



System Configuration: Basic

This chapter addresses the basic features found in the System Configuration section of Cisco Secure ACS Solution Engine.

This chapter contains the following topics:

- [Service Control, page 8-2](#)
- [Logging, page 8-3](#)
- [Date Format Control, page 8-4](#)
- [Local Password Management, page 8-5](#)
- [Cisco Secure ACS Backup, page 8-8](#)
- [Cisco Secure ACS System Restore, page 8-13](#)
- [Cisco Secure ACS Active Service Management, page 8-17](#)
- [VoIP Accounting Configuration, page 8-21](#)
- [Appliance Configuration, page 8-22](#)
- [Support, page 8-25](#)
- [Viewing or Downloading Diagnostic Logs, page 8-28](#)
- [Appliance Upgrade Status, page 8-28](#)

Service Control

Cisco Secure ACS uses several services. The Service Control page provides basic status information about the services, and enables you to configure the service log files and to stop or restart the services. For more information about Cisco Secure ACS services, see [Chapter 1, “Overview”](#).



Tip

You can configure Cisco Secure ACS service logs. For more information, see [Configuring Service Log Detail, page 11-26](#).

This section contains the following topics:

- [Determining the Status of Cisco Secure ACS Services, page 8-2](#)
- [Stopping, Starting, or Restarting Services, page 8-2](#)

Determining the Status of Cisco Secure ACS Services

You can determine whether Cisco Secure ACS services are running or stopped by accessing the Service Control page.

To determine the status of Cisco Secure ACS services, follow these steps:

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

Step 2 Click **Service Control**.

The status of the services appears in the CiscoSecure ACS on *hostname* table, where *hostname* is the name of the Cisco Secure ACS.

Stopping, Starting, or Restarting Services

You can stop, start, or restart Cisco Secure ACS services as needed. This achieves the same result as starting and stopping Cisco Secure ACS services from the serial console. This stops, starts, or restarts the Cisco Secure ACS services except for CSAdmin, which is responsible for the HTML interface.

**Note**

You cannot control the CSAgent service using the Service Control page. To enable or disable the CSAgent service, see [Enabling or Disabling CSAgent, page 8-24](#).

**Tip**

If the CSAdmin service needs to be restarted, you can do so using **stop** and **start** commands on the serial console; however, it is best to use the HTML interface to restart services because there are dependencies in the order in which the services are started.

To stop, start, or restart Cisco Secure ACS services, follow these steps:

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

Step 2 Click **Service Control**.

The status of the services appears in the CiscoSecure ACS on *hostname* table, where *hostname* is the name of the Cisco Secure ACS.

If the services are running, the Restart and Stop buttons appear at the bottom of the page.

If the services are stopped, the Start button appears at the bottom of the page.

Step 3 Click **Stop**, **Start**, or **Restart**, as applicable.

The status of Cisco Secure ACS services changes to the state appropriate to the button you clicked.

Logging

You can configure Cisco Secure ACS to generate logs for administrative and accounting events, depending on the protocols and options you have enabled. For more information, including configuration steps, see [Chapter 1, “Overview”](#).

Date Format Control

Cisco Secure ACS allows for one of two possible date formats in its logs, reports, and administrative interface. You can choose either a month/day/year format or a day/month/year format.

Setting the Date Format

**Note**

If you have reports that were generated before you changed the date format, be sure to move or rename them to avoid conflicts. For example, if you are using the month/day/year format, Cisco Secure ACS assigns the name 2001-07-12.csv to a report generated on July 12, 2001. If you subsequently change to the day/month/year format, on December 7, 2001, Cisco Secure ACS creates a file also named 2001-07-12.csv and overwrites the existing file.

To set the date format, follow these steps:

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

Step 2 Click **Date Format Control**.

Cisco Secure ACS displays the Date Format Selection table.

Step 3 Select a date format option.

Step 4 Click **Submit & Restart**.

Cisco Secure ACS restarts its services and implements the date format you selected.

**Note**

For the new date format to be seen in the HTML interface reports, you must restart the connection to the Cisco Secure ACS. Click the **Logoff** button (a button with an X) in the upper-right corner of the browser window.

Local Password Management

The Local Password Management page enables you to configure settings that apply to managing passwords stored in the CiscoSecure user database. It contains the following two sections:

- **Password Validation Options**—These settings enable you to configure validation parameters for user passwords. Cisco Secure ACS enforces these rules when an administrator changes a user password in the CiscoSecure user database and when a user attempts to change passwords using the CiscoSecure Authentication Agent applet.

**Note**

Password validation options apply only to user passwords stored in the CiscoSecure user database. They do not apply to passwords in user records kept in external user databases nor do they apply to enable or admin passwords for Cisco IOS network devices.

The password validation options are listed below:

- **Password length between X and Y characters**—Enforces that password lengths be between the values specified in the X and Y boxes, inclusive. Cisco Secure ACS supports passwords up to 32 characters in length.
- **Password may not contain the username**—Requires that a user password does not contain the username anywhere within it.
- **Password is different from the previous value**—Requires a new user password to be different from the previous password.
- **Password must be alphanumeric**—Requires a user password to contain both letters and numbers.
- **Remote Change Password**—These settings enable you to configure whether Telnet password change is enabled and, if it is enabled, whether Cisco Secure ACS immediately sends the updated user data to its replication partners.

The remote change password options are listed below:

- **Disable TELNET Change Password against this ACS and return the following message to the users telnet session**—When selected, this option disables the ability to perform password changes during a Telnet session hosted by a TACACS+ AAA client. Users who submit a password change receive the text message that you type in the corresponding box.

- **Upon remote user password change, immediately propagate the change to selected replication partners**—This setting determines whether Cisco Secure ACS sends to its replication partners any passwords changed during a Telnet session hosted by a TACACS+ AAA client, by the CiscoSecure Authentication Agent, or by the User-Changeable Passwords web interface. The Cisco Secure ACSes configured as this Cisco Secure ACS's replication partners are listed below this check box.

