

Administrators and Administrative Policy

This chapter addresses the Cisco Secure ACS Appliance features found in the Administration Control section of the HTML interface.

This chapter contains the following topics:

- [Administrator Accounts, page 12-1](#)
- [Access Policy, page 12-11](#)
- [Session Policy, page 12-16](#)
- [Audit Policy, page 12-18](#)

Administrator Accounts

This section provides details about Cisco Secure ACS administrators.

This section contains the following topics:

- [About Administrator Accounts, page 12-2](#)
- [Administrator Privileges, page 12-3](#)
- [Adding an Administrator Account, page 12-6](#)
- [Editing an Administrator Account, page 12-7](#)
- [Unlocking a Locked Out Administrator Account, page 12-10](#)
- [Deleting an Administrator Account, page 12-10](#)

About Administrator Accounts

Administrators are the only users of the Cisco Secure ACS HTML interface. To access the Cisco Secure ACS HTML interface from a browser run elsewhere than on the Cisco Secure ACS Windows server itself, you must log in to Cisco Secure ACS using an administrator account. If your Cisco Secure ACS is so configured, you may need to log in to Cisco Secure ACS even in a browser run on the Cisco Secure ACS Windows server. For more information about automatic local logins, see [Session Policy, page 12-16](#).



Note

Cisco Secure ACS administrator accounts are unique to Cisco Secure ACS. They are not related to other administrator accounts, such as Windows users with administrator privileges.

In the HTML interface, an administrator can configure any of the features provided in Cisco Secure ACS; however, the ability to access various parts of the HTML interface can be limited by revoking privileges to those parts of the HTML interface that a given administrator is not allowed to access.

For example, you may want to limit access to the Network Configuration section of the HTML interface to administrators whose responsibilities include network management. To do so, you would select only the Network Configuration privilege for applicable administrator accounts. For more information about administrator privileges, see [Administrator Privileges, page 12-3](#).

Cisco Secure ACS administrator accounts have no correlation with Cisco Secure ACS user accounts or username and password authentication. Cisco Secure ACS stores accounts created for authentication of network service requests and those created for Cisco Secure ACS administrative access in separate internal databases.

Administrator Privileges

You can grant appropriate privileges to each Cisco Secure ACS administrator by assigning privileges on an administrator-by-administrator basis. You control privileges by selecting the options from the Administrator Privileges table on the Add Administrator or Edit Administrator pages. These options are listed below:

- **User and Group Setup**—Contains the following privilege options for the User Setup and Group Setup sections of the HTML interface:
 - **Add/Edit users in these groups**—Enables the administrator to add or edit users and to assign users to the groups in the Editable groups list.
 - **Setup of these groups**—Enables the administrator to edit the settings for the groups in the Editable groups list.
 - **Available Groups**—Lists the user groups for which the administrator *does not* have edit privileges and to which the administrator *cannot* add users.
 - **Editable Groups**—Lists the user groups for which the administrator *does* have edit privileges and to which the administrator *can* add users.
- **Shared Profile Components**—Contains the following privilege options for the Shared Profile Components section of the HTML interface:
 - **Network Access Restriction Sets**—Allows the administrator full access to the Network Access Restriction Sets feature.
 - **Downloadable ACLs**—Allows the administrator full access to the Downloadable PIX ACLs feature.
 - **Create New Device Command Set Type**—Allows the administrator account to be used as valid credentials by another Cisco application for adding new device command set types. New device command set types that are added to Cisco Secure ACS using this privilege appear in the Shared Profile Components section of the HTML interface.
 - **Shell Command Authorization Sets**—Allows the administrator full access to the Shell Command Authorization Sets feature.
 - **PIX Command Authorization Sets**—Allows the administrator full access to the PIX Command Authorization Sets feature.



Note Additional command authorization set privilege options may appear, if other Cisco network management applications, such as CiscoWorks2000, have updated the configuration of Cisco Secure ACS.

