



# CHAPTER 7

## System Configuration: Basic

---

This chapter addresses the basic features in the System Configuration section of the web interface for the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

This chapter contains:

- [Service Control, page 7-1](#)
- [Logging, page 7-3](#)
- [Date and Time Format Control, page 7-3](#)
- [Local Password Management, page 7-4](#)
- [ACS Backup, page 7-8](#)
- [ACS System Restore, page 7-14](#)
- [ACS Active Service Management, page 7-18](#)
- [VoIP Accounting Configuration, page 7-21](#)
- [Support Page, page 7-25](#)
- [Appliance Upgrade Mechanism \(ACS SE Only\), page 7-27](#)

## Service Control

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



**Tip**

---

You can configure ACS service logs. For more information, see [Configuring Service Logs, page 10-29](#).

---

This section contains:

- [Determining the Status of ACS Services, page 7-2](#)
- [Stopping, Starting, or Restarting Services, page 7-2](#)
- [Setting Service Log File Parameters, page 7-2](#)

## Determining the Status of ACS Services

You can determine whether ACS services are running or stopped by accessing the Service Control page. To determine the status of ACS services:

---

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

**Step 2** Click **Service Control**.

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

---

## Stopping, Starting, or Restarting Services

You can stop, start, or restart ACS services as needed. The following procedure stops, starts, or restarts most ACS services.



**Tip**

You should use the web interface to control services, due to dependencies in the order in which ACS starts services. If you need to restart the **CSAdmin** service, you can use the Windows Control Panel (ACS for Windows) or the **stop** and **start** commands on the serial console (ACS SE).

---



**Note**

(ACS SE only) You cannot control the **CSAgent** service from the Service Control page. For information, see [Enabling or Disabling CSAgent, page 7-22](#).

---

To stop, start, or restart most ACS services:

---

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

**Step 2** Click **Service Control**.

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

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

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

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

The status of ACS services changes to the state according to which button that you clicked.

---

## Setting Service Log File Parameters

To configure the parameters for the service log file and directory management, use this page. For detailed option descriptions, see [Configuring Service Logs, page 10-29](#).

---

**Step 1** Complete the following:

Field	From the List, Select:
Level of detail	The level of detail.
Generate new file	The schedule to generate log files.
Manage directory	How long to keep log files.

**Step 2** Click **Restart**.

ACS restarts its services and implements the service log settings that you specified.



**Note** Ensure that you have enough disk space in which to store your log files. Consult the logs if any problems occur.

## Logging

You can configure ACS to generate logs for administrative and accounting events, depending on the protocols and options that you enable. Log files are stored in the *drive:\install\_dir\service\_name\Logs* directory. For example, in *C:\CiscoSecureACS\CSAuth\Logs*. For details on service logs and gathering information for troubleshooting, see [Service Logs, page 10-12](#).

## Date and Time Format Control

ACS supports two possible date formats in its logs, reports, and administrative interface. You can choose a month/day/year format or a day/month/year format.

When ACS sends a log to the syslog server, the syslog server displays and records the time. ACS supports two possible time formats in its logs, reports, and administrative interface. You can choose the local time zone or the GMT display.

## Setting the Date and Time Formats



**Note** If you have reports that were generated before you changed the date format, you must move or rename them to avoid conflicts. For example, if you are using the month/day/year format, ACS assigns the name *2007-07-12.csv* to a report that was generated on July 12, 2007. If you subsequently change to the day/month/year format, on December 7, 2001, ACS creates a file also named *2007-07-12.csv* and overwrites the existing file.

To set the date and time formats:

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

**Step 2** Click **Date Format Control**.

ACS displays the Date Format Control page.

- Step 3** Chose a date format.
- Step 4** Chose a time zone for the syslog server display.
- Step 5** Click **Submit & Restart**.

ACS restarts its services and implements the date and time format that you chose.



**Note** For the new date or time format to be visible in the web interface reports, you must restart the connection to the ACS. Click the **X** in the upper-right corner of the browser window to close it.

## Local Password Management

Use the Local Password Management page to configure settings that manage user passwords that were in the ACS internal database.



**Note**

ACS stores user accounts, username, and password authentication information separately from ACS administrator account information. ACS stores accounts that were created for authentication of network service requests and ACS administrative access in separate internal databases. For information on administrator accounts, see [Chapter 11, “Administrators and Administrative Policy.”](#)

The Local Password Management page contains these sections:

- **Password Validation Options**—You use these settings to configure validation parameters for user passwords. ACS enforces these rules when an administrator changes a user password in the ACS internal database and when a user attempts to change passwords by using the Authentication Agent applet.



**Note**

Password validation options apply only to user passwords that are stored in the ACS internal database. They do not apply to passwords in user records in external user databases; nor do they apply to enable or **admin** passwords for Cisco IOS network devices.

The password validation options are:

- **Password length between X and Y characters**—Enforces that password lengths adhere to the values specified in the X and Y boxes, inclusive. ACS supports passwords up to 32 characters long.
- **Password may not contain the username**—Requires that a user password does not contain the username.
- **Password is different from the previous value**—Requires that a new user password to be different from the previous password.
- **Password must be alphanumeric**—Requires that a user password contain letters and numbers.
- **Remote Change Password**—You use these settings to configure whether a TELNET password change is enabled and, if so, whether ACS immediately sends the updated user data to its replication partners.

The remote change password options are:

- **Disable TELNET Change Password against this ACS and return the following message to the users TELNET session**—ACS supports password change from a device that uses TACACS+. Check to disable the password change. When checked, this option disables the ability to perform password changes during a TELNET session that a TACACS+ AAA client hosts. Users who submit a password change receive the text message that you enter in the corresponding box. For more information, see [Changing a User Password from a Device Using TACACS+, page 7-5](#).
- **Upon remote user password change, immediately propagate the change to selected replication partners**—This setting determines whether ACS sends its replication partners any passwords that are changed during a TELNET session, that is hosted by a TACACS+ AAA client, the Authentication Agent, or the User-Changeable Passwords web interface. The ACSs that were configured as the replication partners of this ACS appear below this check box.

This feature depends on the Database Replication feature being configured properly; however, replication scheduling does not apply to propagation of changed password information. ACS sends changed password information immediately, regardless of replication scheduling.

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

For more information about Database Replication, see [ACS Internal Database Replication, page 8-1](#).