This feature depends upon having the CiscoSecure Database Replication feature configured properly; however, replication scheduling does not apply to propagation of changed password information. Cisco Secure ACS sends changed password information immediately, regardless of replication scheduling.

Changed password information is replicated only to Cisco Secure ACSes that are properly configured to receive replication data from this Cisco Secure ACS. The automatically triggered cascade setting for the CiscoSecure Database Replication feature does not cause Cisco Secure ACSes that receive changed password information to send it to their own replication partners.

For more information about CiscoSecure Database Replication, see [CiscoSecure Database Replication, page 9-1](#).

Configuring Local Password Management

To configure password validation options, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Local Password Management**.
The Local Password Management page appears.
 - Step 3** Under Password Validation Options, follow these steps:
 - a. In Password length between *X* and *Y* characters, type the *minimum* valid number of characters for a password in the *X* box. While the *X* box accepts two characters, passwords can only be between 1 and 32 characters in length.

- b. In Password length between *X* and *Y* characters, type the *maximum* valid number of characters for a password in the *Y* box. While the *X* box accepts two characters, passwords can only be between 1 and 32 characters in length.
- c. If you want to disallow passwords that contain the username, select the **Password may not contain the username** check box.
- d. If you want to require that a user password must be different than the previous user password, select the **Password is different from the previous value** check box.
- e. If you want to require that passwords must contain both letters and numbers, select the **Password must be alphanumeric** check box.

Step 4 Under Remote Change Password, follow these steps:

- a. If you want to *enable* user password changes in Telnet sessions, clear the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box.
- b. If you want to *disable* user password changes in Telnet sessions, select the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box.
- c. In the box below the **Disable TELNET Change Password against this ACS and return the following message to the users telnet session** check box, type a message that users should see when attempting to change a password in a Telnet session and when the Telnet password change feature has been disabled in Step b.
- d. If you want Cisco Secure ACS to send changed password information immediately after a user has changed a password, select the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.



Tip

The Cisco Secure ACSes that receive the changed password information are listed below the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.

Step 5 Click **Submit**.

Cisco Secure ACS restarts its services and implements the settings you specified.

Cisco Secure ACS Backup

This section provides information about the Cisco Secure ACS Backup feature, including procedures for implementing this feature.

This section contains the following topics:

- [About Cisco Secure ACS Backup, page 8-8](#)
- [Components Backed Up, page 8-8](#)
- [Reports of Cisco Secure ACS Backups, page 8-9](#)
- [Backup Options, page 8-9](#)
- [Performing a Manual Cisco Secure ACS Backup, page 8-10](#)
- [Scheduling Cisco Secure ACS Backups, page 8-11](#)
- [Disabling Scheduled Cisco Secure ACS Backups, page 8-12](#)

About Cisco Secure ACS Backup

The Cisco Secure ACS Backup feature backs up Cisco Secure ACS system information to a file that it sends to an FTP server you specify. You can manually back up the Cisco Secure ACS system. You can also establish automated backups that occur at regular intervals or at selected days of the week and times. Maintaining backup files can minimize downtime if system information becomes corrupt or is misconfigured. We recommend copying the files from the FTP server to another computer in case the hardware fails on the FTP server.

The filename given to a backup is determined by Cisco Secure ACS. For more information about filenames assigned to backup files generated by Cisco Secure ACS, see [Backup Filenames and Locations, page 8-14](#).

For information about using a backup file to restore Cisco Secure ACS, see [Cisco Secure ACS System Restore, page 8-13](#).

Components Backed Up

The Cisco Secure ACS Backup utility backs up the CiscoSecure user database and other Cisco Secure ACS configuration data. The user database backup includes all user information, such as username, password, and other authentication

information, including server certificates and the certificate trust list. The other configuration data includes information such as NDG information, AAA client configuration, and administrator accounts.

Reports of Cisco Secure ACS Backups

When a system backup takes place, whether it was manually generated or scheduled, the event is logged in the Administration Audit report and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of Cisco Secure ACS.

For more information about Cisco Secure ACS reports, see [Chapter 1](#), “Overview”.

Backup Options

The ACS System Backup Setup page contains the following configuration options:

- **Manually**—Cisco Secure ACS does not perform automatic backups.
- **Every X minutes**—Cisco Secure ACS performs automatic backups on a set frequency. The unit of measurement is minutes, with a default backup frequency of 60 minutes.
- **At specific times...**—Cisco Secure ACS performs automatic backups at the time specified in the day and hour graph. The minimum resolution is one hour, and the backup takes place on the hour selected.
- **FTP Server**—The IP address or hostname of the FTP server that you want to send backup files to. If you specify a hostname, DNS must be enabled on your network.
- **Login**—A valid username to enable Cisco Secure ACS to access the FTP server.
- **Password**—The password for the username provided in the Login box.
- **Directory**—The directory where Cisco Secure ACS writes the backup file. The directory must be specified relative to the FTP root directory. To specify the FTP root directory, enter a single period or “dot”.
- **Encrypt backup file**—Whether Cisco Secure ACS encrypts the backup file.

- **Encryption Password**—The password used to encrypt the backup file. If the Encrypt backup file option is selected, you must provide a password.

**Note**

If an encrypted backup file is used to restore Cisco Secure ACS data, you must provide the exact password entered in the Encryption Password box when the backup was created.

Performing a Manual Cisco Secure ACS Backup

You can back up Cisco Secure ACS whenever you want, without scheduling the backup.

To perform an immediate backup of Cisco Secure ACS, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **ACS Backup**.

The ACS System Backup Setup page appears. At the top of the page, information about the last backup appears, including the following:

 - Whether the last backup succeeded.
 - The IP address of the FTP server used for the backup.
 - The directory used to store the backup.
 - The filename of the backup file created.
 - Step 3** In the FTP Server box under FTP Setup, type the IP address or hostname of the FTP server that you want Cisco Secure ACS to send the backup file to.
 - Step 4** In the Login box under FTP Setup, type a valid username to enable Cisco Secure ACS to access the FTP server.
 - Step 5** In the Password box under FTP Setup, type the password for the username provided in the Login box.
 - Step 6** In the Directory box under FTP Setup, type the relative path to the directory on the FTP server where you want the backup file to be written.
 - Step 7** If you want to encrypt the backup file, follow these steps:
 - a. Select the **Encrypt backup file** check box.

