



System Configuration: Basic

This chapter addresses the basic features in the System Configuration section of the web interface for Cisco Secure Access Control Server Release 4.0 for Windows, hereafter referred to as ACS.

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 8-4](#)
- [ACS Backup, page 8-7](#)
- [ACS System Restore, page 8-11](#)
- [ACS Active Service Management, page 8-13](#)
- [VoIP Accounting Configuration, page 8-15](#)

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 11-24.](#)

This section contains the following topics:

- [Determining the Status of ACS Services, page 8-2](#)
- [Stopping, Starting, or Restarting Services, page 8-2](#)
- [Setting Service Log File Parameters, page 8-3](#)

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. Stopping, starting, or restarting ACS services from within the interface achieves the same result as starting and stopping ACS services from within Windows Control panel. This procedure stops, starts, or restarts the ACS services except for CSAdmin, which is responsible for the web interface.



Note

If you need to restart the CSAdmin service, you can use the Control Panel Services applet; however, you should just let ACS handle the services, due to the dependencies in the order which the services are started.

To stop, start, or restart 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 11-24](#).

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 11-23](#).

Date 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.



Tip

Using a comma-separated value (CSV) file might not work well in different countries; for example, when imported into programs such as Word or Excel. You might need to replace the commas(,) with semicolons (;) if necessary.

Setting the Date Format


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 *2001-07-12.csv* to a report that was generated on July 12, 2001. If you subsequently change to the day/month/year format, on December 7, 2001, ACS creates a file also named *2001-07-12.csv* and overwrites the existing file.

To set the date format:

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

Step 2 Click **Date Format Control**.

ACS displays the Date Format Selection table.

Step 3 Select a date format option.

Step 4 Click **Submit & Restart**.

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


Note

For the new date format to be seen 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

Validation options do not apply to the ACS **admin** password. ACS administrator accounts have no correlation with ACS user accounts, or username and password authentication. ACS stores accounts that were created for authentication of network service requests and those that were created for ACS administrative access in separate internal databases.

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**—When selected, this option disables the ability to perform password changes during a Telnet session that a Terminal Access Controller Access Control System (TACACS+) Authentication, Authorization, and Accounting (AAA) client hosts. 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 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 9-1](#).


- **Password Change Log File Management**—You use these settings to configure how ACS handles log files that are generated for the User Password Change report. For more information about this report, see [ACS System Logs, page 11-8](#).

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.

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:
- 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 Y 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, check the **Password may not contain the username** check box.
 - 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.
 - 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, 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, 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, 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).
 - 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** If you want ACS to generate a new User Password Changes log file at a regular interval, select one:
- 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 6** 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 7** 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.
 - 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 8** 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 must not perform backups, restores, or replication between different versions of ACS.

This section contains the following topics:

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

About ACS Backup

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. 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. 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 ACS, see [ACS System Restore, page 8-11](#).

**Note**

The backup and restore features between different ACS versions are not supported.

Backup File Locations

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 4.0 in the default location, the default backup location would be:

c:\Program Files\CiscoSecure ACS v4.0\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 [Backup Filenames and Locations, page 8-11](#).

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 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.

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

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 8-9](#).
- **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.
- **Directory**—The directory where 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.

Performing a Manual ACS Backup

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

To perform an immediate backup of ACS:

-
- 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**.
ACS immediately begins a backup.
-

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:

-
- 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 ACS should perform backups.



Note Because 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:
- 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.

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 backups, restores, or replication between different versions of ACS.

This section contains the following topics:

- [About ACS System Restore, page 8-11](#)
- [Backup Filenames and Locations, page 8-11](#)
- [Components Restored, page 8-12](#)
- [Reports of ACS Restorations, page 8-12](#)
- [Restoring ACS from a Backup File, page 8-12](#)

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.

Backup Filenames and Locations

The ACS System Restore feature restores the ACS user database and ACS Windows Registry information from a file that the ACS Backup feature created. ACS writes backup files only on the local hard drive. You can restore from any backup file that 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.

The backup directory is selected when you schedule backups or perform a manual backup. 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 3.0 in the default location, the default backup location would be:

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

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
```

If you are uncertain 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: 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 1, “Overview”](#).

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:

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, 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, select the **User and Group Database** check box.
- Step 6** To restore system configuration information, select the **ACS System Configuration** check box.
- Step 7** Click **Restore Now**.
- ACS displays a confirmation dialog box indicating that performing the restoration will restart ACS services and log out all administrators.
- Step 8** 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 the following topics:

- [System Monitoring, page 8-13](#)
- [Event Logging, page 8-15](#)

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 G-4](#).

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.

- **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**—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\C\$Mon\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**—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.
- **Log all events to the NT Event log**—Specifies whether ACS generates a Windows event log entry for each exception event.
- **Email notification of event**—Specifies whether ACS sends an e-mail notification for each event.
 - **To**—The e-mail address to which a notification e-mail 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:
 - 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 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, 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 8-15](#).
 - 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 8-13](#).

Setting Up Event Logging

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.

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** To have ACS send all events to the Windows event log, select **Log all events to the Windows Event log**.
- Step 4** To have ACS send an e-mail when an event occurs:
- Select the **Email notification of event** check box.
 - In the **To** box, type 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 type in this box.

- 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 ACS.

- Step 5** If you want to set up system monitoring, see [Setting Up System Monitoring, page 8-14](#).

- 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

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

To configure VoIP accounting:

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

Step 2 Click **VoIP Accounting Configuration**.



Note

If this feature does not appear, choose **Interface Configuration > Advanced Options**. Then, check 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 that you want.

Step 4 Click **Submit**.

ACS implements the VoIP accounting configuration that you specified.