The log file management options for the User Password Changes Log are:

- **Generate New File**—You can specify the frequency at which ACS creates a *User Password Changes Log* file: daily, weekly, monthly; or, after the log reaches a size in kilobytes that you specify.
- **Manage Directory**—You can specify whether ACS controls the retention of log files. You can use this feature to specify the maximum number of files to retain or the maximum age of files to retain. If the maximum number of files is exceeded, ACS deletes the oldest log file. If the maximum age of a file is exceeded, ACS deletes the file.

## Changing a User Password from a Device Using TACACS+

You can configure ACS to control whether network administrators can change passwords during TELNET sessions that are hosted by TACACS+ AAA clients. Some Cisco devices support a TACACS+ facility for users to change their passwords when connecting for an administration session. The changes made by the user are communicated to ACS over TACACS+ using a routine known as **chpass**.

On an ACS on which **chpass** is enabled (**chpass** should be enabled on a top-level replication master for the installation) the **chpass** sequence is as follows:

Enable **chpass** on a top-level replication master for the installation. On an ACS on which you enable **chpass**, the sequence is described here.

To enable **chpass** from a device:

- 
- Step 1** When prompted for your password, press **Return**.
  - Step 2** When prompted for your current password, enter you current password and then press **Return**.

**Step 3** When prompted for a new password, enter the new password and then press **Return**.

---

When a user tries to change a password on a ACS on which **chpass** is enabled, ACS performs an immediate and automatic propagation of the event to its replication slave partners (all those configured in its GUI as replication slave partners). This process mitigates any possible change propagation issues that may have relied on a timed replication propagation.

You can also use **chpass** after a password was intentionally changed due to password aging. ACS initiates **chpass** so that you can reset or change your password in the ACS internal database.

The password aging feature in ACS requires you to change your password. When a password expires, the administrator must intentionally reset the user password. You will then only be able to log in to the AAA client via TELNET using the password that the administrator assigned, namely the reset password. When **chpass** is initiated, you will be asked to change your password according to the method described in this section.

An alternative method for allowing users to change their passwords is to use the Web-based User Changeable Password (UCP) utility supplied with ACS. For more information see the *Installation and User Guide for Cisco Secure ACS User-Changeable Passwords*.

An ACS receiving TACACS+ authentication traffic from a particular device, may not have yet received the password change update and so may still be operating with the older password. This is a well-known problem with many distributed password control systems. You can disable ACS **chpass** from its TACACS+ clients. When a user on a TACACS+ client device attempts the **chpass** procedure against ACS, on which support for **chpass** is disabled, ACS sends a configurable message back to the device, and to the user, explaining that the **chpass** functionality is not supported on this device. This configurable message can be used to direct device administrators to perform a TELNET to a device that uses a TACACS+ server that allows **chpass**.

## Configuring Local Password Management

To configure password validation options for user account passwords:

---

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

**Step 2** Click **Local Password Management**.

The Local Password Management page appears.

**Step 3** Under Password Validation Options:

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

- Step 4** Under Remote Change Password:
- If you want to enable user password changes in TELNET sessions, uncheck the **Disable TELNET Change Password against this ACS and return the following message to the users TELNET session** check box.
  - If you want to disable user password changes in TELNET sessions, check the **Disable TELNET Change Password against this ACS and return the following message to the users TELNET session** check box.
  - In the box below the **Disable TELNET Change Password against this ACS and return the following message to the users TELNET session** check box, enter a message that users should see when attempting to change a password in a TELNET session and when the TELNET password change feature has been disabled (Step b).
  - If you want ACS to send changed password information immediately after a user has changed a password, check the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.



**Tip** The ACSs that receive the changed password information appear below the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.

- Step 5** Click **Submit**.  
ACS restarts its services and implements the settings that you specified.

## Configuring Intervals for Generating a New Password (ACS for Windows Only)

If you want ACS to generate a User Password Changes log file at a regular interval:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Logging**.  
The Logging Configuration page appears.
- Step 3** In the User Password Changes CSV column, click **Configure**.  
The CSV User Password Changes File Configuration appears.
- Step 4** In the Log File Management section, chose one of the following:
- Every day**—ACS generates a new User Password Changes log file at the start of each day.
  - Every week**—ACS generates a new User Password Changes log file at the start of each week.
  - Every month**—ACS generates a new User Password Changes log file at the start of each month.
- Step 5** If you want ACS to generate a new *User Password Changes* log file when the current file reaches a specific size, select the **When size is greater than X KB** option and type the file size threshold, in kilobytes, in the *X* box.
- Step 6** If you want to manage which *User Password Changes* log files that ACS keeps:
- Check the **Manage Directory** check box.
  - If you want to limit the number of User Password Changes log files that ACS retains, select the **Keep only the last X files** option and type the number of files that you want ACS to retain in the *X* box.

- c. If you want to limit the age of User Password Changes log files that ACS retains, select the **Delete files older than X days** option and type the number of days for which ACS should retain a User Password Changes log file before deleting it.

**Step 7** Click **Submit**.

ACS restarts its services and implements the settings that you specified.

---

## ACS Backup

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



**Caution**

---

As with previous versions of ACS, you cannot perform replication between different versions of ACS.

---

This section contains:

- [About ACS Backup, page 7-8](#)
- [Backup File Locations \(ACS for Windows Only\), page 7-9](#)
- [Directory Management \(ACS for Windows Only\), page 7-9](#)
- [Components Backed Up, page 7-9](#)
- [Reports of ACS Backups, page 7-10](#)
- [Backup Options, page 7-10](#)
- [Performing a Manual ACS Backup, page 7-11](#)
- [Scheduling ACS Backups, page 7-12](#)
- [Disabling Scheduled ACS Backups, page 7-14](#)

## About ACS Backup

Maintaining backup files can minimize downtime if system information becomes corrupt or is misconfigured. You can manually back up the ACS system. You can also establish automated backups that occur at regular intervals, or at selected days of the week and times.

### ACS for Windows

The ACS Backup feature provides the option to back up your user and group databases, and your ACS system configuration information to a file on the local hard drive. We recommend that you copy the files to the hard drive on another computer in case the hardware fails on the primary system.

### ACS SE

The ACS Backup feature backs up ACS system information to a file that ACS sends to an FTP server that you specify. We recommend that you copy the files from the FTP server to another computer in case the hardware fails on the FTP server.

**Note**

ACS determines the filename given to a backup. For more information about filenames that are assigned to backup files generated by ACS, see [Filenames and Locations, page 7-15](#).

**Both Platforms**

For information about using a backup file to restore ACS, see [ACS System Restore, page 7-14](#).