- b. In the Encryption Password box, type the password you want to use to encrypt the backup file.



Note If an encrypted backup file is used to restore Cisco Secure ACS data, you must provide the exact password entered in the Encryption Password box when the backup was created.

Step 8 Click **Backup Now**.

Cisco Secure ACS immediately begins a backup. The filename given to a backup is determined by Cisco Secure ACS. For more information about filenames assigned to backup files generated by Cisco Secure ACS, see [Backup Filenames and Locations, page 8-14](#).

Scheduling Cisco Secure ACS Backups

You can schedule Cisco Secure ACS backups to occur at regular intervals or at selected days of the week and times.

To schedule the times at which Cisco Secure ACS performs a backup, follow these steps:

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

Step 2 Click **ACS Backup**.

The ACS System Backup Setup page appears.

Step 3 To schedule backups at regular intervals, under ACS Backup Scheduling, select the **Every X minutes** option and in the *X* box type the length of the interval at which Cisco Secure ACS should perform backups.



Note Because Cisco Secure ACS is momentarily shut down during backup, if the backup interval is set too low, users might be unable to authenticate.

Step 4 To schedule backups at specific times, follow these steps:

- a. Under ACS Backup Scheduling, select the **At specific times** option.

- b. In the day and hour graph, click the times at which you want Cisco Secure ACS to perform a backup.



Tip Clicking times of day on the graph selects those times; clicking again clears them. At any time you can click **Clear All** to clear all hours, or you can click **Set All** to select all hours.

- Step 5** In the FTP box under FTP Setup, type the IP address or hostname of the FTP server that you want Cisco Secure ACS to send the backup file to.
- Step 6** In the Login box under FTP Setup, type a valid username to enable Cisco Secure ACS to access the FTP server.
- Step 7** In the Password box under FTP Setup, type the password for the username provided in the Login box.
- Step 8** In the Directory box under FTP Setup, type the relative path to the directory on the FTP server where you want the backup file to be written.
- Step 9** If you want to encrypt the backup file, follow these steps:
- a. Select the **Encrypt backup file** check box.
 - b. In the Encryption Password box, type the password you want to use to encrypt the backup file.



Note If an encrypted backup file is used to restore Cisco Secure ACS data, you must provide the exact password entered in the Encryption Password box when the backup was created.

- Step 10** Click **Submit**.
- Cisco Secure ACS implements the backup schedule you configured.

Disabling Scheduled Cisco Secure ACS Backups

You can disable scheduled Cisco Secure ACS backups without losing the schedule itself. This allows you to end scheduled backups and resume them later without having to re-create the schedule.

To disable a scheduled backup, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Backup**.
- The ACS System Backup Setup page appears.
- Step 3** Under ACS Backup Scheduling, select the **Manual** option.
- Step 4** Click **Submit**.

Cisco Secure ACS does not continue any scheduled backups. You can still perform manual backups as needed.

Cisco Secure ACS System Restore

This section provides information about the Cisco Secure ACS System Restore feature, including procedures for restoring your Cisco Secure ACS from a backup file.

This section contains the following topics:

- [About Cisco Secure ACS System Restore, page 8-13](#)
- [Backup Filenames and Locations, page 8-14](#)
- [Components Restored, page 8-15](#)
- [Reports of Cisco Secure ACS Restorations, page 8-15](#)
- [Restoring Cisco Secure ACS from a Backup File, page 8-15](#)

About Cisco Secure ACS System Restore

The ACS System Restore feature enables you to restore your system configuration from backup files generated by the ACS Backup feature. This feature helps minimize downtime if Cisco Secure ACS system information becomes corrupted or is misconfigured.

The ACS System Restore feature only works with backup files generated by a Cisco Secure ACS running an identical Cisco Secure ACS version and patch level.

Backup Filenames and Locations

The ACS System Restore feature restores the Cisco Secure ACS user database and other Cisco Secure ACS configuration data from a backup file that was created by the ACS Backup feature. You can restore from a backup file on any FTP server. You can restore from the latest backup file, or if you suspect that the latest backup was incorrect, you can select an earlier backup file to restore from.

Cisco Secure ACS sends backup files to an FTP server specified on the ACS System Backup Setup page. On the FTP server, backup files are written to the directory specified when you schedule backups or perform a manual backup.

Cisco Secure ACS creates backup files using the date and time format:

*dd-*mmm*-*yyyy*-*hh*-*nn*-*ss*.dmp*

where:

- *dd* is the date the backup started
- *mmm* is the month, abbreviated in alphabetic characters
- *yyyy* is the year
- *hh* is the hour, in 24-hour format
- *nn* is the minute
- *ss* is the second at which the backup started

For example, if Cisco Secure ACS started a backup on October 13, 1999, 11:41:35 a.m., Cisco Secure ACS would generate a backup file named:

13-Oct-1999-11-41-35.dmp

If you chose to encrypt the backup file, the backup filename includes the lowercase letter *e* just before the “.dmp” file extension. If the previous example was an encrypted backup file, the file name would be:

13-Oct-1999-11-41-35e.dmp

If you are not sure of the FTP server and directory used to create the latest backup file, check the ACS System Restore Setup page. Information about the most recent backup and restore, if any, is displayed at the top of the page.

Components Restored

You can select the components to restore: the user and group databases, the system configuration, or both.

Reports of Cisco Secure ACS Restorations

When a Cisco Secure ACS system restoration takes place, the event is logged in the Administration Audit report and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of Cisco Secure ACS.

For more information about Cisco Secure ACS reports, see [Chapter 1, “Overview”](#).

Restoring Cisco Secure ACS from a Backup File

You can perform a system restoration of Cisco Secure ACS whenever needed.

**Note**

Using the Cisco Secure ACS System Restore feature restarts all Cisco Secure ACS services and logs out all administrators.

