



CHAPTER 1

Overview of ACS Configuration

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

This chapter contains:

- [Summary of Configuration Steps, page 1-1](#)
- [Configuration Flowchart, page 1-5](#)

Summary of Configuration Steps

To configure ACS:

Step 1 Plan the ACS Deployment.

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

For detailed information, see [Chapter 2, “Deploy the Access Control Servers.”](#)

Step 2 Install the ACS Servers.

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

- *Installation Guide for Cisco Secure ACS for Windows Release 4.1*, available on Cisco.com at:
http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_installation_guides_list.html
- *Installation Guide for Cisco Secure ACS Solution Engine Release 4.1*, available on Cisco.com at:
http://www.cisco.com/en/US/products/sw/secursw/ps5338/prod_installation_guides_list.html

Step 3 Configure Additional Administrators.

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

**Note**

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

To set up additional administrative accounts:

- a. Add Administrators.
- b. For each administrator, specify administrator privileges.
- c. As needed, configure the following optional administrative policies:
 - **Access Policy**—Specify IP address limitations, HTTP port restrictions, and secure socket layer (SSL) setup.
 - **Session Policy**—Specify timeouts, automatic local logins, and response to invalid IP address connections.
 - **Password Policy**—Configure the password policy for administrators.

For detailed information, see [Chapter 3, “Password Policy Configuration Scenario.”](#)

Step 4 Configure the Web Interface:

- a. Add AAA clients and specify the authorization protocols that the clients will use.
- b. Click **Interface Configuration**.
- c. On the Interface Configuration page, configure the interface to include one or more of:
 - **RADIUS Configuration Options**—For detailed information, see “Displaying RADIUS Configuration Options” in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, “Using the Web Interface.”
 - **TACACS+ Configuration Options**—For detailed information, see “Displaying TACACS+ Configuration Options” in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, “Using the Web Interface.”
 - **Advanced Options**—For detailed information, see “Displaying RADIUS Configuration Options” in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, “Using the Web Interface.”
 - **Customized User Options**—For detailed information, see “Displaying RADIUS Configuration Options” in Chapter 2 of the *User Guide for Cisco Secure ACS 4.1*, “Using the Web Interface.”

Step 5 Configure Basic ACS System Settings:

- a. Click **System Configuration**.
- b. Configure:
 - Service Control
 - Logging
 - Date Format Control
 - Local Password Management
 - ACS Backup
 - ACS Restore
 - ACS Service Management

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

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

Step 6 Configure Users:

- a. As required for your network security setup, configure users. You can configure users:
 - Manually, by using the ACS web interface
 - By using the **CSUtil** utility to import users from an external database
 - By using database synchronization
 - By using database replication

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

Step 7 Configure Certificates.

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

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

Step 8 Configure Global Authentication Settings.

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

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

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

Step 9 Configure Shared Profile Components.

You can configure the following shared profile components:

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

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

Step 10 Set Up Network Device Groups.

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

Step 11 Add AAA Clients.

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

Step 12 Set Up User Groups.

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

Step 13 Configure Posture Validation.

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

Step 14 Set Up Network Access Profiles.

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

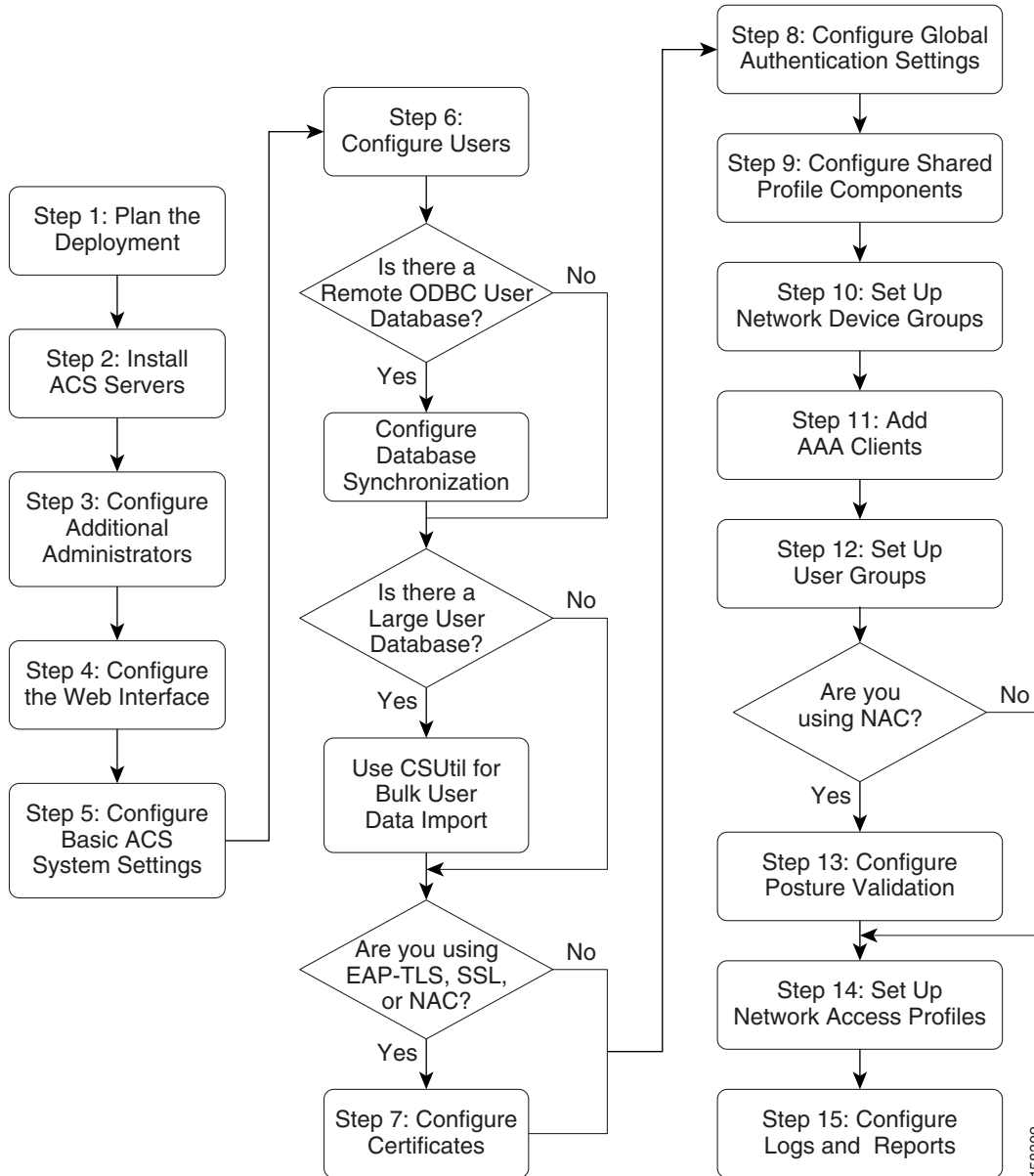
Step 15 Configure Logs and Reports.

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

Configuration Flowchart

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

Figure 1-1 ACS Configuration Flowchart



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

156309