**Note**

We do not support backup and restore features between different versions of ACS.

## Backup File Locations (ACS for Windows Only)

The default directory for backup files is:

*drive*: \path\CSAuth\System Backups

where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory. For example, if you installed ACS version 4.2 in the default location, the default backup location would be:

```
c:\Program Files\CiscoSecure ACS v4.2\CSAuth\System Backups
```

ACS determines the filename that is assigned to a backup. For more information about filenames that ACS assigns to backup files, see [Filenames and Locations, page 7-15](#).

## Directory Management (ACS for Windows Only)

You can configure the number of backup files to keep and the number of days after which backup files are deleted. The more complex your configuration and the more often you back up the system, the more diligent you should be about clearing out old databases from the ACS hard drive.

## Components Backed Up

The ACS System Backup feature backs up the ACS user database that is relevant to ACS. The user database backup includes all user information, such as username, password, and other authentication information, including server certificates and the certificate trust list.

If your ACS for Windows logs information to a remote ACS server, both ACS versions must have identical release, build, and patch numbers; or the logging might fail.

**Caution**

As with previous versions of ACS, you must not perform replication between different versions of ACS.

**Note**

The cert7.db file is not backed up. If you use this certificate file with an LDAP database, we recommend that you back it up on a remote machine for disaster recovery.

## Reports of ACS Backups

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

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

## Backup Options

The ACS System Backup Setup page contains:

- **Manually**—ACS does not perform automatic backups. When this option is selected, you can only perform a backup by following the steps in [Performing a Manual ACS Backup, page 7-11](#).
- **Every X minutes**—ACS performs automatic backups on a set frequency. The unit of measurement is minutes, with a default backup frequency of 60 minutes.
- **At specific times**—ACS performs automatic backups at the time that is specified in the day-and-hour graph. The minimum interval is one hour, and the backup occurs on the hour that you selected.

### ACS for Windows

- **Directory**—The directory to which ACS writes the backup file. You must specify the directory by its full path on the Windows server that runs ACS, such as `c:\acs-bups`.
- **Manage Directory**—Defines whether ACS deletes older backup files. Using the following options, you can specify how ACS determines which log files to delete:
  - **Keep only the last X files**—ACS retains the most recent backup files, up to the number of files that you specified. When the number of files that you specified is exceeded, ACS deletes the oldest files.
  - **Delete files older than X days**—ACS deletes backup files that are older than the number of days that you specified. When a backup file grows older than the number of days that you specified, ACS deletes it.
- **Add Hostname**—Backup file names can include the ACS server host name. Click **Add Hostname** to add the hostname to backup file names. Adding a hostname provides a way to identify which backup file corresponds to which ACS server in distributed deployments with multiple ACS servers.

### ACS SE

- **FTP Server**—The IP address or hostname of the FTP server to which you want to send the backup files. If you specify a hostname, you must enable DNS on your network.
- **Login**—A valid username that enables ACS to access the FTP server.
- **Password**—The password for the username provided in the Login box.
- **Directory**—The directory to which ACS writes the backup file. You must specify the directory relative to the FTP root directory. To specify the FTP root directory, enter a single period (.).
- **Encrypt Backup File**—Determines whether ACS encrypts the backup file.
- **Encryption Password**—The password used to encrypt the backup file. If the you click the Encrypt backup file option, you must provide a password.

**Note**

If you use an encrypted backup file to restore ACS data, you must provide the exact password that you entered in the Encryption Password box when you created the backup.

## Performing a Manual ACS Backup

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

To perform an immediate backup of ACS:

### ACS for Windows

---

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Backup**.  
The ACS System Backup Setup page appears.
- Step 3** In the **Directory** box under Backup Location, enter the drive and path to the directory on a local hard drive to which you want to write the backup file.
- Step 4** Click **Backup Now**.  
ACS immediately begins a backup.
- 

### ACS SE

---

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Backup**.  
The ACS System Backup Setup page appears. At the top of the page, information about the last backup appears, including:
- Whether the last backup succeeded.
  - The IP address of the FTP server used for the backup.
  - The directory used to store the backup.
  - The filename of the backup file that was created.
- Step 3** In the **FTP Server** box under FTP Setup, enter the IP address or hostname of the FTP server to which you want ACS to send the backup file.
- Step 4** In the **Login** box under FTP Setup, enter a valid username to enable ACS to access the FTP server.
- Step 5** In the **Password** box under FTP Setup, enter the password for the username that you provided in the Login box.
- Step 6** In the **Directory** box under FTP Setup, enter the relative path to the directory on the FTP server to which you want to send the backup file.
- Step 7** If you want to encrypt the backup file:
- a. Check the **Encrypt backup file** check box.
  - b. In the **Encryption Password** box, enter the password that you want to use for encryption of the backup file.

**Note**

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

**Step 8** Click **Backup Now**.

ACS immediately begins a backup.

**Note**

ACS determines the backup filename. For more information about filenames assigned to backup files generated by ACS, see [Filenames and Locations](#), page 7-15.

## Scheduling ACS Backups

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

To schedule the times at which ACS performs a backup:

### ACS for Windows

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

The ACS System Backup Setup page appears.

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

Because ACS is momentarily shut down during backup, if the backup interval is too frequent (that is, the setting is too low), users might be unable to authenticate.

**Step 4** To schedule backups at specific times:

- a. Under ACS Backup Scheduling, select the **At specific times** option.
- b. In the day-and-hour graph, click the times at which you want ACS to perform a backup.

**Tip**

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

**Step 5** To change the location where ACS writes backup files, type the drive letter and path in the **Directory** box.**Step 6** To manage which backup files ACS keeps:

- a. Check the **Manage Directory** check box.
- b. To limit the number of backup files that ACS retains, select the **Keep only the last X files** option and type in the *X* box the number of files that you want ACS to retain.

- c. To limit the age of backup files that ACS retains, select the **Delete files older than X days** option and type the number of days for which ACS should retain a backup file before deleting it.

**Step 7** Click **Submit**.

ACS implements the backup schedule that you configured.

---

## ACS SE

---

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

**Step 2** Click **ACS Backup**.

The ACS System Backup Setup page appears.

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



**Note** Because ACS is momentarily shut down during backup, if the backup interval is too frequent (that is, the setting is too low), users might be unable to authenticate.

---

**Step 4** To schedule backups at specific times:

- a. Under ACS Backup Scheduling, click the **At specific times** option.
- b. In the day-and-hour graph, click the times at which you want ACS to perform a backup.



