAA clients

Step 7   To specify the information that this NAR should filter on, type values in the following boxes, as applicable:

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

- **Port:** Enter the number of the port on which to filter.

— **CLI:** Enter the CLI number on which to filter. You can also use this box to restrict access based on values other than CLIs, such as an IP address or MAC address; for information, see "About Network Access Restrictions."

— **DNIS:** Enter the number being dialed into on which to filter.

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

Step 8   Click **Enter**.

Step 9   To enter additional IP-based line items, repeat these steps.

If you want to permit or deny access based on calling location or values other than IP addresses, follow these steps:

Step 1   Check the **Define CLI/DNIS based access restrictions** box.

Step 2   To specify whether you are listing locations that are permitted or denied, from the Table Defines list, choose the applicable value.

Step 3   To specify the clients that this NAR applies to, choose one of the following values from the AAA Client list:

— The name of the NDG

— The name of the NAF

— The name of the particular AAA client

— All AAA clients

Tip   Only NDGs that you have already configured are listed.

Step 4   To specify the information that this NAR should filter on, enter values in the following boxes, as applicable:

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

— **Port:** Enter the number of the port on which to filter.

— **CLI:** Enter the CLI number on which to filter. You can also use this box to restrict access based on values other than CLIs, such as an IP address or MAC address; for information, see "About Network Access Restrictions."

— **DNIS:** Enter the number being dialed into on which to filter.

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

Step 5 Click **Enter**.

Step 6 To enter additional non-IP-based NAR line items, repeat these steps.

Step 7 To save the shared NAR definition, click **Submit**.

Restricting Access Point Login

The process of restricting AP login is very simple. To complete this configuration, you use Network Access Restrictions. A careful review of the previous section will describe how a NAR can be used to restrict login from any device. Simply use the NAR in conjunction with the AP that is defined as an NAD.

Summary

This topic summarizes the key points discussed in this lesson.

- You now understand how downloadable ACLs work.

- You can successfully configure downloadable ACLs and apply them to users and groups.

- You now understand device command authorization.

- You can successfully configure device command authorization sets to authorize commands entered by users.

- You now understand and can configure network access restrictions.

- You are able to restrict access point-device login to the access point only by using the Network Access Restrictions that you have configured.

Lesson 3

ACS Reporting

Overview

It is important to understand the reporting capabilities available in Access Control Server (ACS). This lesson covers the reporting capabilities in ACS for Windows Server only. This lesson also covers how to manage these reports.

Objectives

Upon completing this lesson, you will be able to work with reports in ACS. This ability includes being able to meet these objectives:

- View ACS reports and activity
- Configure report options
- Use reports to troubleshoot, track user activity and check resource allocation

Reports and Activity

This topic describes viewing reports and activity in ACS.
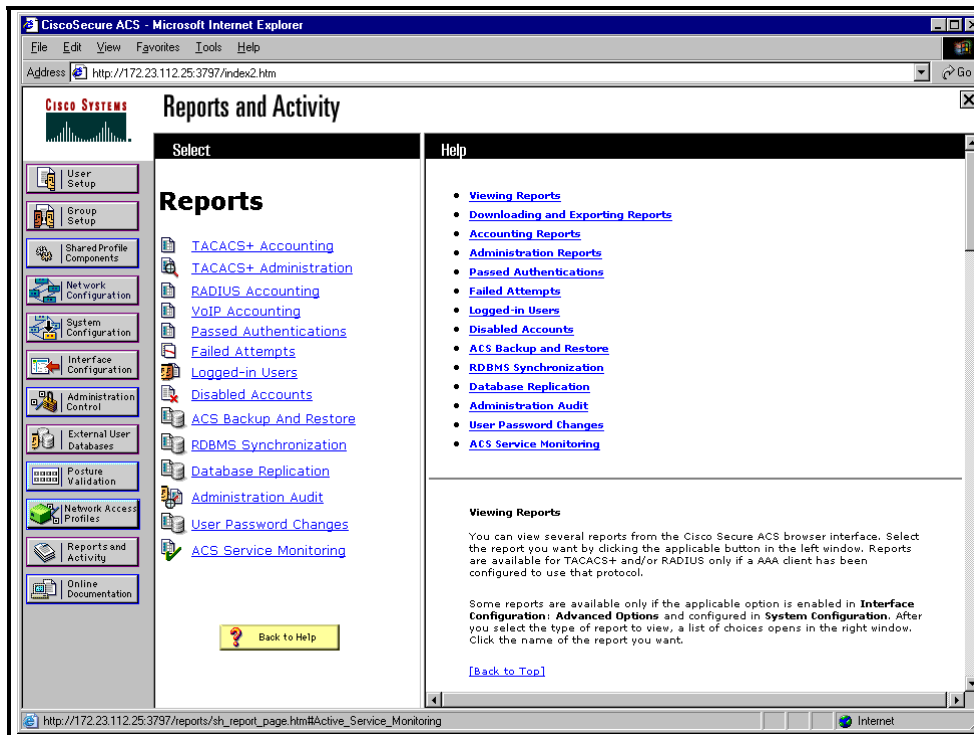
ACS has the capability to provide you, the network administrator, with a number of report logs and can give you information about Remote Authentication Dial-In User Service (RADIUS) interaction with authentication, authorization, and accounting (AAA) clients, TACACS+ interaction with AAA clients, and many other aspects of your AAA environment. You can see a list of these reports in the ACS interface by choosing Reports and Activity from the ACS main navigation page. The result of this is seen in this example. The numerous types of reports that ACS maintains are stored either as comma-separated value (CSV) files or perhaps as a dynamic report that is not stored at all. The CSV files make it easy to import the reports into other programs that generate custom reports, such as Microsoft Excel or Microsoft Access. Although the reports are stored as CSV files on the ACS, you can view them in the HTML interface in the form of a web page with tables. Some of the reports need to interact with accounting configurations on an AAA client while others use information gathered by ACS. Some reports keep track of failed authentication and authorization attempts, while others track the users that have been administratively disabled in ACS.

Each of the report logs in the following list can be viewed in the ACS HTML interface, downloaded and viewed in a text editor such as Notepad, or even imported into other programs that are used for custom reporting. If you have access to the file system of the ACS server, you can find them in the following directory locations:

■ **TACACS+ Accounting Reports:** Program Files\CiscoSecure ACSv*x.x*\Logs\TACACS+ Accounting

■ **TACACS+ Admin Accounting Reports:** Program Files\CiscoSecure ACSv*x.x*\Logs\TACACS+ Administration

---

- **RADIUS Accounting Reports:** Program Files\CiscoSecure ACSv*x.x*\Logs\RADIUS Accounting

- **VOIP Accounting Reports:** Program Files\CiscoSecure ACS v*x.x*\Logs\VoIPAccounting

- **Passed Authentications Reports:** Program Files\CiscoSecure ACSv*x.x*\Logs\Passed Authentications

- **Failed Attempts Reports:** Program Files\CiscoSecure ACS v*x.x*\Logs\FailedAttempts

- **ACS Backup And Restore:** Program Files\CiscoSecure ACS v*x.x*\Logs\Backup andRestore

- **RDBMS Synchronization:** Program Files\CiscoSecure ACS v*x.x*\Logs\DbSync

- **Database Replication:** Program Files\CiscoSecure ACS v*x.x*\Logs\DBReplicate

- **Administration Audit:** Program Files\CiscoSecure ACS v*x.x*\Logs\AdminAudit

- **User Password Changes:** Program Files\CiscoSecure ACS v*x.x*\CSAuth\PasswordLogs

- **ACS Service Monitoring:** Program Files\CiscoSecure ACS v*x.x*\Logs\ServiceMonitoring

If you do not want to view the report log files that ACS creates in CSV format, you can choose to use the Open Database Connectivity (ODBC) relational–database compliant form of reporting and logging. This allows ACS to send report log information directly to an ODBC-compliant relational database such as SQL or Crystal Reports. When in SQL or Crystal Reports, you have the ability to create a much more customized report based on any criteria. When this method is used, ACS still creates the local CSV files, and you can still view the reports using the ACS HTML interface.

Logging Attributes in ACS Reports

When using ACS, you can see special attributes in the ACS reports. These special attributes are designed to give the administrator more information than would normally be seen in an accounting log on an AAA server. These attributes are special because they are derived from the ACS configuration that you create. These attributes include the following:

- User-defined Attributes

- Access Device

- Network Device Group

- Device Command Set

- Filter Information

- ExtDB Info

These logging attributes are discussed in greater detail in the next few sections. All attributes for the user are based on the group that user is a member of. This might be a specific group, or it could be a generic group based on the unknown user authentication policy.

User-Defined Attributes

User attributes appear in the attributes list for any log configuration page that includes information about the user. The default text-box labels are Real Name, Description, User Field, 4, and 5 from the user configuration page. Remember that you can change these values to appear with information that is relevant to your users.

To configure user-defined attributes fields, follow these steps:

Step 1   From the ACS main navigation bar, click **Interface Configuration**.

Step 2   Click **User Attributes**.

Step 3   From the User Attributes configuration page, enter the attribute field labels, as you want them to appear. Note that this action dictates only how these attribute field labels appear in the user configuration page; you still need to enter the individual user attributes in each profile.

When a user authenticates, these "user-defined" attributes are entered into the report to give you additional information about the user.

Access Device

The Access Device attribute is an attribute that reflects the name of the AAA client configuration that is sending logging information to ACS. When AAA clients perform a transaction with ACS, the AAA client includes information for authentication to the ACS. This is done using a shared secret key. All of this information is located on the Network Configuration page. This information is used by ACS to match an AAA client configuration from the list of AAA clients in the Network Configuration page. When a match is found, ACS uses this to log the AAA Client Configuration entry to its report log.

Network Device Group

The Network Device Group attribute indicates the name of the Network Device Group of which the AAA client is a member. When a user authenticates through different AAA clients, each AAA client might be a member of a network device group, depending on your network configuration.

Device Command Set

The purpose of the Device Command Set attribute is to indicate the name of the command authorization set that was used to fulfill a command authorization request. If a command authorization is passed, you *will not* see the name of the command authorization set in a log file. If a command authorization attempt fails, you *will* see the name of the command authorization set that caused the failure, as well as additional information such as the reason for the failure.

Filter Information

Remember that when you configure Network Access Restrictions (NARs), user access can be permitted or denied based on the network access server (NAS) through which they access the network. If an NAR is assigned to a user, this attribute indicates if all of the applicable NARs permitted the user access or denied the user access. More specific information is also given that indicates which NAR, if multiple NARs are used, denied the user access. If no NARs are applied, this attribute also indicates that status. You can see this attribute information in the Passed Authentications log or Failed Attempts log.

ExtDB Info

If you have configured ACS to authenticate users to an external database, the ExtDB Info attribute contains the information that was returned by that database. For Windows NT/2000 external database authentication, this returns the domain name from which the user authenticated. For other external databases, such as CRYPTOCard authentication servers, RSA's SecurID, LDAP servers, and other external servers that are supported in ACS, the information returned is authentication information.

