



System Configuration: Basic

This chapter addresses the basic features found in the System Configuration section of Cisco Secure ACS for Windows Server.

This chapter contains the following topics:

- [Service Control, page 8-1](#)
- [Logging, page 8-3](#)
- [Date Format Control, page 8-3](#)
- [Local Password Management, page 8-5](#)
- [Cisco Secure ACS Backup, page 8-9](#)
- [Cisco Secure ACS System Restore, page 8-14](#)
- [Cisco Secure ACS Active Service Management, page 8-17](#)
- [VoIP Accounting Configuration, page 8-21](#)

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 Logs, page 11-33](#).

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 within Windows Control panel. This procedure stops, starts, or restarts the Cisco Secure ACS services except for CSAdmin, which is responsible for the HTML interface.

**Note**

If the CSAdmin service needs to be restarted, you can do so using the Control Panel Services applet; however, it is best to allow Cisco Secure ACS to handle the 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

You use the Local Password Management page to configure settings that apply to managing passwords stored in the CiscoSecure user database. It contains the following three 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 long.
 - **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 replication partners.

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

- **Password Change Log File Management**—These settings enable you to configure how Cisco Secure ACS handles log files generated for the User Password Change report. For more information about this report, see [Cisco Secure ACS System Logs, page 11-13](#).

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

- **Generate New File**—You can specify the frequency at which Cisco Secure 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 Cisco Secure ACS controls the retention of log files. If enabled, this feature enables you to specify either the maximum number of files to retain or the maximum age of files to retain. If the maximum number of files is exceeded, Cisco Secure ACS deletes the oldest log file. If the maximum age of a file is exceeded, Cisco Secure ACS deletes the file.

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:
- 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.
 - 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.
 - If you want to disallow passwords that contain the username, select the **Password may not contain the username** check box.
 - 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.
 - 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:
- 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.
 - 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.
 - 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 (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 list below the **Upon remote user password change, immediately propagate the change to selected replication partners** check box.

- Step 5** If you want Cisco Secure ACS to generate a new User Password Changes log file at a regular interval, select one of the following options:
- **Every day**—Cisco Secure ACS generates a new User Password Changes log file at the start of each day.
 - **Every week**—Cisco Secure ACS generates a new User Password Changes log file at the start of each week.
 - **Every month**—Cisco Secure ACS generates a new User Password Changes log file at the start of each month.
- Step 6** If you want Cisco Secure 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 7** If you want to manage which User Password Changes log files Cisco Secure ACS keeps, follow these steps:
- a. Select the **Manage Directory** check box.
 - b. If you want to limit the number of User Password Changes log files Cisco Secure ACS retains, select the **Keep only the last X files** option and type the number of files you want Cisco Secure ACS to retain in the *X* box.
 - c. If you want to limit how old User Password Changes log files retained by Cisco Secure ACS can be, select the **Delete files older than X days** option and type the number of days for which Cisco Secure ACS should retain a User Password Changes log file before deleting it.
- Step 8** 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 8-9](#)
- [Backup File Locations, page 8-9](#)
- [Directory Management, page 8-10](#)
- [Components Backed Up, page 8-10](#)
- [Reports of Cisco Secure ACS Backups, page 8-10](#)
- [Backup Options, page 8-11](#)
- [Performing a Manual Cisco Secure ACS Backup, page 8-11](#)
- [Scheduling Cisco Secure ACS Backups, page 8-12](#)
- [Disabling Scheduled Cisco Secure ACS Backups, page 8-13](#)

About Cisco Secure ACS Backup

The ACS Backup feature backs up your Cisco Secure ACS system information to a file on the local hard drive. 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 to the hard drive on another system in case the hardware fails on the primary system.

For information about using a backup file to restore Cisco Secure ACS, see [Cisco Secure ACS System Restore, page 8-14](#).

Backup File Locations

The default directory for backup files is the following:

drive:\path\CSAuth\System Backups

where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory. For example, if you installed Cisco Secure ACS version 3.0 in the default location, the default backup location would be

```
c:\Program Files\CiscoSecure ACS v3.0\CSAuth\System Backups
```

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](#).

Directory Management

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 we recommend you be about clearing out old databases from the Cisco Secure ACS hard drive.

Components Backed Up

The ACS System Backup feature backs up the Cisco Secure ACS user database and information from the Windows Registry that is relevant to Cisco Secure 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. The Windows Registry information includes any system information that is stored in the Windows Registry, 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. When this option is selected, you can only perform a backup by following the steps in [Performing a Manual Cisco Secure ACS Backup, page 8-11](#).
- **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 interval is one hour, and the backup takes place on the hour selected.
- **Directory**—The directory where Cisco Secure ACS writes the backup file. The directory must be specified by its full path on the Windows server that runs Cisco Secure ACS, such as `c:\acs-bups`.
- **Manage Directory**—Defines whether Cisco Secure ACS deletes older backup files. Using the following options, you can specify how Cisco Secure ACS determines which log files to delete:
 - **Keep only the last X files**—Cisco Secure ACS retains the most recent backup files, up to the number of files specified. When the number of files specified is exceeded, Cisco Secure ACS deletes the oldest files.
 - **Delete files older than X days**—Cisco Secure ACS deletes backup files that are older than the number of days specified. When a backup file grows older than the number of days specified, Cisco Secure ACS deletes it.