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

---

**Step 5** In the **FTP** box under FTP Setup, enter the IP address or hostname of the FTP server to which you want ACS to send the backup file.

**Step 6** In the **Login** box under FTP Setup, enter a valid username to enable ACS to access the FTP server.

**Step 7** In the **Password** box under FTP Setup, enter the password for the username that you provided in the Login box.

**Step 8** In the **Directory** box under FTP Setup, enter the relative path to the directory on the FTP server to which you want to write the backup file.

**Step 9** If you want to encrypt the backup file:

- a. Check the **Encrypt backup file** check box.
- b. In the **Encryption Password** box, enter the password that you want to use to encrypt the backup file.



**Note** If you use an encrypted backup file to restore ACS data, you must provide the exact password that you entered in the Encryption Password box when the backup was created.

---

**Step 10** Click **Submit**.

ACS implements the backup schedule that you configured.

---

## Disabling Scheduled ACS Backups

You can disable scheduled ACS backups without losing the schedule itself. You can use this method to end scheduled backups and resume them later without having to recreate the schedule.

To disable a scheduled backup:

- 
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Backup**.
- The ACS System Backup Setup page appears.
- Step 3** Under ACS Backup Scheduling, select the **Manual** option.
- Step 4** Click **Submit**.
- ACS does not continue any scheduled backups. You can still perform manual backups as needed.
- 

## ACS System Restore

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



### Caution

As with previous versions of ACS, you must not perform replication between different versions of ACS.

---

This section contains:

- [About ACS System Restore, page 7-14](#)
- [Filenames and Locations, page 7-15](#)
- [Components Restored, page 7-16](#)
- [Reports of ACS Restorations, page 7-16](#)
- [Restoring ACS from a Backup File, page 7-16](#)

## About ACS System Restore

You use the ACS System Restore feature to restore your user and group databases, and your ACS system configuration information from backup files that the ACS Backup feature generates. This feature helps you to minimize downtime if ACS system information becomes corrupted or is misconfigured.

The ACS System Restore feature only works with backup files that ACS generates when running an identical ACS version and patch level.

If you restore onto a physically different server, it must have the same IP address as the original server; otherwise, replication will not work correctly because the network configuration has a hidden record that contains details of the ACS server.

## Filenames and Locations

The ACS System Restore feature restores the ACS user database and other ACS configuration data from a backup file and location that was created by the ACS Backup feature. You can restore your system from the latest backup file; or, if you suspect that the latest backup was incorrect, you can restore from an earlier backup file.

### ACS for Windows

The ACS System Restore feature restores the ACS user database and ACS Windows Registry information. ACS writes the backup files to the local hard drive. When you schedule backups or perform a manual backup, you select the backup directory. The default directory for backup files is:

```
drive: \path\CSAuth\System Backups
```

where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory. For example, if you installed ACS version 4.2 in the default location, the default backup location would be:

```
c:\Program Files\CiscoSecure ACS v4.2\CSAuth\System Backups
```

### ACS SE

The ACS System Restore feature restores the ACS user database and other ACS configuration data from a backup file and location that the ACS Backup feature created. ACS sends backup files to an FTP server that you specify on the ACS System Backup Setup page. On the FTP server, backup files are written to the directory that you specify when you schedule backups or perform a manual backup. The FTP server uses the following locations. For:

- Windows FTP servers, `FTPROOT dir/user_specified_dir`
- Unix FTP servers, the FTP user home directory is `FTPROOT` by default

### Both Platforms

ACS creates backup files by using the date and time format:

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

where:

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

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

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

### ACS for Windows

If you are uncertain of the location of the latest backup file, check your scheduled backup configuration on the ACS Backup page.

**ACS SE**

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

*13-Oct-2005 11-41-35e.dmp*

If you are uncertain which FTP server and directory was used to create the latest backup file, check the ACS System Restore Setup page. Information about the most recent backup and restore, if any, appears at the top of the page.

## Components Restored

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

## Reports of ACS Restorations

When an ACS system restoration occurs, the event is logged in the Administration Audit report, and the ACS Backup and Restore report. You can view recent reports in the Reports and Activity section of ACS.

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

## Restoring ACS from a Backup File

You can perform a system restoration of ACS whenever needed.

**Note**


---

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

---

To restore ACS from a backup file that the ACS Backup feature generated:

### ACS for Windows

---

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Restore**.  
The **ACS System Restore Setup** page appears.  
The **Directory** box displays the drive and path to the backup directory that is most recently configured in the **Directory** box on the ACS Backup page.  
Beneath the **Directory** box, ACS displays the backup files in the current backup directory. If no backup files exist, <No Matching Files> appears in place of filenames.
- Step 3** To change the backup directory, type the new drive and path to the backup directory in the **Directory** box, and then click **OK**.  
ACS displays the backup files, if any, in the backup directory that you specified.
- Step 4** In the list below the **Directory** box, select the backup file that you want to use to restore ACS.
- Step 5** To restore user and group database information, check the **User and Group Database** check box.
- Step 6** To restore system configuration information, check the **Cisco Secure ACS System Configuration** check box.

- Step 7** To upgrade to ACS 4.2 using the ACS 4.1 backup file check the **Restore from 4.1 backup file to ACS 4.2** check box. You use this option to upgrade to ACS 4.2 using the ACS 4.1 backup file. The upgrade functionality is then implemented, and the user and group databases and the system configuration will be restored.
- Step 8** Click **Restore Now**.
- ACS displays a confirmation dialog box indicating that performing the restoration will restart ACS services and log out all administrators.
- Step 9** To continue with the restoration, click **OK**.
- ACS restores the system components that you specified by using the backup file that you selected. The restoration should require several minutes to finish, depending on the components that you selected to restore and the size of your database.
- When the restoration is complete, you can log in to ACS again.
- 

## ACS SE

---

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Restore**.
- The **ACS System Restore Setup** page appears.
- With the exception of the Decryption Password box, the boxes under Select Backup To Restore From contain the values that were used for the most recent successful backup, as configured on the ACS System Backup Setup page.
- Step 3** If you want to accept the default values for the FTP Server, Login, Password, Directory, and File boxes, proceed to step 5.
- Step 4** If you want to change any of the values in the FTP Server, Login, Password, Directory, and File boxes:
- In the **FTP Server** box under FTP Setup, enter the IP address or hostname of the FTP server from which you want ACS to get the backup file.
  - In the **Login** box under FTP Setup, enter a valid username to enable ACS to access the FTP server.
  - In the **Password** box under FTP Setup, enter the password for the username that you provided in the Login box.
  - In the **Directory** box under FTP Setup, enter the relative path to the directory on the FTP server that contains the backup file.
  - Click **Browse**.
- After a pause to retrieve a file list from the FTP server, a dialog box lists the ACS backup files found in the specified directory. Encrypted backup files include the lowercase letter *e* before the *.dmp* filename extension (*<filename>e.dmp*).