ACS Reports

ACS can provide numerous reports such as accounting reports, administrative reports, and system reports, among others. Some of these reports that ACS maintains might contain information from multiple sources and for multiple reasons. For example, ACS might log a failed password authentication attempt to the Failed Attempts log, and in the same log, you might find a failed attempt caused by an unknown AAA client attempting to communicate with ACS. This is where the third-party reporting programs, such as aaa-reports by Extraxi, SQL, or Microsoft Access, can provide enhanced functionality by allowing you to pull information from the logs and see only what you want to see.

Accounting Reports

ACS also maintains TACACS+, RADIUS, and Voice over IP (VoIP) accounting reports, which contain records of successful authentications during selected time periods. In addition to logging successful authentications, these logs contain information such as time/date, username, type of connection, amount of time logged in, and bytes transferred. Accounting logs contain information about the use of remote access services by users. By default, these report logs are available in CSV format. With the exception of the Passed Authentications log, you can also configure ACS to export the data for these logs to an ODBC-compliant relational database.

TACACS+ Accounting

The TACACS+ accounting report logs contain the start and stop times for a user session, AAA client messages with username, caller line identification information, and session duration.

RADIUS Accounting

RADIUS accounting files contain the following information: the start and stop times for a user session, AAA client messages with username, caller line identification information, and session duration. You can also configure ACS to include accounting for VoIP in this RADIUS accounting report log or in a separate VoIP accounting log. This is seen in the next section, "VoIP Accounting."

VoIP Accounting

Another type of accounting report that ACS provides is for VoIP. You can find this accounting information in the RADIUS accounting report log or optionally in a separate VoIP accounting report log. You might want to send VoIP accounting to both report logs. You can configure these reports in the System Configuration page under the Logging link. VoIP accounting reports contain the following information:

- VoIP session start and stop times

- AAA client messages with username

- Calling line identification (CLID) information

- VoIP session duration

As previously mentioned, you can configure ACS to include accounting for VoIP in this separate VoIP accounting log, in the RADIUS accounting log, or in both places.

Failed Attempts Report

The Failed Attempts report provides you with information related to authentication attempts that were not successful. From this report, you can gather information such as the username attempting to authenticate as well as the IP address from which they made the attempt. You also receive information to help you troubleshoot if authentication is not successful. An example of this would be a failed authentication attempt to an external database. In this situation, you receive a message similar to the following: External DB user invalid or bad password. In cases such as this, you might need to reset the user password in the external database or verify that the password entered is correct.

Passed Authentications Report

The Passed Authentications report gives you information about successful authentications. This report includes the following information:

- Date

- Time

- Message-Type

- User-Name

- Group-Name

- Caller-ID

- NAS-Port

- NAS-IP-Address

Administrative Reports

Three different administrative reports exist in ACS: TACACS+ Administration, Logged-in Users, and Disabled Accounts. Of the three reports, only TACACS+ Administration is not dynamic. It records information as it happens and can be downloaded in CSV format. The other two reports are dynamic.

TACACS+ Administration Report

The administrative report contains information about all of the TACACS+ commands requested during the period of time covered in the report. You use this report most often when you are using ACS to control access to network devices or when using command authorization sets. To use the TACACS+ Administration log, you must configure TACACS+ AAA clients to perform command accounting with ACS.

Logged-in Users and Disabled Accounts Reports

The last two administrative reports are dynamic in nature, meaning that they populate the report based on the current status of ACS. The dynamic administrative reports have the following traits:

- **Logged-in Users:** the Logged-in Users report lists all users receiving services from a single AAA client or all AAA clients with access to ACS. For this log to work, you must configure AAA clients to perform authentication and accounting using the same protocol— either TACACS+ or RADIUS. This log does not work if users access the AAA device using Telnet.

- **Disabled Accounts:** The Disabled Accounts report lists all user accounts that are disabled and the reason they were disabled. From here you can re-enable the account by selecting the username link that accesses the user profile.

System Reports

System reports are report logs that record events directly related to ACS and actions it has taken. Examples of these reports are as follows:

- ACS Backup and Restore
- RDBMS Synchronization
- Database Replication
- Administration Audit
- User Password Changes
- ACS Service Monitoring

ACS Backup and Restore

The ACS Backup and Restore report lists ACS backup and restore activity that ACS has taken. This report is not configurable in the interface. The information that gets populated in this log is placed there automatically when a backup occurs, whether it is a scheduled or manual backup. The report is also populated when a restore occurs.

RDBMS Synchronization

The RDBMS Synchronization report lists RDBMS Synchronization activity. You cannot configure this.

Database Replication

The Database Replication report lists database replication activity. You cannot configure this report. It is a good idea to check this report from time to time so that you can verify that replication is being performed successfully.

Administration Audit

The Administration Audit report lists actions taken by each system administrator, such as adding users, editing groups, configuring an AAA client, or viewing reports. The Administrative Audit report can be modified. You can configure the administration audit report by following these steps:

Step 1   From the ACS main navigation bar, click **Administration Control**.

Step 2   Choose **Audit Policy**.

Step 3   To generate a new Administrative Audit CSV file at a regular interval, choose one of the following options:

- **Every day:** ACS generates a new Administrative Audit CSV file at the start of each day.

- **Every week:** ACS generates a new Administrative Audit CSV file at the start of each week.

- **Every month:** ACS generates a new Administrative Audit CSV file at the start of each month.

Step 4   To generate a new Administrative Audit CSV file when the current file reaches a specific size, choose the **When size is greater than X KB** option, and then enter the file size threshold in kilobytes in the *X* box.

To select the Administrative Audit CSV files to be saved, perform the following steps:

Step 1   From the Audit Policy page, check the **Manage Directory** box.

Step 2   To limit the number of Administrative Audit CSV files ACS retains, choose the **Keep only the last X files** option and enter the number of files you want ACS to retain in the X box.

Step 3   To limit how old Administrative Audit CSV files retained by ACS can be, choose the **Delete files older than X days** option and enter the number of days for which ACS should retain an Administrative Audit CSV file before deleting it.

Step 4   Click **Submit**.

This completes the process of configuring and managing the Administrative Audit reports.

User Password Changes

The User Password Changes report lists user password changes initiated by users, regardless of which password change mechanism was used to change the password. This log contains records of password changes accomplished by the CiscoSecure authentication agent, by the user changeable password HTML interface, or by a Telnet session on a network device using TACACS+. It does not list password changes made by an administrator in the ACS HTML interface.

You can configure this log. If you want ACS to generate a new User Password Changes log file at a regular interval, perform these steps:

Step 1   From the ACS main navigation bar, click **System Configuration**.

Step 2   Click **Local Password Management**.

Step 3   Scroll to the bottom of the page to the Password Change Log File Management section. In this configuration page, you configure options for your log files. The following options are available:

- **Every day:** ACS generates a new User Password Changes log file at the start of each day. This creates numerous .csv files.

- **Every week:** ACS generates a new User Password Changes log file at the start of each week. These logs are larger than the everyday logs and you can easily sort them in third-party software such as Microsoft Access or SQL.

- **Every month:** ACS generates a new User Password Changes log file at the start of each month. This file can be very large depending on your password change policy.

Step 4   If you want ACS to generate a new User Password Changes log file when the current file reaches a specific size, choose the **When size is greater than *X* KB** option and enter the file size threshold, in kilobytes, in the X box.

If you want to manage which User Password Changes log files ACS keeps, follow these steps:

Step 1   Check the **Manage Directory** box.

Step 2   If you want to limit the number of User Password Changes log files ACS retains, choose the **Keep only the last X files** option and enter the number of files you want ACS to retain in the X box.

Step 3   If you want to limit how old User Password Changes log files retained by ACS can be, choose the **Delete files older than X days** option and enter the number of days for which ACS should retain a User Password Changes log file before deleting it.

Step 4   Click **Submit**.

This completes the management of ACS User Password Changes log files. You can view these log files in the Reports and Activity section of the ACS HTML interface.

ACS Service Monitoring

The ACS Service Monitoring report is designed to report when the ACS services start and stop. The CSMon process builds this report. CSMon watches the ACS process and when it sees the services change, it adds a message to this log. You can configure this report to log to the Windows Event Log, which is discussed in the next section. To configure ACS service monitoring logs, perform the following tasks:

Step 1   From the ACS main navigation bar, click **System Configuration**.

Step 2   Click **ACS Service Management**.

To instruct ACS to test the login process, follow these steps:

Step 1   Check the **Test login process every *X* minutes** box.

Step 2   Enter the number of minutes (up to 3 characters) that should pass between each login process test. For example, if you choose to allow for 2 minutes between each login, you would populate the field with the number 2.

Step 3   From the If no successful authentications are recorded list choose the action that you want ACS to take when the login test fails five times.

Step 4   To have ACS generate a Windows event when a user attempts to log in to your network using a disabled account, check the **Generate event when an attempt is made to log in to a disabled account** box. You can also configure event logging either to log events to the Windows event log or to generate e-mail when an event occurs.

To configure event logging, continue with these steps:

Step 5   Under the Event Logging header, you can send all events to the Windows event log. To do this, check the **Log all events to the Windows Event log** box.

Step 6   To send an e-mail notification when an event occurs, check the **Email notification of event** box and enter an e-mail address and SMTP server.

Step 7   Click **Submit**.

Now your ACS sends you e-mail as well as logs events to the Windows Event log. To view the Windows Event log, you use the event viewer. Follow these steps to access the viewer in Windows 2000:

Step 1   Right-click the **My Computer** Icon on your desktop.

Step 2   Click **Manage**.

Step 3   Double-click in **Event Viewer**.

Step 4   Double-click the **Application** log.

You can now view the service log messages in the Windows Event Viewer.

Summary

This topic summarizes the key points discussed in this lesson.

Reports are a vital part of an ACS deployment. With this lesson, you have learned how to view reports, configure them, and now have the ability to use them for troubleshooting, user tracking, and checking resource allocation.

References

For additional information, refer to www.cisco.com/go/acs.

Module Summary

In this lesson, you learned how to work with the different authentication types that ACS supports. In addition, you learned how to work with downloadable ACLs, command authorization sets, and NARs, as well as how to view and customize different reports supplied by ACS.

Module 4

Configuring Network Access Profiles

Overview

In the past, the configuration of ACS network access was static in nature employing a one type fits all methodology. However, typical network deployments have users who tend to access and use the network in different ways. ACS 4.0 introduces the concept of Network Access Profiles, which briefly stated provides the ability to process network access requests differently depending on characteristics of the request. In this module, you will learn how to configure Network Access Profiles and their associated policies.

Module Objectives

Upon completion of this module, you will be able to configure Network Access Profiles within ACS. This ability includes being able to meet these objectives:

- Understand the role of Network Access Profiles

- General ACS Configuration for Network Access Profiles

- Create Network Access Profiles

- Configure Profile Based Policies

Getting Familiar with Network Access Profiles

Overview

A network policy may specify that a user's access requests from the internal network should be processed using EAP-PEAP and a back-end AD directory, while the same user requesting access via a VPN connection should be processed using PAP authentication and a LDAP directory. In earlier versions of ACS, this scenario was not possible; all user access requests would be processed identically. Starting with ACS 4.0, processing according to this scenario is now possible through the use of Network Access Profiles. This lesson introduces the concept of Network Access Profiles.