To restore Cisco Secure ACS from a backup file generated by the Cisco Secure ACS Backup feature, follow these steps:

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

Step 2 Click **ACS Restore**.

The ACS System Restore Setup page appears.

With the exception of the Decryption Password box, the boxes under Select Backup To Restore From contain the values used for the most recent successful backup, as configured on the ACS System Backup Setup page.

Step 3 If you want to accept the default values for the FTP Server, Login, Password, Directory, and File boxes, proceed to step 5.

- Step 4** If you want to change any of the values in the FTP Server, Login, Password, Directory, and File boxes, follow these steps:
- a. In the FTP Server box under FTP Setup, type the IP address or hostname of the FTP server that you want Cisco Secure ACS to get the backup file from.
 - b. In the Login box under FTP Setup, type a valid username to enable Cisco Secure ACS to access the FTP server.
 - c. In the Password box under FTP Setup, type the password for the username provided in the Login box.
 - d. In the Directory box under FTP Setup, type the relative path to the directory on the FTP server where the backup file is.
 - e. Click **Browse**.

After a pause to retrieve a file list from the FTP server, a dialog box lists the Cisco Secure ACS backup files found in the directory specified. Encrypted backup files include the lowercase letter e before the “.dmp” filename extension.

**Tip**

If no files are found or the FTP server could not be accessed, click **Cancel** to close the dialog box, and repeat Step a through d.

- f. Click the filename of the backup file you want to use to restore Cisco Secure ACS.

The filename you select appears in the File box. The dialog box closes.

- Step 5** If the backup file specified the File box is encrypted, in the Decryption Password box, type the same password used to encrypt the backup file.

**Note**

The decryption password must exactly match the password specified in the Encryption Password box on the ACS System Backup Setup page.

- Step 6** If you want to restore user and group database information, select the **User and Group Database** check box.

- Step 7** If you want to restore system configuration information, select the **CiscoSecure ACS System Configuration** check box.

- Step 8** Click **Restore Now**.

Cisco Secure ACS displays a confirmation dialog box indicating that performing the restoration will restart Cisco Secure ACS services and log out all administrators.

Step 9 To continue with the restoration, click **OK**.

Cisco Secure ACS restores the system components specified using the backup file you selected. The restoration should require several minutes to complete, depending on which components you selected to restore and the size of your database.

When the restoration is complete, you can log in again to Cisco Secure ACS.

Cisco Secure ACS Active Service Management

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

This section contains the following topics:

- [System Monitoring, page 8-17](#)
- [Event Logging, page 8-19](#)

System Monitoring

Cisco Secure ACS system monitoring enables you to determine how often Cisco Secure ACS tests its authentication and accounting processes, and what automated actions it takes should tests detect a failure of these processes. Cisco Secure ACS accomplishes system monitoring with the CSMon service. For more information about the CSMon service, see [CSMon, page F-4](#). For information about monitoring the performance of system services, see [Monitoring System Information, page 8-27](#).

System Monitoring Options

You have the following options 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 often 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 a test fails, after four unsuccessful retries 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 login process failed. This list contains several built-in actions and reflects custom actions that you define. The items beginning with asterisks (*) are built-in actions.
 - ***Restart All**—Restart all Cisco Secure ACS services.
 - ***Restart RADIUS/TACACS+**—Restart only the RADIUS and TACACS+ services.
 - ***Reboot**—Reboot the Cisco Secure ACS.
 - **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.
- **Email notification of event**—Specifies whether Cisco Secure ACS sends an e-mail notification for each event.
 - **To**—The e-mail address that notification e-mail is sent to. 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.

Setting Up System 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:
- a. Select the **Test login process every X minutes** check box.
 - b. Type the number of minutes that should pass between each login process test in the X box (up to 3 characters).
 - c. From the **If no successful authentications are recorded** list, select the action Cisco Secure ACS should take when the login test fails.
- Step 4** To have Cisco Secure ACS create a log entry when a user attempts to access your network using a disabled account, select the **Generate event when an attempt is made to log in to a disabled account** check box.
- Step 5** If you want to setup event logging, proceed to [Setting Up Event Logging](#), page 8-20.
- Step 6** If you are done setting up Cisco Secure ACS Service Management, click **Submit**. Cisco Secure ACS implements the service management settings you made.
-

Event Logging

The Event Logging feature enables you to configure whether Cisco Secure ACS generates an e-mail when an event occurs. Cisco Secure ACS detects events using the System Monitoring feature. For more information about system monitoring, see [System Monitoring Options](#), page 8-17.

Setting Up Event Logging

To setup 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 an e-mail when an event occurs, follow these steps:

- a. Select the **Email notification of event** check box.
- b. In the To box, type the e-mail address to which Cisco Secure ACS should send event notification e-mail (up to 200 characters).



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

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



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

Step 4 If you want to setup system monitoring, proceed to [Setting Up System Monitoring, page 8-18](#).

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.

VoIP Accounting Configuration

The VoIP Accounting Configuration feature enables you to specify which accounting logs receive VoIP accounting data. There are three options for VoIP accounting:

- **Send to both RADIUS and VoIP Accounting Log Targets**—Cisco Secure ACS appends VoIP accounting data to the RADIUS accounting data and logs it separately to a CSV file. To view the data, you can use either RADIUS Accounting or VoIP Accounting under Reports and Activity.
- **Send only to VoIP Accounting Log Targets**—Cisco Secure ACS only logs VoIP accounting data to a CSV file. To view the data, you can use VoIP Accounting under Reports and Activity.
- **Send only to RADIUS Accounting Log Targets**—Cisco Secure ACS only appends VoIP accounting data to the RADIUS accounting data. To view the data, you can use RADIUS Accounting under Reports and Activity.

Configuring VoIP Accounting

**Note**

The VoIP Accounting Configuration feature does not enable VoIP accounting. To enable VoIP accounting, see [Chapter 1, “Overview”](#).

To configure VoIP accounting, follow these steps:

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

Step 2 Click **VoIP Accounting Configuration**.