**Tip** If no files are found or the FTP server could not be accessed, click **Cancel** to close the dialog box, and repeat Step 4.

---

- Click the filename of the backup file that you want to use to restore ACS.
- The filename that you select appears in the File box, and the dialog box closes.

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



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

**Step 6** To restore user and group database information, check the **User and Group Database** check box.

**Step 7** To restore system configuration information, check the **ACS System Configuration** check box.

**Step 8** To upgrade to ACS 4.2 using the ACS 4.1 backup file check the **Restore from 4.1 backup file to ACS 4.2**.

**Step 9** Click **Restore Now**.

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

**Step 10** To continue with the restoration, click **OK**.

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

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

## ACS Active Service Management

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

This section contains:

- [System Monitoring, page 7-18](#)
- [Event Logging, page 7-20](#)

## System Monitoring

You use ACS system monitoring to determine how often ACS tests its authentication and accounting processes, and to determine what automated actions to take if the tests detect a failure of these processes. ACS performs system monitoring with the CSMon service. For more information about the CSMon service, see [CSMon, page F-10](#).

## System Monitoring Options

The options for configuring system monitoring are:

- **Test login process every X minutes**—Controls whether ACS tests its login process. The value in the X box defines, in minutes, how often ACS tests its login process. The default frequency is once per minute, which is also the most frequent testing interval possible.

When you enable this option, at the interval defined, ACS tests authentication and accounting. If the test fails, after four unsuccessful retries ACS performs the action identified in the **If no successful authentications are recorded** list and logs the event.



**Note** You can also create scripts in the *CSMon\Scripts* folder to run in case the test login fails.

- **If no successful authentications are recorded**—Specifies what action ACS takes if it detects that its test login process failed. This list contains several built-in actions and actions that you define. The items beginning with asterisks (\*) are predefined actions:
  - **\*Restart All**—Restart all ACS services.
  - **\*Restart RADIUS/TACACS+**—Restart only the Proxy Remote Access Dial-In User Service (RADIUS) and TACACS+ services.
  - **\*Reboot**—Reboot ACS.
  - **Custom actions** (ACS for Windows)—You can define other actions for ACS to take if failure of the login process occurs. ACS can execute a batch file or executable on the failure of the login process. To make a batch or executable file available in the on failure list, place the file in:

*drive:\path\CSMon\Scripts*

where *drive* is the local drive where you installed ACS and *path* is the path from the root of *drive* to the ACS directory.



**Tip** Restart CSAdmin to see the new batch file or executable in the list.

- **Take No Action** (both platforms)—Leave ACS operating as is.
- **Generate event when an attempt is made to log in to a disabled account**—Specifies whether ACS generates a log entry when a user attempts to log in to your network by using a disabled account.



**Note** You can also create scripts in the *CSMon\Scripts* folder to run in case the test login fails.

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

## Setting Up System Monitoring

To set up ACS System Monitoring:

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

**Step 2** Click **ACS Service Management**.

The ACS Active Service Management Setup page appears.

- Step 3** To have ACS test the login process:
- Check the **Test login process every X minutes** check box.
  - Use the **X** box to enter the interval (up to 3 characters) between each login process test.
  - From the **If no successful authentications are recorded** list, select the action that ACS should take when the login test fails five successive times.
- Step 4** To generate a Windows event when a user tries to log in to your network by using a disabled account, check the **Generate event when an attempt is made to log in to a disabled account** check box.
- Step 5** If you want to set up event logging, see [Setting Up Event Logging, page 7-20](#).
- Step 6** If you are finished setting up ACS Service Management, click **Submit**.  
ACS implements the service-management settings that you made.
- 

## Event Logging

You use the Event Logging feature to configure whether ACS logs events to the Windows event log and ACS generates an e-mail when an event occurs. ACS uses the System Monitoring feature to detect the events to be logged. For more information about system monitoring, see [System Monitoring Options, page 7-18](#).

## Setting Up Event Logging

To set up ACS event logging:

- 
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Service Management**.  
The ACS Active Service Management Setup page appears.
- Step 3** (ACS for Windows only) To have ACS send all events to the Windows event log, select **Log all events to the Windows Event log**.



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

---

- Step 4** (Both platforms) To have ACS send an e-mail when an event occurs:
- Check the **Email notification of event** check box.
  - In the **To** box, enter the e-mail address (up to 200 characters) to which ACS should send event notification e-mail.



**Note** Do not use underscores (\_) in the e-mail addresses that you enter in this box.

---

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



---

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

---

- Step 5** If you want to set up system monitoring, see [Setting Up System Monitoring, page 7-19](#).
- Step 6** If you are finished setting up ACS Service Management, click **Submit**.  
ACS implements the service-management settings that you made.
- 

## VoIP Accounting Configuration

You use the voice over IP (VoIP) Accounting Configuration feature to specify which accounting logs receive VoIP accounting data. The options for VoIP accounting are:

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

## Configuring VoIP Accounting



---

**Note** If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check the **Voice-over-IP (VoIP) Accounting Configuration** check box. See [Chapter 2, “Advanced Options \(for Interface Configuration\)”](#) for more information.

---

To configure VoIP accounting:

- 
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **VoIP Accounting Configuration**.  
The VoIP Accounting Configuration page appears. The Voice-over-IP (VoIP) Accounting Configuration table displays the options for VoIP accounting.
- Step 3** Select the VoIP accounting option that you want.
- Step 4** Click **Submit**.  
ACS implements the VoIP accounting configuration that you specified.
-

# Appliance Configuration (ACS SE Only)

You use the Appliance Configuration page to set the ACS hostname, domain names, system date, and time. If you are using an appliance base image that incorporates the CSA or have applied a CSA update to ACS, you can use the Appliance Configuration page to enable and disable the **CSAgent** service.

This section contains:

- [Enabling or Disabling CSAgent, page 7-22](#)
- [Configuring SNMP Support, page 7-23](#)
- [Configuring SNMP Support, page 7-23](#)
- [Setting System Time and Date, page 7-23](#)
- [Setting the ACS Host and Domain Names, page 7-24](#)
- [Enabling or Disabling CSAgent, page 7-22](#)

## Enabling or Disabling CSAgent



### Note

The CSA section appears only if you are using appliance base image 3.3.1.3 or later or if you have applied the CSA update to the appliance.