Objectives

Upon completion of this lesson you will have an understanding of Network Access Profiles, and what needs to be configured. This ability includes being able to meet these objectives:

- Define a Network Access Profile
- Identify components of a Network Access Profile

A New Access Request Paradigm

Although a major feature of ACS is its ability to support multiple authentication types and backend databases, prior to ACS 4.0, ACS handled all user network access requests the same according to the general authentication rules configured. Because of the diversity of most enterprises, this one type fits all methodology fails to provide the necessary access flexibility to support different types of users and access locations. In reality, different entities need to be evaluated according to different security policies to determine the type of authentication necessary for network access and usage. For example: security policies for endpoints requesting network access via a VPN connection may be different then endpoints requesting network access from a branch office.

Network Access Profiles

ACS 4.0 introduces the concept of Network Access Profiles, which allow administrators to accommodate different access types and/or security policy enforcement by providing the ability to process network access requests differently depending on characteristics of the request. The configuration of a Network Access Profile consists of defining the characteristics of an access request that will determine an access requests membership in the profile, and the authentication and authorization policies that are to be applied to access request matching the profile.
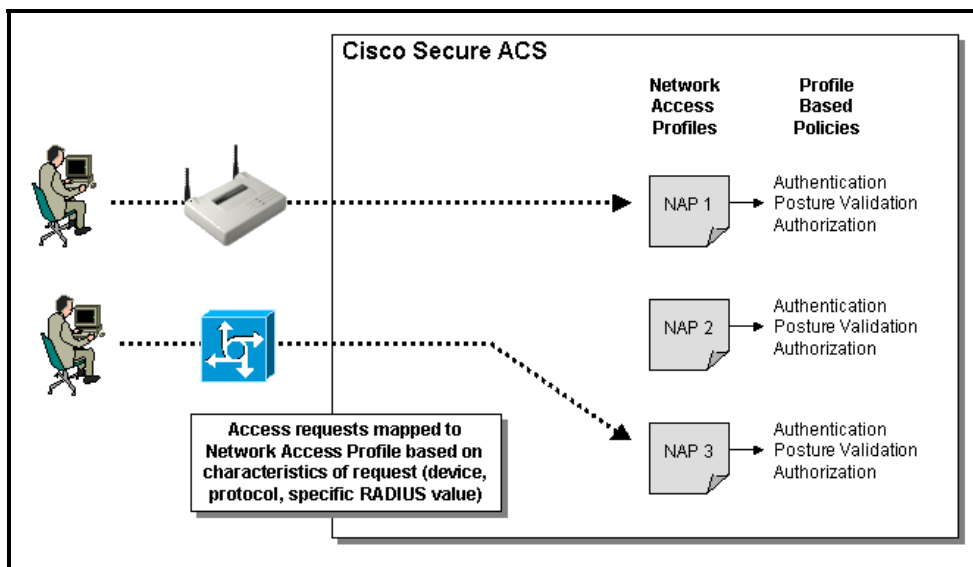
Three characteristics of an access request are used to determine how it is classified and mapped to a profile:

1. *Network Access Filter* - groupings of AAA client configurations (which may represent multiple network devices), network device groups (NDGs), or IP addresses of specific AAA client devices.

2. *Protocol Type* - AAA client vendor types from which access-requests are allowed.

Note   AAA clients are mapped to vendor when adding the clients to ACS using the **Network Configuration** task.

---

3. *Specific Radius attribute value(s)* sent by the Network Access Device that an endpoint attaches to when requesting network access.

Policies

For each Network Access Profile created, the administrator configures a set of policies to reflect the security policy for the access type represented by the profile (i.e. access via VPN connection). Configuring a profile-based policy includes creating rules for the follow activities:

■   *Authentication Rules* - Allowed protocols and Credential Validation Databases.

■   *Posture Validation Rules* – Though this step is optional, it is the bases for a Network Admissions Control (NAC) implementation.

    A complete discussion of NAC is outside the scope of this document, however, briefly stated; NAC is an industry-wide collaboration effort (led by Cisco Systems) to help ensure that every endpoint fully complies with established network security policies before being granted access to the network.

    A Posture is the term used to describe the set of attributes sent by the Communication Agent of the endpoint requesting network access defining it's state and health.

    A Posture Validation Rule is comprised of a condition and actions. The condition is a set of Required Credential Types. The actions are to determine which internal policies or external servers should be used for posture validation.

■   *Authorization Rules* – What the user is allowed to do on the network. Rules may be based on group membership, the posture of the machine that is used to access the network, or both.

Applying Policies

When ACS receives a Radius network access request, the ordered list of active Network Access Profiles is traversed until the first match is made (the Radius access request transaction could potentially map to multiple Network Access Profiles). The actions defined by the Policies associated with the matched Network Access Profile are then executed.

If no policy is matched, the administrator can configure ACS to either deny access or grant access using regular ACS global configuration for authentication and authorization.

Summary

A Network Access Profile can be simply defined as a classification of network access requests for applying common policy. One example use of a profile is to aggregate all policies that should be activated for a certain location in the network. The policies will be selected every time an access-request is initiated from that network location. Another usage is to aggregate all policies that handle the same device-type (VPN, AP).

Lesson 2

General ACS Configurations for Use with Network Access Profiles

Overview

Before detailing how to create Network Access Profiles and configure the associated policies, general ACS configurations are necessary and discussed in this lesson.

Objectives

Upon completion of this lesson you will be able to identify and configure the general configuration components of ACS necessary for the use and configuration of Network Access Profiles. This ability includes being able to meet the following objective:

- Enable general ACS configuration to complete NAP creation and configuration

General Configurations

To facilitate the configuration of Network Access Profiles and their corresponding policies, several ACS constructs must first be configured.

Note	This section assumes that configuration steps in Modules 1, 2, and 3 were completed (i.e. general authentication and authorization mechanisms, users, and groups).

AAA Clients

The first tasks are to configure both the Network Access Devices (NAD) to send RADIUS packets to ACS and to add those devices into ACS as AAA clients. Use the following steps to add NADs as AAA clients to ACS:

Step 1   In the navigation bar, click **Network Configuration** (assumes the ACS desktop is already displayed)

Step 2   Under AAA Clients, click **Add Entry**. Enter a Name, IP Address, and key for the NAD. If Network Device Groups are enabled, select a NDG for this device

Step 3   Choose **RADIUS (*vendor*)** from the *Authenticate Using* list

Step 4   Click **Submit & Restart**. (If many devices are to be added, just click Submit until all NADs are added and then click Submit & Restart.)

Note	Currently, configuring Network Access Profiles is based on RADIUS requests only. Therefore, if AAA clients (Network Access Devices) were previously added to ACS using TACACS+ as the authentication protocol (i.e. for access to the device itself), they will need to be re-added ensuring that **RADIUS (*vendor*)** is selected from the *Authenticate Using* list.

Network Access Filtering

Earlier it was mentioned that Network Access Profiles use three request characteristics to classify incoming access requests one of which is Network Access Filtering. Therefore, the ACS GUI must be configured to display the configuration task for Network Access Filtering. To display the Network Access Filtering configurations in the ACS GUI use the following steps:
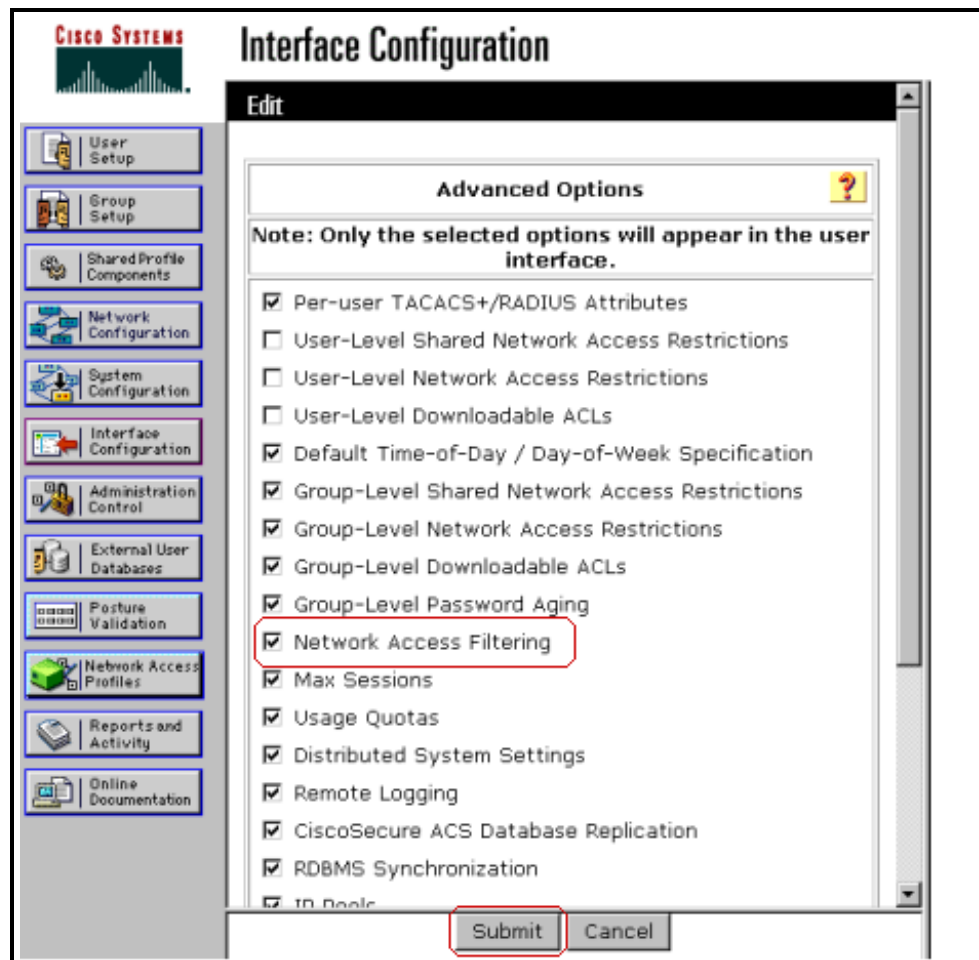
Step 1   In the navigation bar, click **Interface Configuration**

Step 2   From the displayed menu of options, click **Advance Options**

Step 3   Enable **Network Access Filtering**.