Note If this feature does not appear, click **Interface Configuration**, click **Advanced Options**, and then select the **Voice-over-IP (VoIP) Accounting Configuration** check box.

The VoIP Accounting Configuration page appears. The Voice-over-IP (VoIP) Accounting Configuration table displays the options for VoIP accounting.

Step 3 Select the VoIP accounting option you want.

Step 4 Click **Submit**.

Cisco Secure ACS implements the VoIP accounting configuration you specified.

Appliance Configuration

Use the Appliance Configuration page to set the Cisco Secure ACS hostname, domain names, and system date and time. If you are using an appliance base image that incorporate Cisco Security Agent (CSA) or have applied an CSA update to Cisco Secure ACS Solution Engine, you can use the Appliance Configuration page to enable and disable the CSAgent service.

This section contains the following topics:

- [Setting System Time and Date, page 8-22](#)
- [Setting the Cisco Secure ACS Host and Domain Names, page 8-23](#)
- [Enabling or Disabling CSAgent, page 8-24](#)

Setting System Time and Date

This procedure details how to set system time and date from within the HTML interface. This procedure also details how to maintain the system date and time using a network time protocol (NTP) server with which the system synchronizes its date and time.



Tip

You can also perform this procedure using the serial console interface to the Cisco Secure ACS. For details, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.

To set the system date and time, follow these steps:

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

Step 2 Click **Appliance Configuration**.

Cisco Secure ACS displays the Appliance Configuration page.



Note If the system does not display the Appliance Configuration page, check your connectivity to the Cisco Secure ACS.

- Step 3** From the **Time Zone** list, select the system time zone.
- Step 4** In the **Time** box, enter the system time in the format hh:mm:ss.
- Step 5** From the **Day** list, select the day of the month.
- Step 6** From the **Month** list, select the month.
- Step 7** From the **Year** list, select the year.
- Step 8** Perform the following substeps only if you want to set up the NTP server to automatically synchronize date and time.
- Click the **NTP Synchronization Enabled** check box.
 - In the **NTP Server(s) box**, type the IP address or addresses of the NTP server(s) you want the system to use. If you enter more than one, separate the IP addresses with a space.



Note Be sure that the IP addresses you specify are valid NTP servers. Incorrect IP addresses or incorrectly operating NTP servers can greatly slow the NTP synchronization process.

- Step 9** Click **Submit**.
- The system time and date are set as specified.
-

Setting the Cisco Secure ACS Host and Domain Names

Use this procedure to configure Cisco Secure ACS host and domain names.



Note This procedure requires that you reboot the Cisco Secure ACS and, therefore, you should perform the procedure during off hours to minimize disruption of users.

To set the Cisco Secure ACS host and domain names, follow these steps:

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

Step 2 Click **Appliance Configuration**.

Cisco Secure ACS displays the Appliance Configuration page.



Note If the system does not display the Appliance Configuration page, check your connectivity to the Cisco Secure ACS.

Step 3 In the **Host Name** box, type the hostname.

Step 4 In the **Domain Name** box, type the domain name.

Step 5 At the bottom of the page, click **Reboot**.

Enabling or Disabling CSAgent

You enable or disable the protection and restrictions imposed by CSA on an appliance by enabling or disabling CSAgent. Disabling CSAgent is necessary for the following two purposes:

- Upgrading or applying patches to Cisco Secure ACS Solution Engine.
- Allowing the appliance to respond to ping requests.



Note When CSAgent is disabled, the appliance is not protected by CSA. For information about the protection CSA provides for Cisco Secure ACS Solution Engine, see [CSA Policies, page 1-25](#).

When you disable CSAgent, it remains disabled until you explicitly re-enable it. Rebooting the appliance does not restart a disabled CSAgent service.

To enable or disable CSAgent on the appliance, follow these steps:

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

Step 2 Click **Appliance Configuration**.

Cisco Secure ACS displays the Appliance Configuration page.



Note If the system does not display the Appliance Configuration page, check your connectivity to the Cisco Secure ACS.

Step 3 Select or clear the CSA Enabled check box, as applicable.

Step 4 Click **Submit**.

Cisco Secure ACS enables or disables CSAgent, as specified.

Support

You use the Support page for two purposes:

- To package system state information into a file that can be forwarded for tech support.
- To monitor the state of the Cisco Secure ACS services.

Each of these activities is detailed in the following procedures:

- [Running Support, page 8-25](#)
- [Monitoring System Information, page 8-27](#)

Running Support

You use the Support page to package system information that can be forwarded to your Technical Assistance Center (TAC) representative. When you perform this procedure, Cisco Secure ACS automatically packages all its current logs. You also have the option to package either, or both, of the following:

- User database
- System logs for the number of preceding days that you specify.

Support information is packaged in a cabinet file, which has the file extension *.cab*. Cabinet files are a compressed format, so that you can more easily send the support information to TAC or other support personnel.

To package system state information into a file for tech support, follow these steps:

**Note**

The AAA services of the Cisco Secure ACS are briefly suspended when you run this procedure. We recommend that you perform this procedure during periods of least AAA activity to minimize user impact.

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

Step 2 Click **Support**.

The Support page appears.

Step 3 If you want to include the Cisco Secure ACS user database in the support file, in the Details to collect table, select the **Collect User Database** check box.

Step 4 If you want to include archived system logs, in the Details to collect table, follow these steps:

a. Select the **Collect Previous X Days logs** check box.

b. In the X box, type the number of preceding days whose logs you want collected. The maximum number of preceding days is 9999.

Step 5 Click **Run Support Now**.

The File Download dialog box appears.

Step 6 On the File Download dialog box, click **Save**.

The Save As dialog box appears.

Step 7 Use the Save As dialog box to specify where and with what filename you want to save the cabinet file. Then click **Save**.

Cisco Secure ACS briefly suspends normal services while a support file is generated and saved as specified. When the download is complete, a Download Complete dialog box appears.

Step 8 Make note of the name and location of the support file, and then click **Close**.

A current cabinet file of support information is written to the location you specified. You can forward it as needed to a TAC representative or other Cisco support personnel.