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.

Step 3 In the Directory box under Backup Location, type the drive and path to the directory on a local hard drive where you want the backup file to be written.

Step 4 Click **Backup Now**.

Cisco Secure ACS immediately begins a backup.

Scheduling Cisco Secure ACS Backups

You can schedule Cisco Secure ACS backups to occur at regular intervals or on 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 too frequent, 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** To change the location where Cisco Secure ACS writes backup files, type the drive letter and path in the Directory box.
- Step 6** To manage which backup files Cisco Secure ACS keeps, follow these steps:
- Select the **Manage Directory** check box.
 - To limit the number of backup files Cisco Secure ACS retains, select the **Keep only the last X files** option and type in the *X* box the number of files you want Cisco Secure ACS to retain.
 - To limit how old backup files retained by Cisco Secure ACS can be, select the **Delete files older than X days** option and type the number of days for which Cisco Secure ACS should retain a backup file before deleting it.
- Step 7** 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 8-14](#)
- [Backup Filenames and Locations, page 8-14](#)
- [Components Restored, page 8-15](#)
- [Reports of Cisco Secure ACS Restorations, page 8-16](#)
- [Restoring Cisco Secure ACS from a Backup File, page 8-16](#)

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 Cisco Secure ACS Windows Registry information from a file that was created by the ACS Backup feature. Cisco Secure ACS writes backup files only on the local

hard drive. You can restore from any backup file you select. For example, 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.

The backup directory is selected when you schedule backups or perform a manual backup. The default directory for backup files is the following:

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

where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory. For example, if you installed Cisco Secure ACS version 3.0 in the default location, the default backup location would be:

```
c:\Program Files\CiscoSecure ACS v3.0\CSAuth\System Backups
```

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 are not sure of the location of the latest backup file, check your scheduled backup configuration on the ACS Backup 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.

The Directory box displays the drive and path to the backup directory most recently configured in the Directory box on the ACS Backup page.

Beneath the Directory box, Cisco Secure 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**.

Cisco Secure ACS displays the backup files, if any, in the backup directory you specified.

Step 4 In the list below the Directory box, select the backup file you want to use to restore Cisco Secure ACS.

- Step 5** To restore user and group database information, select the **User and Group Database** check box.
- Step 6** To restore system configuration information, select the **CiscoSecure ACS System Configuration** check box.
- Step 7** 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 8** 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 8-20](#)

System Monitoring

Cisco Secure ACS system monitoring enables you to determine how often Cisco Secure ACS tests its authentication and accounting processes, and to determine what automated actions it takes 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 G-4](#).

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 the test fails, after four unsuccessful re-tries Cisco Secure ACS performs the action identified in the If no successful authentications are recorded list and logs the event.

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


```
drive:\path\CSMon\Scripts
```

where *drive* is the local drive where you installed Cisco Secure ACS and *path* is the path from the root of *drive* to the Cisco Secure ACS directory.
 - **Take No Action**—Leave Cisco Secure ACS operating as is.
- **Generate event when an attempt is made to log in to a disabled account**—Specifies whether Cisco Secure ACS generates a log entry when a user attempts to log in to your network using a disabled account.
- **Log all events to the NT Event log**—Specifies whether Cisco Secure ACS generates a Windows event log entry for each exception event.

- **Email notification of event**—Specifies whether Cisco Secure ACS sends an e-mail notification for each event.
 - **To**—The e-mail address 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 in the X box the number of minutes (up to 3 characters) that should pass between each login process test.
 - c. From the **If no successful authentications are recorded** list, select the action Cisco Secure ACS should take when the login test fails five successive times.
- Step 4** To have Cisco Secure ACS generate a Windows event when a user attempts to log in to your network using a disabled account, select 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 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 logs events to the Windows event log and whether Cisco Secure ACS generates an e-mail when an event occurs. Cisco Secure ACS uses the System Monitoring feature to detect the events to be logged. For more information about system monitoring, see [System Monitoring Options, page 8-18](#).

Setting Up Event Logging

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

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

- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **ACS Service Management**.
The ACS Active Service Management Setup page appears.
- Step 3** To have Cisco Secure ACS send all events to the Windows event log, select **Log all events to the Windows Event log**.
- Step 4** To have Cisco Secure ACS send an e-mail when an event occurs, follow these steps:
- a. Select the **Email notification of event** check box.
 - b. In the To box, type the e-mail address (up to 200 characters) to which Cisco Secure ACS should send event notification e-mail.



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

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

**Note**

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

- Step 5** If you want to set up system monitoring, see [Setting Up System Monitoring, page 8-19](#).
- 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.
-

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.