Step 4   Click **Submit**

Once the Network Access Filtering configuration task is enabled for display, create groups of devices using AAA Clients, AAA Servers, NDGs, and/or specific IP addresses using the following steps:
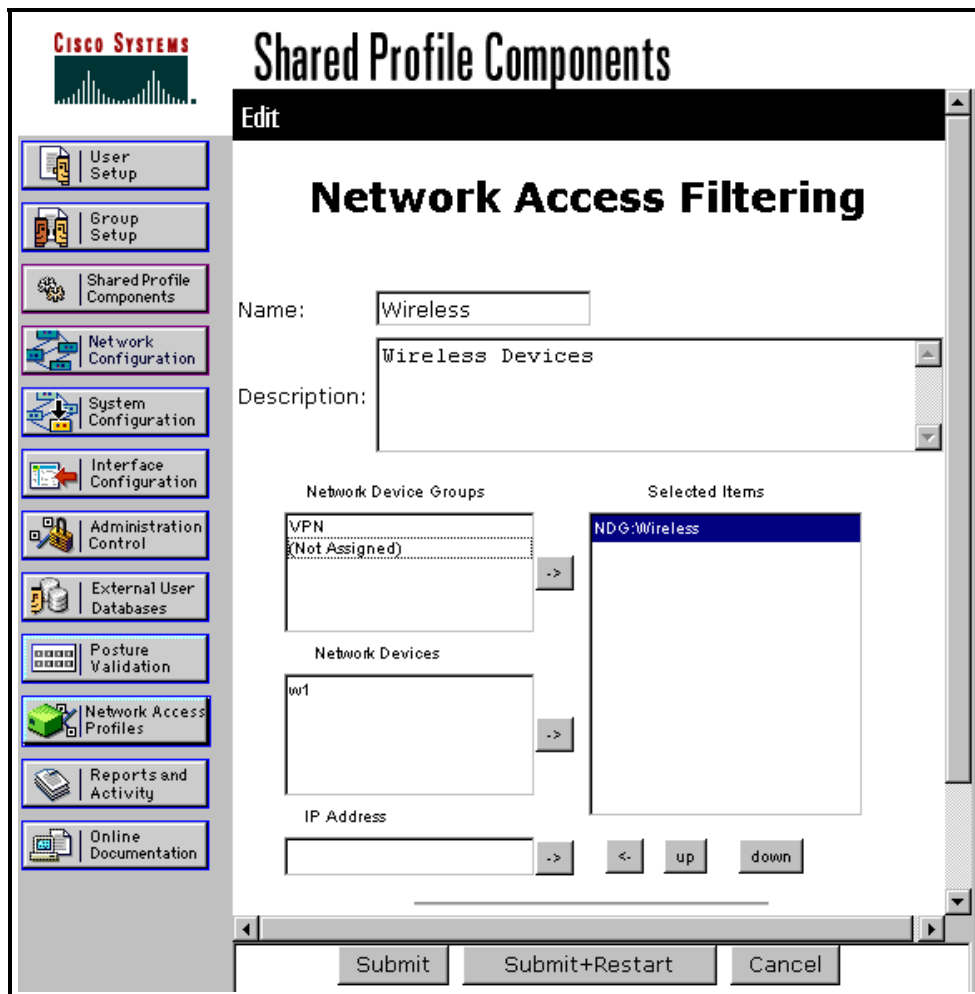
Step 1   In the navigation bar, click **Shared Profile Components**

Step 2   From the displayed menu of options, click **Network Access Filtering**

Step 3   Click **Add**

Step 4   Name the Network Access Filter and move devices and device groups to the *Selected Items* list

Step 5   Click **Submit+Restart**

Downloadable ACLs

Based on the authentication of a user and/or the posture of their machine, authorization policies may permit, deny, or limit the endpoints network access. This is carried out through the use of ACLs downloaded from ACS to the NAD. In order to configure downloadable ACLs, the configuration dialogs for downloadable ACLs must be enabled for display using the following steps:

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

Step 2   From the displayed menu of options, click **Advance Options**

Step 3   Enable Group-Level Downloadable ACLs

Step 4   Click **Submit**

For details on creating Downloadable ACLs, see Module 3 Lesson 2.

Logs and Reports

ACS includes a wide assortment of logs and reports to facilitate tracking, debugging, and troubleshooting activities. One such useful report in the context of Network Access Profiles is the **Passed Authentications** report because it can be configured to show a group mapping for each access request, thus helping to validate the Network Access Profile mapping characteristics. Enable and configure the Passed Authentication report using the following steps:

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

Step 2   From the displayed menu of options, click **Logging**

Step 3   Click the CSV Passed Authentications

Step 4   Select the Log to CSV Passed Authentications Report check box

Step 5   Click **Submit**

Summary

Because of how Network Access Profiles are configured and used, ACS must first be configured to display certain configuration tasks.

- Add Network Access Devices.

- Create Network Device Groups, if desired.

- Enable Network Access Filtering for display (allowing for their creation).

- Create Network Access Filters to be used for characterizing access requests using Network Access Profiles.

- Enable Downloadable ACLs for display (allowing for their creation).

- Enable Passed-Authentications report to assist in troubleshooting group-mappings for each processed access request.

Lesson 3

Creating Network Access Profiles

Overview

The first step in the processing of access requests by ACS is to determine which Network Access Profile the request is a member of. This lesson details the creation of Network Access Profiles and the configuration of the characteristics used to map access requests to the profile.

Objectives

Upon completion of this lesson you will be able to create and configure Network Access Profiles for use in ACS processing of Network Access Requests. This ability includes being able to meet these objectives:

- Create a new Network Access Profile
- Configure the characteristics used to map an access request to a profile
- Configure non-matching policy

Creating a New Network Access Profile

The configuration of a Network Access Profile consists of creating the set of access request matching characteristics, and the set of policies to be applied to the matching access requests. Each Network Access Profile contains a name, description, active flag, a set of three matching characteristics, and a set of policies.

Note	The next lesson will detail the configuration of the set of policies to associate with the profile.

ACS allows for the creation of Network Access Profiles from scratch as well as using templates ideally suited for NAC environments. Use the following steps to create a Network Access Profile from scratch:

Step 1   From the navigation bar, click **Network Access Profiles**

Step 2   A list of any currently defined Network Access Profiles is displayed. Click **Add Profile** to create a new profile (to edit an existing profile, click the name of the profile)

Step 3   Enter a name and description for the profile

Step 4   Select the **Active** check box to activate the profile

Access Request Characteristics

The next step in configuring the Network Access Profile is to configure the access request characteristics that determine membership in this profile. As mentioned in an earlier lesson, three conditions are used to determine how an access-request is classified and mapped to a profile. An access request is considered mapped to a profile when all three conditions match. For each of the conditions, the value "Any" can be used to always match the condition.

The following three AND'ed conditions are used to determine how an access request is classified and mapped to a profile.

1. Access request comes from a member of the selected Network Access Filter. Allows for profiles based on device type or location.

2. Access Request protocol is a member of the selected Protocol Types (The Protocol Types are a subset of the VSAs that NAS supports. ACS version 4.0 does not support the TACACS+ protocol.) Allows for profiles based on requests from a specific vendor type of equipment.

3. Access request matches a defined rule that contains one or more RADIUS attributes and values. Allows for profiles based on specific RADIUS AV pairs.

Use the following steps (continued from above) to set the access request matching criteria and complete the creation of the Network Access Profile:

Step 5   Choose the appropriate Network Access Filter to use for matching purposes from the Network Access Filter pull down list or select (Any)

Step 6 Choose the appropriate Protocols to use for matching purposes from the Protocol Types dialog or select the **Allow any Protocol** radio button

Step 7 In the Advance Filtering dialog enter an AND'ed Boolean expression that comprises RADIUS attributes and values to be used for matching purposes or select **Any**.

Step 8 Click **Submit** to create the Network Access Profile.

Creating a Network Access Profile from a Template

For NAC environments, ACS allows for the creation of Network Access Profiles from templates. The templates will populate the profile with default values. The profiles can then be customized to the specific needs of the security policy.

Note	Use of the templates requires the administrator to first enable the use of posture validations. Enable Posture Validation in **System Configuration > Global Authentications Setup**

The following types of Profile Templates available:

- Layer 3 NAC

  Use this template when network admission control is enforced by a layer-3 router based security (using EAPoUDP).

- Layer 2 NAC

  Use this template to create profiles to match users that connect to the network over a NAC and 802.1x-secured Cisco switch.

- Mac-Auth-Bypass

  This template can be used for Cisco Catalyst switches that support NAC and the MAC Authentication Bypass feature. Use this template to create profiles to match devices without a Cisco Trusted Agent, which might still be allowed access to the network after MAC address authentication. A typical example might be a printer or IP phone.

- Layer 3 NRH

  This template supports network admission control in cases when an external audit server can provide posture validation for devices without a Cisco Trusted Agent (such devices are referred to as Non Responsive Hosts).

Use the following steps to create a Network Access Profile using one of the above templates:

Step 1	From the navigation bar, click **Network Access Profiles**
Step 2	A list of any currently defined Network Access Profiles is displayed. Click **Add Template Profile** to create a new template profile
Step 3	Enter a name and description for the profile
Step 4	From the Template pull down list, select an appropriate template
Step 5	Select the **Active** check box to activate the profile
Step 6	Click **Submit** to create the Network Access Profile

Note	To edit the default values provided by this template to match specific needs of the security policy, click on the Network Access Profile name in the list displayed by clicking the **Network Access Profiles** button in the navigation bar.

Policy Order

Upon receipt of a network access request, ACS will traverse the ordered list of active profiles, and map the request to the profile first matched strategy. Therefore, the order of the profiles becomes crucial.

To change the order of the listed profiles use the following steps:

Step 1 From the list of Network Access Profiles displayed by clicking the **Network Access Profiles** button in the navigation bar, select the radio button to the left of the profile to be moved.

Step 2 Click the appropriate **Up** or **Down** button.

Step 3 Repeat steps 1 and 2 until the profile is in the desired position.

Setting Non-Matching Policy

The administrator must also set a global policy to be used in the event that an access request does not match any of the active policies. The policy can either deny access or grant access using regular ACS global configuration for authentication and authorization.

To set the global non-matching policy use the following steps:

Step 1 From the navigation bar, click **Network Access Profiles**

Step 2 A list of any currently defined Network Access Profiles is displayed. Scroll to the bottom of this list and select the radio button next to the desired non-matching policy:

— Deny access when no profile matches

— Grant access using global configuration, when no profile matches

Deleting a Network Access Profile

If necessary, use the following steps to delete a profile:

Step 1   From the Network Access Profile page, click on the **Profile Name**.

Step 2   Click **Delete** to remove the selected profile. A warning message is displayed to confirm your action.

Note	Instead of deleting the profile, the profile can also be de-activated from this page by unselecting the Active flag.

Summary

This lesson looked at the creation of Network Access Profiles. The basic creation steps include:

- Naming the Profile

- Configuring Access Request Characteristics used to map request to the profile

- Customization of the HTML interface is done via interface configuration

- Setting Profile Order

- Setting Non-matching policy

The next lesson will detail how to associate a set of rules/policies with a profile.

Associating Policies to a Profile

Overview

After setting up a profile, a set of rules/policies can be associated with it, to reflect the organization's security policies. These associations are called **Profile Based Policies**. Policies assigned to a Network Access Profile are applied when an access requests matches all three of the defined characteristics of a Network Access Profile.

Objectives

Upon completion of this lesson you will have an understanding of the ACS configuration tasks necessary to associate authentication, posture validation, and authorization policies with a Network Access Profile. This ability includes being able to meet the following objective:

■ Configure rules for authentication, Posture Validation, and authorization for a specific Network Access Profile

Profile Based Policies

After clicking the Submit button when setting up a Network Access Policy, ACS will display the list of existing Network Access Policies. For each listed profile, hyperlinks exist to allow the administrator to configure policies for Authentication, Posture Validation, and Authorization. Configuring Profile Based Policies consists of clicking each rules hyper-link and creating the rules for the following actions:

- *Authentication* – a set of configuration policies that are related to authentication mechanisms

- *Posture Validation* – If NAC is to be deployed in the network; Posture Validation is the set of attributes that define the state and health of the endpoint requesting network access.

- *Authorization* – a set of optional rules governing what an endpoint entering the network is allowed to do. If Authorization policies are not used, ACS defaults to the legacy method of authorizing by user-groups.

The following looks at the configuration for each of the policy components.