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

- Upgrading or applying patches to ACS.
- Allowing the appliance to respond to ping requests.



### Note

When **CSAgent** is disabled, the CSA no longer protects the appliance. For information on CSA protection, see [Cisco Security Agent Policies, page 1-18](#).

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

To enable or disable **CSAgent** on the appliance:

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

**Step 2** Click **Appliance Configuration**.

ACS displays the Appliance Configuration page.



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

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

**Step 4** Click **Submit**.


ACS enables or disables **CSAgent**.

## Configuring SNMP Support

You use the SNMP support in ACS SE to monitor information for the appliance, such as, processes, memory, CPU utilization, version of the appliance and ACS software version, ethernet interface status, and so on.

To configure the SNMP Agent, choose **System Configuration > Appliance Configuration** from the navigation bar.

To configure SNMP Agent settings:

- 
- Step 1** Check the **SNMP Agent Enabled** check box. The default is enabled.
- Step 2** In the **SNMP Communities** box, enter the community strings for SNMP. With the exception of the comma(,), all characters are valid. You must use a comma (,) separator between community strings.
-  **Note** An SNMP client cannot retrieve information from ACS SE if the SNMP Communities field is empty.
- 
- Step 3** In the **SNMP Port** box, enter the connectivity port number.
- Step 4** In the **Contact** box, enter the name of the network administrator.
- Step 5** In the **Location** box, enter the location of the device.
- Step 6** Check the **Accept SNMP packets from select hosts** check box if you want to restrict the requests that the SNMP agent accepts to a list of specific SNMP client host addresses.
- Step 7** In the **Host Addresses** box, enter the specific SNMP client host addresses. You must use a comma (,) delimiter between host addresses.
- 

## Setting System Time and Date

Use this procedure to set the system time and date from the web interface. In addition, you can use this procedure to maintain the system time and date by using a network time protocol (NTP) server that the system can use to automatically synchronize time and date.



### Tip

You can also use the serial console to perform this procedure. For details, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

To set the system date and time:

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



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

- Step 3** From the **Time Zone** list, select the system time zone.

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



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

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


## Setting the ACS Host and Domain Names

Use this procedure to configure ACS host and domain names.



**Note** This procedure requires that you reboot the ACS. You should perform this procedure during off hours to minimize disruption of users.

To set the ACS host and domain names:

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Appliance Configuration**.
- ACS displays the Appliance Configuration page.
-  **Note** If the system does not display the Appliance Configuration page, check connectivity to ACS.
- Step 3** In the **Host Name** box, enter the hostname.
- Step 4** In the **Domain Name** box, enter the domain name.
- Step 5** At the bottom of the page, click **Submit** and then click **Reboot**.

# Support Page

You use the Support page for two purposes:

- To package system state information into a file that can be forwarded to the Cisco Technical Assistance Center.
- To monitor the state of ACS services.

Each of these activities is detailed in the following sections:

- [Running Support, page 7-25](#)
- [Monitoring System Information, page 7-26](#)

This section contains:

- [Running Support, page 7-25](#)
- [Monitoring System Information, page 7-26](#)

## Running Support

You can use the Support page to package system information for forwarding to your Technical Assistance Center (TAC) representative. When you perform this procedure, ACS automatically packages all current logs.

You also have the options to package:

- The user database.
- System logs for the number of preceding days that you specify.
- Diagnostic logs

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



---

**Note** AAA services are briefly suspended when you run the **Support** procedure. We recommend that you perform this procedure during periods of least AAA activity to minimize user impact.

---

To package system state information into a file for the Cisco Technical Assistance Center:

- 
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Support**.
- The Support page appears.
- Step 3** If you want to download diagnostic log information, check the **Collect Log Files** check box. If you select this option, ACS services are not restarted during the generation of package.cab. See [Viewing or Downloading Diagnostic Logs \(ACS SE Only\), page 7-27](#) for more information about diagnostic log information for the appliance only.
- Step 4** If you want to include the ACS internal database in the support file, check the **Collect User Database** check box in the **Details to collect** table.
- Step 5** If you want to include archived system logs:
- a. Check the **Collect Previous X Days logs** check box.




---

**Note** If you want the support information to be downloaded to include service log files that are older than the current log files, check the **Collect Previous X Days logs** check box and type the number of days of log files to be included. For example, if you want an archived copy of the *Backup and Restore.csv* log to be included, type the number of days prior to today that you want ACS to look for *Backup and Restore.csv* files. The current log file may not be today's date. It is the current one, which may be several days older than today's date.

---

- b. In the *X* box, enter the number of preceding days for which you want logs collected. The maximum number of preceding days is 9999.

**Step 6** Click **Run Support Now**.

The File Download dialog box appears.

**Step 7** On the **File Download** dialog box, click **Save**.

The Save As dialog box appears.

**Step 8** Use the **Save As** dialog box to specify the path and filename for the cabinet file. Then click **Save**.

ACS briefly suspends normal services while a support file is generated and saved. When the download is complete, a ACS displays the Download Complete dialog box.

**Step 9** You should make note of the name and location of the support file, and then click **Close**.

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

---

## Monitoring System Information

You use this procedure to monitor the status and distribution of ACS resources. The top row in the Resource Usage table displays CPU idle resource percentage and available memory space. The remainder of the Resource Usage table shows the following allocations for each service:

- **CPU**—The percentage of CPU cycles being used. In the System category, ACS numbers the CPUs, starting with zero (0). If there is more than one CPU, the System category displays CPU information for each CPU.
- **Memory**—The amount of memory allocated by each service.
- **Handle count**—The number of system handles (that is, resources) allocated by each service.
- **Thread count**—The number of threads spawned by each service.

To monitor the status of the ACS services:

---

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

**Step 2** Click **Support**.

ACS displays the Support page.

**Step 3** Read system information in the Resource Usage table.

**Tip**

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

## Viewing or Downloading Diagnostic Logs (ACS SE Only)

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

In addition, if you are using an appliance base image that incorporates the CSA or have applied a CSA update to ACS, the View Diagnostic Logs page provides access to two logs that the CSA creates.

To view or download an appliance diagnostic log:

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

**Step 2** Click **View Diagnostic Logs**.

ACS displays the View Diagnostic Logs page:

- In the Log File column, the log files are listed by name.
- In the File Size column, the size of each log file appears (in kilobytes).