Monitoring System Information

You use this procedure to view the status and distribution of Cisco Secure ACS resources.

The top row in the Resource Usage table displays CPU idle resource percentage and available memory space.

The remainder of the Resource Usage table shows each service, profiled as having allocated to it:

- **CPU**—A certain percentage of CPU cycles being used. In the System category, Cisco Secure ACS numbers the CPUs, starting with zero. If there is more than one CPU, the System category displays CPU information for each CPU.
- **Memory**—The amount of memory allocated by each service.
- **Handle count**—The number of system handles (that is, resources) allocated by each service.
- **Thread count**—The number of threads each service has spawned.

To monitor the status of the Cisco Secure ACS services, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Support**.
Cisco Secure ACS displays the Support page.
- Step 3** Read system information in the Resource Usage table.



Tip The first row of the Resource Usage table, marked System, displays the percentage of CPU cycles that are idle. Other rows indicate the percentage of CPU cycles used by each service. Taken together, these total 100 percent.

Viewing or Downloading Diagnostic Logs

Cisco Secure ACS records diagnostic logs whenever you apply upgrades or patches to the software running on the appliance. It also creates a diagnostic log if you use the recovery CD to restore the appliance to its original state.

In addition, if you are using an appliance base image that incorporates Cisco Security Agent (CSA) or have applied a CSA update to Cisco Secure ACS, the View Diagnostic Logs page provides access to two logs created by CSA.

To view or download an appliance diagnostic log,

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

Step 2 Click **View Diagnostic Logs**.

Cisco Secure ACS displays the View Diagnostic Logs page. In the Log File column, the log files are listed by name. In the File Size column, the size of each log file appears, in kilobytes. If Cisco Secure ACS failed to create an expected log file, “Log file is not created” appears in the File Size column.

Step 3 If you want to download a diagnostic log, right-click on the log filename and use the applicable browser feature to save the log to the location you want.

A copy of the log file is available for viewing in a third-party application, such as Microsoft Excel or a text editor. If it is requested, you can also send the diagnostic log file to Cisco support technicians.

Step 4 If you want to view a diagnostic log, click on the log filename.

Cisco Secure ACS displays the contents of the diagnostic log.

Appliance Upgrade Status

This section contains the following topics:

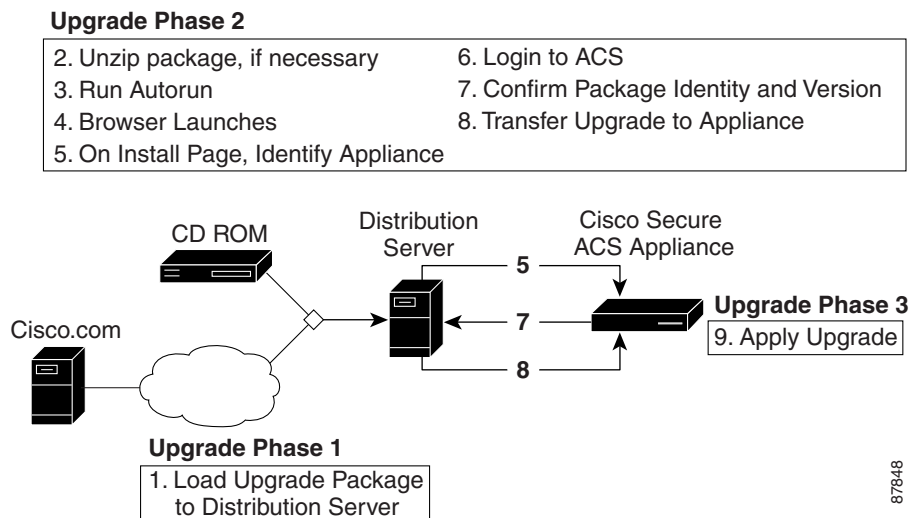
- [About Appliance Upgrades and Patches, page 8-29](#)
- [Distribution Server Requirements, page 8-30](#)
- [Upgrading an Appliance, page 8-31](#)

- [Transferring an Upgrade Package to an Appliance, page 8-33](#)
- [Applying an Upgrade, page 8-36](#)

About Appliance Upgrades and Patches

All upgrades and patches for Cisco Secure ACS Solution Engine are packaged using the upgrade mechanism. Upgrading or patching a Cisco Secure ACS Solution Engine is a three-phase process. See [Figure 8-1](#).

Figure 8-1 Appliance Upgrade Process



- **Phase One**—In the first phase, you obtain an upgrade package and load it onto a computer designated as a distribution server for Cisco Secure ACS Solution Engine upgrade distribution. The upgrade package may be obtained either as a CD ROM or as a file that you download from [Cisco.com](#).
- **Phase Two**—In the second phase you transfer installation package files from the distribution server to the appliance. File transfer is done by the HTTP server that is part of the installation package. The upgrade files are signed and the signature is verified after uploading to ensure that they have not been corrupted.

- **Phase Three**—The final phase of upgrading the appliance is to apply the upgrade. Before the upgrade files are applied to the appliance, Cisco Secure ACS verifies the digital signature on the files to ensure their authenticity and to verify that they are not corrupt.

**Tip**

While you apply the upgrade, Cisco Secure ACS cannot provide AAA services. If it is not critical to apply an upgrade package immediately, consider performing this phase when Cisco Secure ACS downtime will have the least impact.

Distribution Server Requirements

The distribution server must meet the following requirements:

- The distribution server must be able to run Sun Java Runtime Environment (JRE) 1.3.1. For system requirements of JRE 1.3.1, see <http://java.sun.com>. Upgrade package support for JRE 1.3.1 varies with the operating system of the distribution server, as follows:
 - If the distribution server uses Microsoft Windows, the distribution server need not have JRE 1.3.1 installed. The upgrade package includes JRE 1.3.1, which is used if the JRE is not found on the distribution server.

**Note**

Using the JRE in the upgrade package does not install the JRE on the distribution server.