Authentication Rules

In Module 3 of this primer, the **System Configuration > Global Authentication Setup** task discussed how to configure support for various authentication protocols. Module 3 also discussed the configuration of user databases. For the configuration of a profile's Authentication Rules, the administrator sets the allowed protocols and the ordered set of Credential Validation Databases to be used. The Authentication Rules for a profile can be populated from the Global Settings and then customized or can simply be set from scratch. As a result of the authentication activity, the user requesting access is mapped to a user-group.

Use the following steps to set the Authentication Rules for a specific profile:

Step 1   From the Network Access Profile page, click on the **Authentication** hyperlink for the Profile to be modified

Step 2   Select the Authentication protocols to be used by this profile (list is based on protocols configured using general configuration tasks – see module 3 for details)

EAP Configuration

PEAP
- ☐ Allow EAP-GTC
- ☐ Allow EAP-MSCHAPv2
- ☐ Allow Posture Validation

EAP-FAST
- ☐ Allow EAP-FAST
- ☐ Allow anonymous in-band PAC provisioning
- ☐ Allow authenticated in-band PAC provisioning
  - ☐ Accept client on authenticated provisioning
  - ☐ Require client certificate for provisioning
- ☐ Allow Stateless session resume

Authorization PAC TTL [1] [hours ▼]

Allowed inner methods
- ☐ EAP-GTC
- ☐ EAP-MSCHAPv2
- ☐ EAP-TLS

Posture Validation:
- ◉ None
- ○ Required
- ○ Optional – Client may not supply posture data. Use token [Unknown ▼]
- ○ Posture only

Credential Validation Databases [?]

Available Databases
- Windows Database(Windo
- External ODBC Database

Selected Databases
- Internal Users Database

[->]
[<-]

[Up] [Down]

[Submit] [Cancel]

Step 3   Select the Credential Validation Databases to be used from the list of available databases (list of available databases based on databases configured using general configuration tasks – see modules 2 and 3 for more details). Use the Up/Down arrows to order the selected databases. ACS will try each selected database in order until a match is found

Step 4   Click **Submit** to accept this policy

Posture Validation

A Profile's Posture Validation configuration is used to determine the state and health of the machine requesting access. Posture Validation is the bases for a Network Admission Control (NAC) implementation, which is not within the scope of this primer and will only be briefly discussed.

Posture Validation Rules are used to select the posture validation components. A Posture Validation Rule comprises of a condition and actions. The condition is a set of Required Credential Types. The actions are to determine which internal policies or external servers should be used for posture validation.

Note	To configure Posture Validations, the **Allow Posture Validation** option must be enabled in the Authentications page (EAP Configuration) of the Network Access Profile.

As a result of the Posture Validation activity, a Posture Token representing the state of the endpoint is returned. Token values include: Healthy, Checkup, Transition, Quarantine, Infected, Unknown. Tokens can be used as a condition in an Authorization rule as described next.

Authorization

The Authentication Rules for a Network Access Profile are used to authenticate a user and to map the user to a user group; the profile's Posture Validation Rules (if used) supplies a Posture Token based on the state and health of the user's workstation. The profile's Authorization Rules make use of these two results to determine the authorizations to provide a user. Multiple rules can be configured for the authorization policy for a given Network Access Profile allowing for different actions depending on the requesting user's group membership or the returned posture token for the requesting end-point (i.e. user's in group 23 are denied access, and user's in group 14 are allowed restricted access controlled by a downloadable ACL).

Authorization rules are composed of:

- *Conditions* - assigned user-group and/or posture token

  And

- *Actions* – deny access, or the provisioning of the requesting device with a combination of downloadable ACL and Shared RADIUS Authorization Components

Authorization rules are evaluated in order, and the first matching condition dictates the applied actions. If no rule conditions are matched, a default action is applied.

Defining Downloadable ACLs

Restricted access to the network based on the authenticated user's user-group or the posture of his end-point is controlled using downloadable ACLs (i.e. a posture token with the value of Quarantine should allow network access only to an area to bring the workstation into compliance with security policy).

To configure Downloadable ACLs (see Module 3 Lesson 2 for complete details):

Step 1   Select **Shared Profile Components** from the navigation bar

Step 2   Select Downloadable IP ACLs.

Defining RADIUS Authorization Components (RAC)

Typically, user groups hold authorization attributes for a common group of users. However, the static nature of group attributes does not cater to the differing access needs of the same groups of users for different network services (WAN, VPN, and so on). However, creating a Network Access Profile for each network service will allow for the application of different attributes to the same user for each service through the use of RADIUS Authorization Components (RACs) selected in the authorization rules of the profile. (For example, perhaps the session-timeout needs to be several days for VPN but only several hours for WAN.) Therefore, RACs should be used when the customer requires *profile- differentiated* RADIUS authorization.

Note	Attributes defined in a static ACS group are overridden by those assigned by a Shared RAC. That attribute set is then overridden with attributes from downloadable ACL and so on. Caution is necessary when using Network Access Profile authorization policies.
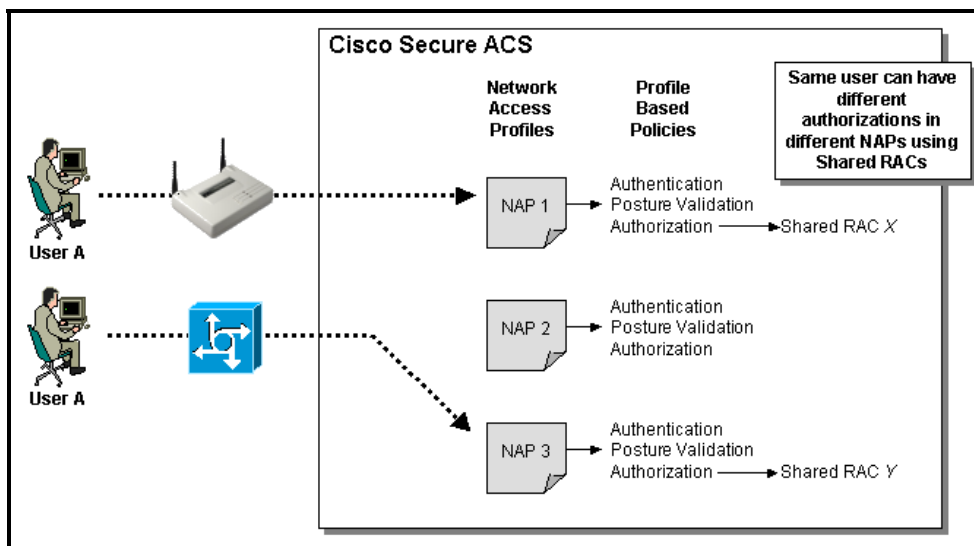
To configure Shared RADIUS Authorization Components:

Step 1 Select **Shared Profile Components** from the navigation bar

Step 2 Select RADIUS Authorization Components

Add and Configure an Authorization Rule

Use the following steps to add a new authorization rule and set its condition parameters and actions:

Step 1   From the Network Access Profile page, click on the **Authorization** hyperlink for the Profile to be modified

Step 2   Click **Add Rule**. A new row is added to the Authorization Rules list

Step 3   Under the **Conditions > User Group** column, use the pull down list to select the user group match for this rule. Select "Any Group" for the rule to match any user group assignment

Step 4   Under the **Conditions > Assessment Result** column, use the pull down list to select the Posture Token to match for this rule. Select "Any Assessment" for the rule to match any end station posture assessment (setting for a non-NAC policy)

Step 5   To deny access to users who match the conditions set in the previous two steps, enable the check box in the **Action > Deny Access** column. Go to step 7

Step 6   If the users matching the conditions set previously for this rule are to be granted access to the network with certain provisions, then select the appropriate provision from the pull down lists found in the **Action > Shared RAC** and **Action > Downloadable ACL** columns. Only previously defined RAC and ACLs will be displayed in the pull down lists

Step 7   This rule is configured; add more rules, reorder, or **Submit** the policy

RADIUS Attributes

As part of the authorization policy, the "**Include RADIUS attributes from user-group/user record**" rules are automatically enabled. If left enabled, ACS will merge the RADIUS attributes defined in the user record, user-groups, and RAC according to the following rules:

- Add all non-conflicting attributes from all sources
- If a conflict arises, then use the attribute from the highest priority source, where priority is as follows (high to low): User, RAC, and User-group.

Order the Authorization Rules

Authorization Rules are applied on a first match basis, so it is important to place your highest priority authorization policies at the top of the list. When specifying the order of Authorization Rules in a policy, determine the likelihood of each condition to be true and then order the rules so that the condition most likely to be true is first and the least likely to be true is last.

Note	If the first rule uses the condition **Any Group** for the User Group and **Any Assessment** for the Posture Token, then underlying rules will never be used.

Use the following steps to order the rules:

Step 1   From the Network Access Profile page, click on the Authorization hyperlink for the Profile to be modified

Step 2   Select the radio button to the left of the authorization rule to be reordered

Step 3   Click either the **Up** or **Down** to set the desired order for the selected authorization rule

Delete an Authorization Rule

If necessary, use the following steps to delete an authorization rule:

Step 1   From the Network Access Profile page, click on the Authorization hyperlink for the Profile to be modified

Step 2   Select the radio button to the left of the authorization rule to be deleted

Step 3   Click **Delete** to remove the selected authorization rule

Default Authorization Rule

ACS will check the conditions of each authorization rule in order to determine if there is a match. If no condition matches, the default authorization action will be applied.

Use the following steps to set the default action:

Step 1   From the Network Access Profile page, click on the Authorization hyperlink for the Profile to be modified

Step 2   After all defined authorization rules will be a table line with the condition labeled "*If a condition is not defined or there is no matched condition:*" this is where the default action is defined

Step 3   To deny access, select the check box in the "Deny Access" column. Else select the appropriate shared RAC or downloadable ACL to apply from the respective pull down lists

Activate the Changes

When a change is made to the ACS configuration, which modifies how ACS processes requests, the system must be restarted. Thus, after adding or modifying Network Access Profiles, select the **Apply and Restart** button at the bottom of the Network Access Profiles dialog.

Summary

Once a Network Access Profile has been created and configured with the set of characteristics of an access request that determines membership, a set of rules/policies can be associated with it to reflect the organization's security policies for authentication and authorization. A profile's Authentication Rules assign the access protocols and Credential Validation Databases to be used for authenticating the user. Besides authenticating a user, the authentication step maps a user to a user group.

For environments using Network Admission Control (NAC), the Posture Validation rules determine the state of the machine requesting access to assure it meets network security standards. The Posture Validation rules return a Posture Token. The mapped user group and/or the returned Posture Token are then used as conditions for determining the authorizations to apply to the user requesting access. Authorizations actions include: denying access, limiting access through downloadable ACLs, and RADIUS attributes specific to the NAP and Authorization rule through Share RACs.

Lesson 5

Use Cases

Overview

By now you should have a good understanding of the power and flexibility of Network Access Profiles. This lesson provides three use cases to further your understanding on how to create and use Network Access Profiles to meet specific security guidelines.

Objectives

Upon completing this lesson, you will have a better understanding of the power and flexibility of using Network Access Profiles. This ability includes being able to meet the following objective:

■ Know how to create Network Access Profiles to meet specific security guidelines

Use Case 1

Corporate policy dictates that users attempting network access wirelessly be authenticated differently from other users (wired access). Policy also states that different authorization variables are to be used when access is via wireless mechanisms.