If ACS failed to create an expected log file, a `Log file is not created` message appears in the File Size column.

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

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

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

ACS displays the contents of the diagnostic log.

## Appliance Upgrade Mechanism (ACS SE Only)

This section contains:

- [About Appliance Upgrades and Patches, page 7-28](#)
- [Distribution Server Requirements, page 7-29](#)
- [Upgrading an Appliance, page 7-29](#)
- [Transferring an Upgrade Package to an Appliance, page 7-30](#)
- [Applying an Upgrade to an Appliance, page 7-33](#)

## About Appliance Upgrades and Patches

All upgrades and patches for ACS are packaged using the upgrade mechanism. For more information about installing ACS 4.2, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.



### Note

To upgrade to the ACS 4.2 release, you will need to reimage the appliance with the 4.2 recovery CD and then restore the ACS 4.1 database. The upgrade to ACS 4.2 includes the Windows 2003 Operating System upgrade.

Use the following three-phase process to upgrade or patch your existing ACS.

- **Phase one**—Obtain an upgrade package and load it onto a computer designated as a distribution server for ACS upgrade distribution. You can obtain the upgrade package as a CD-ROM or as a file that you download from [Cisco.com](http://Cisco.com).
- **Phase two**—Transfer installation package files from the distribution server to the appliance. The HTTP server, which is part of the installation package, performs file transfer. The upgrade files are signed and the signature is verified after uploading to ensure that the files have not been corrupted.
- **Phase three**—Apply the upgrade to the appliance. Before the upgrade files are applied to the appliance, ACS verifies the digital signature on the files to ensure their authenticity and to verify that they are not corrupt.

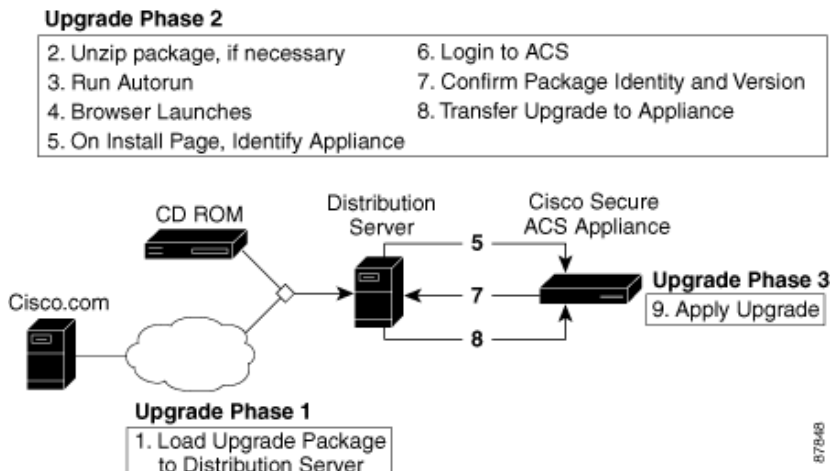


### Note

While you apply the upgrade, ACS cannot provide AAA services. If it is not critical to immediately apply an upgrade package, you should consider performing this phase when ACS downtime will have the least impact on users. For example, when you apply the upgrade, it will stop the AAA servers, apply the new patch, and then restart the AAA servers again.

Figure 7-1 summarizes the process.

**Figure 7-1 Appliance Upgrade Process**



## Distribution Server Requirements

The distribution server must meet the following requirements:

- For support, the distribution server must use an English-language version of one of the following operating systems:
  - Windows Server 2003 R2, Enterprise Edition
  - Windows 2000 Server with Service Pack 3 installed
  - Windows XP Professional with Service Pack 1 installed
  - Solaris 2.8

**Note**

While the upgrade process may succeed by using an unsupported operating system, the list reflects the operating systems that we used to test the upgrade process. We do not support upgrades from distribution servers that use untested operating systems.

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

**Tip**

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

- A supported web browser should be available on the distribution server. If necessary, you can use a web browser on a different computer than the distribution server. For a list of supported browsers, see the *Release Notes for Cisco Secure ACS Release 4.2*. The most recent revision to the Release Notes is posted on [Cisco.com](http://Cisco.com).

Gateway devices between the distribution server and any appliance that you want to upgrade must permit HTTP traffic to the distribution server on port 8080. They must also permit an ACS remote administrative session; therefore, they must permit HTTP traffic to the appliance on port 2002 and the range of ports allowed for administrative sessions. For more information, see [HTTP Port Allocation for Administrative Sessions, page 1-19](#).

## Upgrading an Appliance

Use the information in this section to upgrade the appliance software.

**Before You Begin**

Always back up ACS before upgrading. For information on backing up ACS, see [ACS Backup, page 7-8](#).

To upgrade an appliance:

**Step 1**

Acquire the upgrade package. Acquisition of an upgrade package differs depending on the type of upgrade package and service agreement. For:

- **Commercial upgrade packages**—Contact your Cisco sales representative.
- **Maintenance contracts**—You may be able to download upgrade packages from [Cisco.com](http://Cisco.com). Contact your Cisco sales representative.

- **Upgrade packages that apply patches for specific issues**—Contact your TAC representative.

**Step 2** Choose a computer to use as the distribution server. The distribution server must meet the requirements discussed in [Distribution Server Requirements, page 7-29](#).

**Step 3** If you have acquired the upgrade package in a compressed file format, such as a *.zip* or *.gz*:

- If you have not already done so, copy the upgrade package file to a directory on the distribution server.
- Use the appropriate file decompression utility to extract the upgrade package.




---

**Tip** Consider extracting the upgrade package in a new directory that you create for the contents of the upgrade package.

---

**Step 4** If you have acquired the upgrade package on CD, do not insert the CD in a CD-ROM drive until instructed to do so. The CD contains *autorun* files, and if the distribution server uses Microsoft Windows, the CD-ROM drive can prematurely start the *autorun* process.

**Step 5** Transfer the upgrade package to an appliance. For detailed steps, see [Transferring an Upgrade Package to an Appliance, page 7-30](#).

The upgrade package is now on the appliance and ready to be applied.

**Step 6** If the CSA is running on the appliance, disable the CSA. For detailed steps, see [Enabling or Disabling CSAgent, page 7-22](#).

**Step 7** Apply the upgrade package to the appliance. For detailed steps, see [Applying an Upgrade to an Appliance, page 7-33](#).

ACS applies the upgrade and runs using the upgraded software.