- If the distribution server uses Solaris, the distribution server must have JRE 1.3.1 installed.
- For support, the distribution server must use an English-language version of one of the following operating systems:
 - Windows Server 2003, Enterprise Edition
 - Windows 2000 Server with Service Pack 3 installed
 - Windows XP Professional with Service Pack 1 installed
 - Solaris 2.8



Note While the upgrade process may succeed using a different operating system than those listed above, this list reflects the operating systems we used to test the upgrade process. We do not support upgrades from distribution servers that use untested operating systems.

- If you acquire the upgrade package on CD, the distribution server must have a CD ROM drive or be able to use the CD ROM drive on another computer that you can access.
- TCP port 8080 should not be in use on the distribution server. The upgrade process requires exclusive control of it.



Tip

We recommend that no other web server runs on the distribution server.

- A supported web browser should be available on the distribution server. If necessary, you can use a web browser on a different computer than the distribution server. For a list of supported browsers, see the Release Notes. The most recent revision to the Release Notes is posted on Cisco.com (<http://www.cisco.com>).

Gateway devices between the distribution server and any appliance that you want to upgrade must permit HTTP traffic to the distribution server on port 8080. They must also permit a Cisco Secure ACS remote administrative session; therefore, they must permit HTTP traffic to the appliance on port 2002 and the range of ports allowed for administrative sessions. For more information, see [HTTP Port Allocation for Administrative Sessions, page 1-22](#).


Upgrading an Appliance

Upgrading the software on Cisco Secure ACS Solution Engine

Before You Begin

Always back up Cisco Secure ACS Solution Engine before upgrading. For information about backing up Cisco Secure ACS, see [Cisco Secure ACS Backup, page 8-8](#).

To upgrade an appliance, follow these steps:

-
- Step 1** Acquire the upgrade package. Depending upon the type of upgrade package and any applicable service agreement for Cisco Secure ACS, the way to acquire an upgrade package differs.
- For commercial upgrade packages, contact your Cisco sales representative.
 - If you have a maintenance contract, you may be able to download upgrade packages from Cisco.com. Contact your Cisco sales representative.
 - For upgrade packages that apply patches for specific issues, work with your TAC representative to acquire the upgrade package.
- Step 2** Pick a computer to use as the distribution server. The distribution server must meet the requirements discussed in [Distribution Server Requirements, page 8-30](#).
- Step 3** If you have acquired the upgrade package in a compressed file format, such as a .zip or .gz file, follow these steps:
- a. If you have not already done so, copy the upgrade package file to a directory available from the distribution server.
 - b. Use the applicable file decompression utility to extract the upgrade package.
-  **Tip** Consider extracting the upgrade package in a new directory created for the contents of the upgrade package.
-
- Step 4** If you have acquired the upgrade package on CD, do not insert the CD in a CD ROM drive until instructed to do so. The CD contains autorun files, and if the distribution server uses Microsoft Windows, the CD ROM drive may automatically run the autorun files before you want.
- Step 5** Transfer the upgrade package to an appliance. For detailed steps, see [Transferring an Upgrade Package to an Appliance, page 8-33](#).
- The upgrade package is on the appliance and ready to be applied.
- Step 6** If Cisco Security Agent is running on the appliance, disable it. For detailed steps, see [Enabling or Disabling CSAgent, page 8-24](#).
- Step 7** Apply the upgrade package to the appliance. For detailed steps, see [Applying an Upgrade, page 8-36](#).
- Cisco Secure ACS applies the upgrade and runs using the upgraded software.

- Step 8** If you want Cisco Security Agent to protect the appliance, enable it. For detailed steps, see [Enabling or Disabling CSAgent, page 8-24](#).



Note The system restarts performed during the upgrade do not reenble CSAgent.

Transferring an Upgrade Package to an Appliance

Use this procedure to transfer an upgrade package from a distribution server to a Cisco Secure ACS Solution Engine.

After you have performed this procedure to upload the upgrade files, you must still apply the upgrade for it to become effective. For information on applying the upgrade, see [Applying an Upgrade, page 8-36](#). For more general information about the upgrade process, see [About Appliance Upgrades and Patches, page 8-29](#).

Before You Begin

You must have acquired the upgrade package and selected a distribution server. For more information, see [Upgrading an Appliance, page 8-31](#).

To transfer an upgrade to your Cisco Secure ACS appliance, follow these steps:

-
- Step 1** If the distribution server uses Microsoft Windows, follow these steps:
- a. If you have acquired the upgrade package on CD, insert the CD in a CD ROM drive on the distribution server.



Tip You can also use a shared CD drive on a different computer. If you do so and autorun is enabled on the shared CD drive, the HTTP server included in the upgrade package starts on the other computer.

- b. If either of the following conditions are true:
- You have acquired the upgrade package as a compressed file.
 - Autorun is not enabled on the CD ROM drive.

locate the `autorun.bat` file on the CD or in the directory that you extracted the compressed upgrade package in and run it.

The HTTP server starts. Messages from `autorun.bat` appear in a console window. Two web browser windows appear. The browser window titled Appliance Upgrade contains the Enter appliance hostname or IP address box. You can use the second browser window, titled New Desktop, to start transfers to other appliances.

Step 2 If the distribution server uses Sun Solaris, follow these steps:

- a. If you have acquired the upgrade package on CD, insert the CD in a CD ROM drive on the distribution server.
- b. Locate the `autorun.sh` file on the CD or in the directory that you extracted the compressed upgrade package in.
- c. Run `autorun.sh`.



Tip If `autorun.sh` has insufficient permissions to be run, enter `chmod +x autorun.sh` and repeat **c.**

The HTTP server starts. Messages from `autorun.sh` appear in a console window. Two web browser windows appear. The browser window titled Appliance Upgrade contains the Enter appliance hostname or IP address box. You can use the second browser window, titled New Desktop, to start transfers to other appliances.

Step 3 If, after you have run the applicable `autorun` file, no web browser opens, start a web browser on the distribution server and open the following URL:

```
http://127.0.0.1:8080/install/index.html
```



Tip You can access the HTTP server of the distribution server from a web browser on a different computer using the following URL: `http://IP address:8080/install/index.html`, where *IP address* is the IP address of the distribution server.