Analysis

Remember that authentication mechanisms are assigned to Network Access Profiles. This indicates that we will need two different Network Access Profiles: one for wireless users and one for all other users. Next, we need to determine how to associate each access request with the appropriate Network Access Policy. This is achieved by looking at three characteristics of the access request: sending access device, protocol, or specific RADIUS values. This leads to potentially multiple ways of defining the Network Access Profiles to map access requests. For this example, we will use the network access device as the differentiator between wireless and wired access.

Typically, authorization is defined in the group and/or user configuration. This means that the same set of authorizations could be used for a particular user whether access was wireless or wired. To enforce different authorizations for wireless access, Shared RACs can be created and applied to users of particular groups when access is via wireless mechanisms.

Execution

The first step is to create a Network Access Filter that contains all wireless access points in the network.

Note   For this example, we assume that all wireless access devices have already been added to ACS as AAA clients and optionally be assigned to Network Device Groups, and that the display of the Network Access Filtering task has already been enabled as detailed in Lesson 2 of this module.
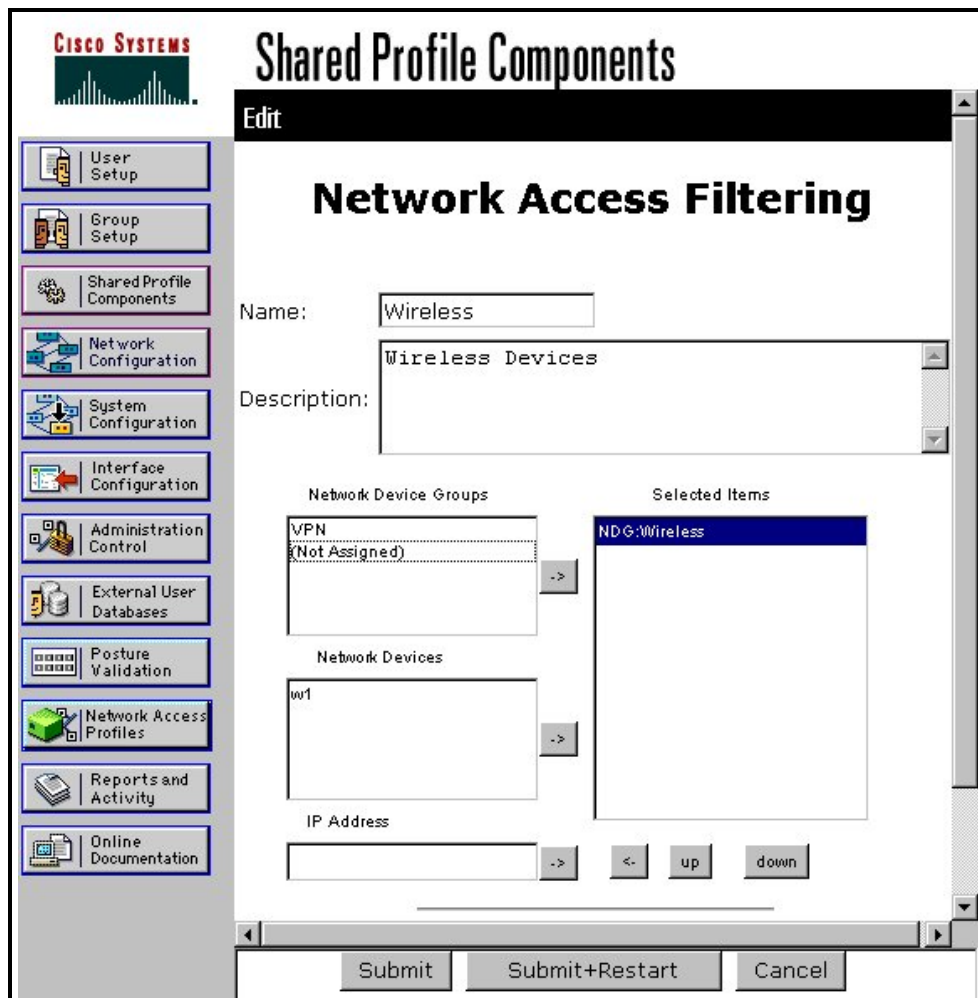
Step 1   In the navigation bar, click **Shared Profile Components**

Step 2   From the displayed menu of options, click **Network Access Filtering**

Step 3   Click **Add**

Step 4   Name the Network Access Filter and move wireless devices and device groups containing wireless access points to the *Selected Items* list

Step 5   Click **Submit+Restart**

At this point we could create a second Network Access Filter that contains all the non-wireless access points. Alternatively, since Network Access Profiles are searched in order, we can simply set the Wireless NAP as the first in the list to process any wireless access request and create a second profile that would handle all other requests – a default NAP.

Next, create the Shared RACs to be enforced for groups of users when accessing the network wirelessly.

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

Step 2   From the displayed menu of options, click **RADIUS Authorization Components.**

Step 3   A list of any currently defined RADIUS Authorization Components is displayed. Click **Add** to create a new RADIUS Authorization Component.

Step 4   Enter a **Name**, and use the pull down lists of *Attribute* categories to find the attribute to add. Click **Add** next to the attribute of choice.

Step 5   A new dialog will be displayed for configuring the selected attribute. Make the configuration and click **Submit**. You are returned to the previous screen to which a new dialog has been added for the selected and configured attribute

Step 6   Continue adding attributes. When finished click **Submit.**

Step 7   Repeat steps 3 – 6 to create and configure other RADIUS Authorization
               Components.

Note   For the new RACs to take effect, ACS must be restarted. Select **System Configuration >
             Service Control > Restart**

Now we can create the two NAPs to achieve our desire processing.

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

Step 2   A list of any currently defined Network Access Profiles is displayed. Click **Add
               Profile** to create a new profile (to edit an existing profile, click the name of the
               profile).

Step 3   Enter a name (Wireless) and description for the profile.

Step 4   Select the **Active** check box to activate the profile.

Step 5   Choose the 'Wireless" Network Access Filter created previously to use for matching
               purposes from the Network Access Filter pull down list.

Step 6   Since the Network Access Filter allows us to meet our goal of processing only
               access requests from wireless devices, we can select the **Allow any Protocol** radio
               button for the Protocol rule, and **Any** for the Advanced Filtering rule.

Step 7 Click **Submit** to create the Network Access Profile.

Repeat the above steps for our Default NAP except select **Any** (or the appropriate Network Access Filter, if created) for the Network Access Filter.

When created in this order, there is no need to modify the matching order. All 'wireless' requests will match the wireless NAP, and any 'non-wireless' request will match the default NAP.

Alternatively, instead of a "default" NAP, the NAP non-match rule could be defined as "***Grant access using global configuration when no profile matches.***" The global authentication mechanism would then be set to the authentication mechanism required for authenticating users accessing the network from "non-wireless" devices.

At this point the administrator would select the Authentication and Authorization links of both NAPs and set them according to the security policy.

To set the Authorization Policy for the Wireless NAP:

Step 1   From the Network Access Profiles dialog, select the **Authorization** link for the Wireless NAP .

Step 2   The Authorization Rules dialog is displayed. Click **Add Rule** to enter a new Authorization rule.

Step 3   Select a **Group** from the *User Group* pull-down list.

Step 4 Select a **Assessment Result** (if applicable) from the *Assessment Result* pull-down list.

Step 5 Select a **RAC** from the *Shared RAC* pull-down list.

Step 6 Repeat steps 2-5 for any addition Authorization Rules.

Step 7 Use **UP/DOWN** buttons to order rules if necessary.

Step 8 Click **Submit** to create the Network Access Profile.

Note RADIUS attributes can be merged. The order of overwriting is: static ACS groups, Shared RACs, Downloadable ACLs, Authentication Protocol, Dynamic Session, and those defined in the User configuration overriding all others. Caution is necessary when using Network Access Profile authorization policies.

When finished with all configurations, select **Apply and Restart** from the Network Access Profiles Edit dialog to have the new configuration take effect.

Use Case 2

For this example, the desired access request processing is to direct any machine authentications to an Active Directory database, and normal access requests to an OTP server.

Analysis

The first NAP that we need to create has to match access request coming from machines. To do this, we can use the Advanced Filtering part of the matching criteria to look for the NT Domain name as the first part of the user name (machine access requests are of the form NTDOMAIN/name@domain). If there are multiple NT Domains, a separate NAP will need to be created for each one since multiple Advanced Filtering rules are AND'ed together and not OR'ed. For the normal access requests, we can create a default NAP like we did in Use Case 1, or set the non-match rule to "***Grant access using global configuration when no profile matches.***" The global authentication mechanism would then be set to the authentication mechanism required for authenticating normal users (OTP database as the Credential Validation Database).

Execution

The first step is to create a separate NAP for each NT Domain to process machine access requests. In this example we will detail creating a NAP for the NT Domain CORPORATE.

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

Step 2   A list of any currently defined Network Access Profiles is displayed. Click **Add Profile** to create a new profile (to edit an existing profile, click the name of the profile).

Step 3   Enter a name (CorporateMachine) and description for the profile.

Step 4   Select the **Active** check box to activate the profile.

Step 5   Select **Any** for the Network Access Filter, and select the **Allow any Protocol** radio button for the Protocol rule.

Step 6   Use the Advanced Filtering section to match the machine user request. In the *Advanced Filtering* entry area, select **User-Name** from the pull-down *Attribute* list. Select **starts-with** from the *Operator* pull-down list. Enter the **NT Domain name** (CORPORATE) in the *Value* entry box. Click **Enter** to add rule to the element list.

Step 7   Click **Submit** to create the Network Access Profile.

Use the same steps above to add a NAP for each unique NT Domain name from which machines will request access.

Next, create a default NAP just like in Use Case 1. It will be used to process all the normal user access requests.

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

Step 2   A list of any currently defined Network Access Profiles is displayed. Click **Add Profile** to create a new profile (to edit an existing profile, click the name of the profile).

Step 3   Enter a name (Default) and description for the profile.

Step 4   Select the **Active** check box to activate the profile.

Step 5   Since this Network Access Filter is used to process any RADIUS request not previously matched, select **Any** for the Network Access Filter, select the **Allow any Protocol** radio button for the Protocol rule, and **Any** for the Advanced Filtering rule.

Step 6   Click **Submit** to create the Network Access Profile.

The next steps would be to set the authentication database to Active Directory for each of the machine access NAPs and to an OTP database for the normal user access.

Step 1 From the Network Access Profiles Edit dialog, click the **Authentication** link found under the Policies column for the NAP to be configured.

Step 2 Enable the appropriate authentication protocols to use with this NAP.

Step 3 Scroll to the bottom of the dialog to the *Credentials Verification Databases* input area. Highlight the appropriate database (previously configured) in the *Available Databases* list, and click **->** to move it to the *Selected Databases* list.