**Step 8** If you want the CSA to protect the appliance, enable it. For detailed steps, see [Enabling or Disabling CSAgent, page 7-22](#).




---

**Note** System restarts performed during the upgrade do not re-enable **CSAgent**.

---

## Transferring an Upgrade Package to an Appliance

Use this procedure to transfer an upgrade package from a distribution server to an appliance.




---

**Note** After you have performed this procedure, you must still apply the upgrade for it to become effective. For information on applying the upgrade, see [Applying an Upgrade to an Appliance, page 7-33](#). For more general information about the upgrade process, see [About Appliance Upgrades and Patches, page 7-28](#).

---

### Before You Begin

You must have acquired the upgrade package and selected a distribution server. For more information, see [Upgrading an Appliance, page 7-29](#).

To transfer an upgrade to your appliance:

- Step 1** If the distribution server uses Solaris, go to Step 2. If the distribution server uses Microsoft Windows:
- a. If you have acquired the upgrade package on CD, insert the CD in a CD-ROM drive on the distribution server.



**Tip** You can also use a shared CD drive on a different computer. If you do so and *autorun* is enabled on the shared CD drive, the HTTP server included in the upgrade package starts on the other computer. For example, if computer A and computer B share a CD drive, and you use the CD drive on computer B where *autorun* is also enabled, the HTTP server starts on computer B.

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

Locate the *autorun.bat* file on the CD or in the directory to which you extracted the compressed upgrade package, and start the *autorun*.

- c. The HTTP server starts, messages from *autorun.bat* appear in a console window, and ACS displays the following two browser windows:
  - Use **Appliance Upgrade** to enter the appliance hostname or IP address.
  - Use **New Desktop** to start transfers to other appliances.

- Step 2** If the distribution server uses Sun Solaris:

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



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

- d. The HTTP server starts, messages from *autorun.bat* appear in a console window, and the following two browser windows appear:
  - Use **Appliance Upgrade** to enter the appliance hostname or IP address.
  - Use **New Desktop** to start transfers to other appliances.

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

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



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

- Step 4** In the Appliance Upgrade browser window, enter the appliance IP address or hostname in the **Enter appliance hostname or IP address** box, and click **Install**.

The ACS login page for the specified appliance appears.

**Step 5** Log in to the ACS web interface:

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

**Step 6** In the navigation bar, click **System Configuration**.

**Step 7** Click **Appliance Upgrade Status**.

ACS displays the Appliance Upgrade page.

**Step 8** Click **Download**.

ACS displays the Appliance Upgrade Form page. This page contains the Transfer Setup table, which you use to identify the distribution server.

**Step 9** In the **Install Server** box, enter the hostname or IP address of the distribution server.

**Step 10** Click **Connect**.

The Appliance Upgrade Form page displays the Software Install table, which details the version and name of the upgrade available from the distribution server.

**Step 11** Examine the Software Install table to confirm that the version, name, and condition of the upgrade is satisfactory, and click **Download Now**.

ACS displays the Appliance Upgrade page and the upgrade file is downloaded from the distribution server to the appliance. ACS displays the status of the download below the Appliance Versions table.



**Tip**

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

**Step 12** If you want to update the transfer status message, click **Refresh**. **Refresh** exhibits the following behavior:



**Tip**

During the transfer, you can click **Refresh** as often as necessary to update the status message.

- If you click **Refresh**

While the transfer is in progress, ACS displays the number of downloaded kilobytes.

After the transfer is complete, ACS displays the Apply Upgrade button and the transfer progress text is replaced with a message indicating that an upgrade package is available on the appliance.

**Step 13** To ensure that the download was successful and the upgrade is ready to be applied, confirm that the following message appears on the Appliance Upgrade page: *Ready to Upgrade to version*, where *version* is the version of the upgrade package you have transferred to the appliance.

The upgrade package is now successfully transferred to the appliance.

**Step 14** If you want to transfer the upgrade package to another appliance, access the browser window titled **New Desktop**, click **Install Next**, and return to Step 4.



**Tip**

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

- Step 15** If you are finished transferring upgrade packages to appliances, access the browser window titled **New Desktop** and click **Stop Distribution Server**.
- The HTTP server stops and the distribution server releases the resources that the HTTP server used.
- Step 16** If you want to apply the upgrade, perform the steps in [Applying an Upgrade to an Appliance, page 7-33](#). Alternatively, you can use the **upgrade** command by using the serial console. For more information about the **upgrade** command, see *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.
- 

## Applying an Upgrade to an Appliance

You use this procedure to apply an upgrade package to an ACS.



### Note

As an alternative, you can apply an upgrade package by using the **upgrade** command on the serial console. For more information, see the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

---

### Before You Begin

Before you apply the upgrade:

- Transfer the upgrade package to the appliance. For detailed steps, see [Transferring an Upgrade Package to an Appliance, page 7-30](#). For the steps required to upgrade an appliance, see [Upgrading an Appliance, page 7-29](#).
- Back up ACS. For information about backing up ACS, see [ACS Backup, page 7-8](#).
- Disable the **CSAgent** service. Application of the upgrade will fail if **CSAgent** is running. For detailed steps, see [Enabling or Disabling CSAgent, page 7-22](#).



### Note

During the upgrade, ACS cannot provide AAA services. If it is not critical to immediately apply an upgrade package, consider performing this procedure when ACS downtime will have the least impact on users.

---

To apply an upgrade to an ACS:

---

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

**Caution**

---

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

---

After you have answered all confirmation prompts, ACS applies the upgrade. Be aware that:

- During an upgrade, ACS services and the web interface are not available. When the upgrade is complete, the ACS services and the web interface become available.
- Application of an upgrade can take several minutes. A full upgrade of ACS takes longer if the ACS internal database contains a large number of user profiles.
- Upgrade of ACS usually requires the appliance to restart itself once or twice. Smaller patches might not require restarts.
- If the browser window is open and the web interface is not available, wait for the appliance to resume normal operation. Then close the original browser window, open a new browser window, and log in to ACS.

**Caution**

---

Do not reset the appliance during application of an upgrade unless the TAC directs you to do so.

---

**Step 6**

After application of the upgrade, go to the Appliance Upgrade page and verify the versions of the software on the appliance. The Appliance Versions table lists the versions of software running on the appliance. Table entries should reflect the upgrade package that you applied.

**Note**

---

If the browser window is open and the web interface is not available, wait for the appliance to resume normal operation. Then close the original browser window, open a new browser window, and log in to ACS.

---