- Step 4** In the Appliance Upgrade browser window, type the appliance IP address or hostname in the **Enter appliance hostname or IP address** box, and click **Install**. The Cisco Secure ACS login page for the appliance specified appears.
- Step 5** Log in to the Cisco Secure ACS HTML interface. To do so, follow these steps:
- In the Username box, type a valid Cisco Secure ACS administrator name.
 - In the Password box, type the password for the administrator specified.
 - Click **Login**.
- Step 6** In the navigation bar, click **System Configuration**.
- Step 7** Click **Appliance Upgrade Status**.
Cisco Secure ACS displays the Appliance Upgrade page.
- Step 8** Click **Download**.
Cisco Secure ACS displays the Appliance Upgrade Form page. This page contains the Transfer Setup table, which enables you to identify the distribution server.
- Step 9** In the **Install Server** box, type the hostname or IP address of the distribution server and click **Connect**.
The Appliance Upgrade Form page displays the Software Install table, which details the version and name of the upgrade available from the distribution server.
- Step 10** Examine the table to confirm that the version, name, and condition of the upgrade is satisfactory, and click **Download Now**.
The Appliance Upgrade page appears and the upgrade file is downloaded from the distribution server to the appliance. Below the Appliance Versions table, Cisco Secure ACS displays the status of the download.



Tip On the Appliance Upgrade page, the system displays the message “Distribution Download in Progress”, followed by the number of kilobytes downloaded.

- Step 11** If you want to update the transfer status message, click **Refresh**.



Tip You can click **Refresh** as often as necessary to update the status message until the transfer completes.

If you click Refresh while the transfer is in progress, Cisco Secure ACS displays the number of kilobytes downloaded. If you click Refresh after the transfer is complete, the Apply Upgrade button appears and the transfer progress text is replaced with a message indicating that an upgrade package is available on the appliance.

- Step 12** To ensure that the upload was successful and the upgrade is ready to be applied, confirm that the following message appears on the Appliance Upgrade page: **Ready to Upgrade to** *version*, where *version* is the version of the upgrade package you have transferred to the appliance.

The upgrade package is successfully transferred to the appliance.

- Step 13** If you want to transfer the upgrade package to another appliance, access the browser window titled New Desktop, click **Install Next**, and return to Step 4.



Tip If you know the URL for the HTML interface of another appliance, you can type it in the browser location box and return to Step 5 to transfer the upgrade package to that appliance.

- Step 14** If are finished transferring upgrade packages to appliances, access the browser window titled New Desktop and click **Stop Distribution Server**.

The HTTP server stops and the resources it used on the distribution server are released.

- Step 15** If you want to apply the upgrade, perform the steps in [Applying an Upgrade, page 8-36](#). Alternatively, you can apply the **upgrade** command using the serial console. For more information about the **upgrade** command, see *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.
-

Applying an Upgrade

Perform this procedure to apply an upgrade package to a Cisco Secure ACS Solution Engine.



Note As an alternative to this procedure, you can apply the upgrade by using the **upgrade** command at the serial console for the Cisco Secure ACS Solution Engine. For more information, see *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.

Before You Begin

Before performing this procedure, you must have transferred the upgrade package to the appliance. For detailed steps, see [Transferring an Upgrade Package to an Appliance, page 8-33](#). For general steps required to upgrade an appliance, see [Upgrading an Appliance, page 8-31](#).

Always back up Cisco Secure ACS before upgrading. For information about backing up Cisco Secure ACS, see [Cisco Secure ACS Backup, page 8-8](#).

Be sure that the CSAgent service is disabled. Applying the upgrade will fail if CSAgent is running. For detailed steps, see [Enabling or Disabling CSAgent, page 8-24](#).

While you apply the upgrade, Cisco Secure ACS cannot provide AAA services. If it is not critical to apply an upgrade package immediately, consider performing this phase when Cisco Secure ACS downtime will have the least impact.

To apply an upgrade to a Cisco Secure ACS Solution Engine, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **Appliance Upgrade Status**.
Cisco Secure ACS displays the Appliance Upgrade page.
 - Step 3** Verify that the message “Ready to Upgrade to *version*” appears, where *version* is the version of the upgrade package available on the appliance.
 - Step 4** Click **Apply Upgrade**.
Cisco Secure ACS displays the Apply Upgrade Message table. This table displays messages about the upgrade process.
 - Step 5** For each message that Cisco Secure ACS displays, read the message carefully and click the applicable button.



Note You may receive a warning message that an upgrade package is not verified. Before applying an upgrade or patch, Cisco Secure ACS attempts to verify that the upgrade or patch is certified by Cisco. Some valid upgrade packages may not pass this verification, such as patches distributed for an urgent fix. Do not apply any upgrade package if you have unresolved concerns about the validity of the upgrade package.

After you have answered all confirmation prompts, Cisco Secure ACS applies the upgrade. Be aware of the following:

- While applying an upgrade, Cisco Secure ACS services are not available. This usually includes the HTML interface. After the upgrade is complete, the services and the HTML interface are available again.
- Applying an upgrade may take several minutes or more. A full upgrade of Cisco Secure ACS takes longer if the CiscoSecure user database has many user profiles.
- Upgrading Cisco Secure ACS usually requires the appliance to restart itself once or twice. Only smaller patches may not require restarts.
- While services restart or the appliance restarts, the HTML interface is not available. If this occurs, wait for the appliance to resume normal operation, and then close the original browser window, open a new browser window, and login to Cisco Secure ACS again.

**Caution**

Do not reset the appliance while an upgrade is being applied, unless directed to do so by TAC.

Step 6

After the upgrade is applied, go to the Appliance Upgrade page and verify that the versions of software on the appliance are as expected.



Note The HTML interface is unavailable while services restart and while the appliance restarts. When this occurs, the HTML interface is available again after the upgrade process is complete. Close the original browser window, open a new browser window, and log in to Cisco Secure ACS again.

The Appliance Versions table lists the versions of software running on the appliance. The table entries should reflect the upgrade package that you applied.

■ Appliance Upgrade Status