Step 4 Click **Submit** to save the authentication configuration.
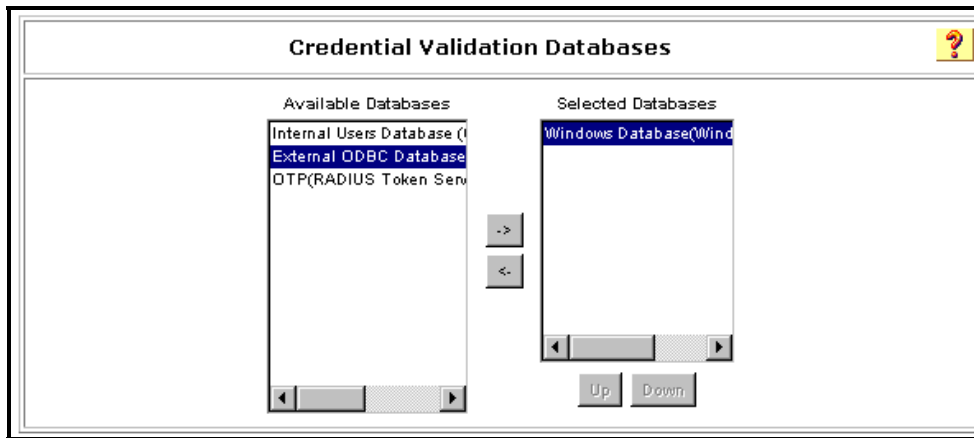
Select Windows database for all Machine Access NAPs.
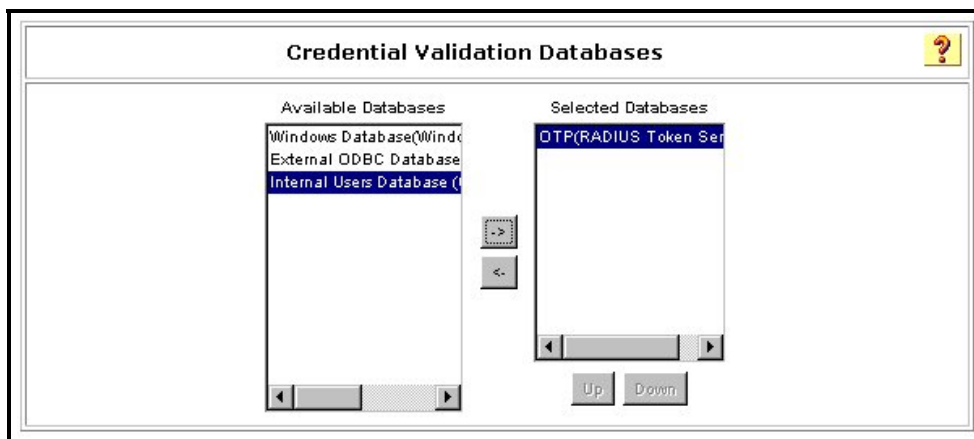
Select OTP database for default NAP.

When the machine NAPs are created first (prior to default NAP), there is no need to modify the matching order. All 'machine' requests will match the appropriate machine NAP, and any 'normal' user request will match the default NAP.

Network Access Profiles

Edit

	Name	Policies	Description	Active
○	CorporateMachine	Authentication Posture Validation Authorization	Machine access requests from the CORPORATE NT Domain.	YES
○	Default	Authentication Posture Validation Authorization	Default NAP	YES

Add Profile   Add Template Profile
Up Down
The Up/Down buttons submit and save the sort order to the database.

○ Deny access when no profile matches
⦿ Grant access using global configuration, when no profile matches

Apply and Restart

The current configuration has been changed. 'Apply and Restart' to adopt the new settings.

At this point the administrator would select the Authorization links of both NAPs and set them according to the security policy.

When finished with all configurations, select **Apply and Restart** to have the new configuration take effect.

Use Case 3

For this example, the desired access request processing is for any TACACS+ request to be authenticated using the internal database, but all RADIUS access requests to be authenticated using an OTP database.

Analysis

At first glance one might assume that two Network Access Profiles need to be created to handle the two different authentication mechanisms. However, in the current version of ACS, v4.0, NAPs do not handle TACACS+ requests. Therefore, the TACACS+ requests are handled using traditional global configuration mechanisms. If the RADIUS requests were to be authenticated the same as the TACACS+ requests, then there would not be a need to use NAPs. However, since the RADIUS requests are to be authenticated differently then the TACACS+ request, a NAP must be created to process all RADIUS requests.

Note   For this example, we assume that One Time Password (OTP) external database has already been defined and configured.

Execution

Here the NAP configuration is simple. We can use the same default configuration as we did in Use Case 1.

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

Step 2   A list of any currently defined Network Access Profiles is displayed. Click **Add Profile** to create a new profile (to edit an existing profile, click the name of the profile).

Step 3   Enter a name (Default) and description for the profile.

Step 4   Select the **Active** check box to activate the profile.

Step 5   Since this Network Access Filter is used to process any RADIUS request, select **Any** for the Network Access Filter, select the **Allow any Protocol** radio button for the Protocol rule, and **Any** for the Advanced Filtering rule.

Step 6   Click **Submit** to create the Network Access Profile.

The next step would be to set the authentication database to the OTP database.

Step 1 From the Network Access Profiles Edit dialog, click the **Authentication** link found under the Policies column for the Default NAP just created.

Step 2 Enable the appropriate authentication protocols to use with this NAP.

Step 3 Scroll to the bottom of the dialog to the *Credentials Verification Databases* input area. Highlight the OTP database (previously configured) in the *Available Databases* list, and click **->** to move it to the *Selected Databases* list.

Step 4 Click **Submit** to save the authentication configuration.
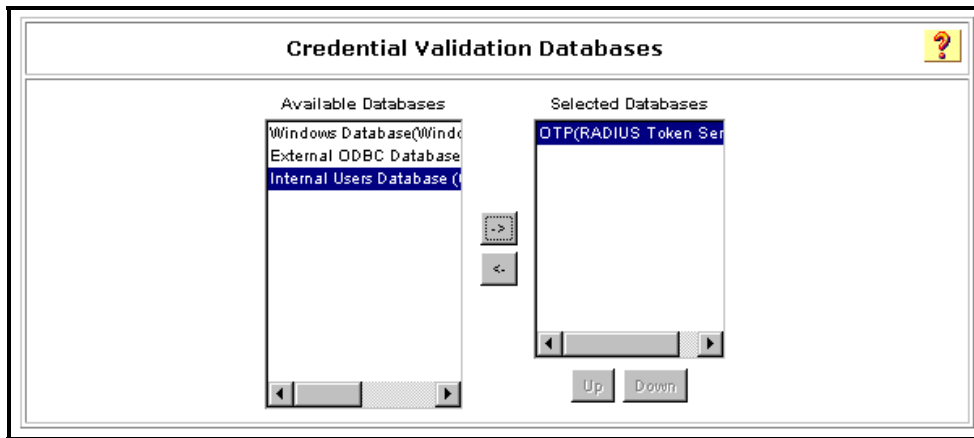
When finished with all configurations, select **Apply and Restart** from the *Network Access Profiles Edit* page to have the new configuration take effect.

Summary

This topic detailed three use cases to further increase your understanding of how beneficial and flexible Network Access Profiles are, and how they are configured.

Module Summary

Network Access Profiles add substantial flexibility to AAA processing by allowing different types of access requests to be processed as desired. An access request membership in a NAP is determined by AND'ing together three characteristics of the access request: NAD, protocol, and specific RADUIS AV pairs. Once membership in a NAP is determined, the access request is processed according to the authentication and authorization policies defined in the NAP. Starting with ACS 4.0 it is now possible to process access requests via VPN differently from access requests originating from the internal network.

References

For additional information, refer to *Cisco Secure Access Control Server for Windows* at www.cisco.com/go/acs/.

Module 5

Troubleshooting ACS

Overview

The previous modules have demonstrated how Cisco Secure ACS can be used to extend access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework, allowing greater flexibility and mobility, increased security, and user productivity gains. This module will focus on presenting a set of tools and heuristics for troubleshooting network and device access when employing ACS.

Module Objectives

Upon completion of this module, you will be able to use and apply several techniques for troubleshooting network and device access in a Cisco Secure ACS environment. This ability includes being able to meet these objectives:

■ Understand the tools available for troubleshooting access issues when ACS is used for access security

■ Use a set of heuristics to determine the source of the problem: end-point, AAA client, ACS server, or backend

Lesson 1

Troubleshooting Tools

Overview

This lesson provides a brief look at the different tools available to the Cisco Secure ACS administrator that can be useful when troubleshooting access issues. The tools discussed within this lesson can be used to help determine where the problem exists, including if it lies within the realm of a third party database back-end used for authentication by ACS.

Note	Due to the large number and diversity of back-end databases that can be used for authentication purposes by ACS, this document does not discuss the details of troubleshooting them, but rather focuses on identifying the source of the problem including it being in the back-end database. Please refer to the database manufacturer's documentation for details concerning troubleshooting their products.

Objectives

Upon completion of this lesson you will have an understanding of the tools available for troubleshooting ACS. This ability includes being able to meet these objectives:

- Identify ACS reports and service logs available for troubleshooting
- Identify ACS CLI tools available for troubleshooting
- Identify AAA client debug commands

ACS Reports

As previously discussed in Module 3 - Lesson 3, ACS provides numerous reports detailing the behavior of ACS. These reports are perhaps the primary tool used when troubleshooting ACS. In particular, the following reports provide a wealth of information when troubleshooting AAA services in an ACS environment.

- *Failed Authentications Report* – This report can typically be used as the starting point in determining the source of the problem - endpoint, the AAA client, the ACS server, or the database back-end.

- *Passed Authentications Report* - This report is useful for verifying that the appropriate authorization mappings were made.

- *Accounting Reports* - These reports are also useful for verifying that the appropriate authorization mappings were made.

In general, ACS reports provide detailed information about both RADIUS and TACACS+ interactions with respect to AAA activities.

Report Configuration

Of course, the reports are only as useful as the information they contain. ACS allows the administrator to configure each report to include the information deemed pertinent by the administrator. For example, when using Network Access Profiles, it is paramount for troubleshooting activities to include the name of the Network Access Profile that the access request was mapped to. The following steps outline how to customize the contents of an ACS report.

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

Step 2   From the displayed menu of options, click **Logging.**

Step 3   Select the desired report to configure from the list of displayed ACS reports.

Step 4   In the *Select Columns to Log* dialog, select the **Attributes** to include in the report and click **->** to add them to the **Logged Attributes** column.

Step 5   Highlight a **Logged Attribute** and use the **Up/Down** buttons to put it in the desired order.

Step 6   Click **Submit.**

System Configuration

Edit

CSV Failed Attempts File Configuration

Enable Logging ?

☑ Log to CSV Failed Attempts report

Select Columns To Log ?

Attributes

- AAA Server
- Priv-lvl
- Proxy-IP-Address
- ExtDB Info
- Source-NAS
- Filter Information
- Network Device Grou
- Access Device
- Device Command S
- PEAP/EAP-FAST-CI
- Global Message Id
- Logged Remotely
- EAP Type
- EAP Type Name
- Outbound Class
- Shared RAC
- Downloadable ACL
- System-Posture-Asse
- Application-Posture-

-> <-

Logged Attributes

- Message-Type
- User-Name
- Group-Name
- Network Access Profile N
- Authen-Failure-Code
- Author-Failure-Code
- Author-Data
- NAS-Port
- NAS-IP-Address
- Caller-ID

Up   Down

Submit   Reset Columns   Cancel

ACS Service Logs

ACS keeps numerous service log files that record all ACS service actions and activities. These logs can be used for debugging and troubleshooting activities. Unlike the ACS reports, the service log files are only accessible from the file system of the ACS server. When service logging is enabled, each ACS service generates a log whenever it is running, whether or not the provided service is being used. For example, RADIUS service logs are created even if you are not using the RADIUS protocol in your network.

Note	The service logs are typically only used by Cisco Support personnel to assist the ACS administrator in troubleshooting activities, but do contain information that can be useful to ACS administrators for troubleshooting purposes. See Module 2 – Lesson 2 page 2-64 for more details on using Service Logs for Troubleshooting.

Configuring Service Logs

ACS allows the administrator to control the creation of the service logs, the level of detail to be logged, the frequency of new file generation, and how long to keep each log. To configure Service Logging use the following steps:

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

Step 2   From the list of options, click **Service Control**.

Step 3   Use the Service Log File Configuration to control the parameters for the Service log file and directory.

— Level of Detail – control level of detail to record to service log files

> **None** - No log file is generated.
> **Low** - Only start and stop actions are logged. This is the default setting.
> **Full** - All services actions are logged.

— Generate New File - control how often a new service log file is created

> **Every Day** - ACS generates a new log file at 12:01 A.M. local time every day.
> **Every Week** - ACS generates a new log file at 12:01 A.M. local time every Sunday.
> **Every Month** - ACS generates a new log file at 12:01 A.M. on the first day of every month.
> **When Size is Greater than *x* KB** - ACS generates a new log file after the current service log file reaches the size specified, in kilobytes, by *x*.

— Manage Directory - control how long service log files are kept

> **Keep only the last *x* files** - ACS retains up to the number of files specified by *x*.
> **Delete files older than *x* days** - ACS retains only those service logs that are not older than the number of days specified by *x*.

Step 4   Click **Restart**. ACS restarts its services and implements the service log settings specified.

System Configuration

Select

CiscoSecure ACS on eclipse-ru-1 [?]

Is Currently Running

Services Log File Configuration [?]

Level of detail
- ○ None
- ○ Low
- ◉ Full

Generate New File
- ○ Every day
- ○ Every week
- ○ Every month
- ◉ When size is greater than `10240` KB

☑ Manage Directory
- ◉ Keep only the last `30` files
- ○ Delete files older than `7` days

[?] **Back to Help**

| Restart | Stop | Cancel |

ACS Command Line Utilities

ACS has a few command line utilities that can be useful when debugging access issues.

CSSupport.exe

The previous section talked about the many service logs that ACS maintains to record ACS behavior. The CSSupport utility can be used to package all the service logs together, making it easier to transfer the log files, possibly to TAC personnel for troubleshooting assistance.

CSUtil.exe

CSUtil is another ACS command line utility enabling the administrator to add, change, and delete users and AAA clients from a colon-delimited text files, as well as, perform other ACS functions. For the purposes of debugging and troubleshooting, CSUtil can be used with the '-e' option to decode error numbers found in Cisco Secure ACS service logs, thus assisting the administrator in determining the cause of the error.

| **Note** | For more information on CSUtil see Module 2 Lesson 1 |

For example, the CSRadius service log could contain a message similar to the following:

```
CSRadius/Logs/RDS.log:RDS 05/22/2001 10:09:02 E 2152 4756 Error -
1087 authenticating geddy - no NAS response sent
```

In this example, the error code number that you could use CSUtil.exe to decode is "-1087". To debug this error code, open an MS DOS command prompt on the computer running ACS, and change directories to the directory containing CSUtil.exe, and enter **CSUtil.exe -e –number** as follows:

```
C:\> cd C:\Program Files\CiscoSecure ACS v4.0\Utils
C:\Program Files\CiscoSecure ACS v4.0\Utils> CSUtil.exe -e -1087
```

Output as follows:

```
CSUtil v3.0(1.14), Copyright 1997-2001, Cisco Systems Inc

Code -1087: External database reported error during authentication
```

The decoding of this particular error code indicates the problem exists with the external database; thus, providing the administrator with the information needed to focus further troubleshooting efforts.

| **Note** | The -e option applies to ACS internal error codes only, not to Windows error codes sometimes captured in ACS service logs, such as when Windows authentication fails. |

IOS Debug

The AAA Client is an active component of the ACS AAA process. Therefore, at times, it may be useful for the administrator to have detailed information about the AAA client's processing of AAA requests. Cisco IOS includes several debugging commands that can be used to provide this information.

For general information about AAA processing including which protocol is being used, use one or more of the following commands:

— debug AAA authentication
— debug AAA authorization
— debug AAA accounting

For specific processing details for the actual AAA protocol being used, use the appropriate command from the following:

— debug radius
— debug tacacs

Summary

At some point in time, the administrator may need to troubleshoot access requests that do not behave as intended. The administrator has several tools at their disposable to assist in this effort. The ACS reports provide excellent details about each transaction, thus possibly indicating the exact problem or starting point for further investigation. Similarly, ACS can be configured to create logs for each ACS service to provide more in-depth details about the commands being executed by the services. Finally, Cisco IOS includes helpful debug commands targeted at the actual AAA processes.

Troubleshooting Heuristics

Overview

The dictionary defines troubleshooting as the activity of finding and repairing trouble, and heuristics as an aid or direction in the solution of a problem. Often times when a problem arises the toughest part is determining where to begin looking. Having a set of heuristics will greatly assist in at least providing a starting point.

This lesson provides a set of heuristics to help in determining the cause of access problems when they arise. These heuristics are ideas, rules to follow, or a method to encourage the discovery of a solution to a problem. The heuristic may not provide the exact answer to the problem, but it provides a method of troubleshooting that encourages the administrators to possibly discover the solution for themselves.

The reader should note, that many troubleshooters don't necessarily start off by trying to fix the problem, but rather apply a set of heuristics to eliminate various components (physical or of a process) in order to isolate the component responsible for the problem. Once the problem has been isolated to a component, the problem can then be corrected.

Objectives

Upon completion of this lesson you will be able to use various tools and techniques to discover the possible reasons for a failing process or service. This ability includes being able to meet these objectives:

- Understand the process of troubleshooting
- Apply heuristics to narrow down the possible location or reason for the problem

Troubleshooting Access Issues

Probably the condition that requires troubleshooting the most often when using ACS for security access, is when an end-user calls the help-desk because they can either not gain access or their authorizations aren't what were expected. Most of the time after ACS has been deployed, access issues are due to changed configurations either in the end-user system, the AAA client, the ACS server, or the database back-end (occasionally the network could actually be down as well). Therefore, to troubleshoot access issues, the administrator needs to eliminate each component until the "guilty" party is found. Luckily, the tools described in the previous lesson of this module can greatly simplify this process.

When a user first reports an unsuccessful access, the administrator should go through a number of steps to determine the source of the issue:

- *User and Group Setup* - First check the user and group setup to make sure that access wasn't denied due to a configured access restriction (Access restrictions will also be listed in the Failed Attempts report).

- *Failed Attempts Report* – This report lists authentication and authorization failures with an indication of the cause of the failed attempt. This report alone can quickly determine the cause of the failed attempt and allow the administrator to rectify the situation.

Date ▼	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port	NAS-IP-Address	Network Access Profile Name
10/17/2005	14:35:25	Authen failed	userd	Default Group	..	CS user unknown	..	..	userd	10.21.80.184	RadTestRJP
10/17/2005	14:33:51	Authen failed	userd	Default Group	..	External DB reports error condition	..	..	userd	10.21.80.184	RadTestRJP
10/17/2005	14:32:36	Authen failed	userc	Group 8	..	CS logon time restriction	..	..	userc	10.21.80.184	RadTestRJP
10/17/2005	14:29:04	Authen failed	usera	Group 499	..	Access rejected due to authorization policy	..	..	usera	10.21.80.184	RadTestRJP

This table lists a few possible error messages in the Failed Attempts report.

Code	Description
CS User Unknown	Requesting user is not found in the user database
CS CHAP Password invalid	Known user but password not correct
CS Login Time Restriction	User or Group profile has an access time restriction
Access Rejected due to Authorization Policy	Authorization policy in the mapped NAP denies user group access. Use the listed group and NAP to review the configuration of the NAP
Access Denied because their was no profile that matched	Default NAP action is to deny access. Use NAD and other information to determine why request was not matched to a NAP
External DB reports error condition	An unknown error reaching the database backed has occurred. Refer to the CSAuth service log file for more detail.

Note	The ExtDB Info attribute, found in each entry in the Failed Attempts report, contains the database that last successfully authenticated the user. It does not list the database that failed the current user authentication attempt.

If not enough information is provided or the correction of the indicated problem does not fix the issue, the administrator may try to further determine the source by using the following:

— *Logged-In Users Report* – Use this report to determine other users who also access the network through the AAA client in question, and thus if they too are having problems via the Failed Attempts report.

— *RADIUS Service Log* – This service log will provide details of the RADIUS transactions and may be used to further pinpoint the source of the fault.

■ *IOS Debug Commands* - If there is no record in the Failed Attempt report, the issue needs to be debugged from the AAA client. Use the AAA debug commands on the AAA client in question to view details of the AAA transaction. Also try:

— *Ping* – Attempt to Ping the ACS server from the AAA client to verify reachability

Note	The ping response only indicates ICMP reachability; routers in the path may have access lists that deny the forwarding of RADUIS/TACACS packets.

— *Configuration Changes* – If CiscoWorks is deployed in the network; verify that no changes have occurred to the configuration of the AAA client. At the very least, see when the AAA client's configuration was last changed.

Using the heuristics above, the administrator should now have the source of the problem narrowed down or determined.

Troubleshooting Authorization Issues

If the user is able to access the network or device, but their authorizations do not seem correct, use the following to determine the issue:

- *User and Group Setup* - First check the user and group setup to verify the authorization configuration.

- *Passed Authentications Report* – This report lists the successful authentication requests. In the case of Network Access Profiles, where mapping of authorizations is dependent on the conditions configured, this report will detail the mapping. If the mapping is not as expected, review the conditions for authorization mapping in the Network Access Profile.

Date ⬇	Time	Message-Type	User-Name	Caller-ID	NAS-Port	NAS-IP-Address	Network Access Profile Name	Shared RAC	Reason	EAP Type	EAP Type Name	PEAP/EAP FAST-Clear-Name
10/20/2005	11:32:59	Authen OK	userd	..	userd	10.21.89.165	RadTestRJP	Quarantine_RAC	..	..	..	..
10/20/2005	11:32:51	Authen OK	userc	..	userc	10.21.89.165	RadTestRJP	Quarantine_RAC	..	..	..	..
10/20/2005	11:32:43	Authen OK	userb	..	userb	10.21.89.165	RadTestRJP	Healthy_RAC	..	..	..	..

- *Accounting Reports* – If accounting is enabled on the AAA client, these reports detail the authorization mappings. The TACACS+ Accounting report is especially useful for verifying command authorization.

Summary

Through the use of a few simple heuristics, the administrator should be able to quickly isolate the exact nature of the access fault.

Module Summary

Upon completion of this module you should have an understanding of how to troubleshoot access issues. This ability includes being able to meet these objectives:

■ Understand the set of tools available for troubleshooting and their use.

■ Understand how to apply a set of heuristics to determine the source of the issue.