- **Network Configuration**—Allows the administrator full access to the features in the Network Configuration section of the HTML interface.
- **System Configuration...** —Contains the privilege options for the features found in the System Configuration section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
 - **Service Control**—For more information about this feature, see [Service Control, page 8-1](#).
 - **Date/Time Format Control**—For more information about this feature, see [Date Format Control, page 8-3](#).
 - **Logging Control**—For more information about this feature, see [Logging, page 8-3](#).
 - **Local Password Management**—For more information about this feature, see [Local Password Management, page 8-5](#).
 - **DB Replication**—For more information about this feature, see [CiscoSecure Database Replication, page 9-1](#).
 - **RDBMS Synchronization**—For more information about this feature, see [RDBMS Synchronization, page 9-24](#).
 - **IP Pool Address Recovery**—For more information about this feature, see [IP Pools Address Recovery, page 9-50](#).
 - **IP Pool Server Configuration**—For more information about this feature, see [IP Pools Server, page 9-43](#).
 - **ACS Backup**—For more information about this feature, see [Cisco Secure ACS Backup, page 8-9](#).
 - **ACS Restore**—For more information about this feature, see [Cisco Secure ACS System Restore, page 8-14](#).
 - **ACS Service Management**—For more information about this feature, see [Cisco Secure ACS Active Service Management, page 8-18](#).

- **VoIP Accounting Configuration**—For more information about this feature, see [VoIP Accounting Configuration, page 8-22](#).
- **ACS Certificate Setup**—For more information about this feature, see [Cisco Secure ACS Certificate Setup, page 10-33](#).
- **Global Authentication Setup**—For more information about this feature, see [Global Authentication Setup, page 10-25](#).
- **Interface Configuration**—Allows the administrator full access to the features in the Interface Configuration section of the HTML interface.
- **Administration Control**—Allows the administrator full access to the features in the Administration Control section of the HTML interface.
- **External User Databases**—Allows the administrator full access to the features in the External User Databases section of the HTML interface.
- **Reports & Activity**—Contains the privilege options for the reports and features found in the Reports and Activity section of the HTML interface. For each of the following features, enabling the option allows the administrator full access to the feature.
 - **TACACS+ Accounting**—For more information about this report, see [Accounting Logs, page 11-5](#).
 - **TACACS+ Administration**—For more information about this report, see [Accounting Logs, page 11-5](#).
 - **RADIUS Accounting**—For more information about this report, see [Accounting Logs, page 11-5](#).
 - **VoIP Accounting**—For more information about this report, see [Accounting Logs, page 11-5](#).
 - **Passed Authentications**—For more information about this report, see [Accounting Logs, page 11-5](#).
 - **Failed Attempts**—For more information about this report, see [Accounting Logs, page 11-5](#).
 - **Logged-in Users**—For more information about this report, see [Dynamic Administration Reports, page 11-8](#).
 - **Purge of Logged-in Users**—For more information about this feature, see [Deleting Logged-in Users, page 11-10](#).
 - **Disabled Accounts**—For more information about this report, see [Dynamic Administration Reports, page 11-8](#).

- **ACS Backup and Restore**—For more information about this report, see [Cisco Secure ACS System Logs, page 11-11](#).
- **DB Replication**—For more information about this report, see [Cisco Secure ACS System Logs, page 11-11](#).
- **RDBMS Synchronization**—For more information about this report, see [Cisco Secure ACS System Logs, page 11-11](#).
- **Administration Audit**—For more information about this report, see [Cisco Secure ACS System Logs, page 11-11](#).
- **ACS Service Monitor**—For more information about this report, see [Cisco Secure ACS System Logs, page 11-11](#).
- **User Change Password**—For more information about this report, see [Cisco Secure ACS System Logs, page 11-11](#).

Adding an Administrator Account

Before You Begin

For descriptions of the options available while adding an administrator account, see [Administrator Privileges, page 12-3](#).

To add a Cisco Secure ACS administrator account, follow these steps:

-
- Step 1** In the navigation bar, click **Administration Control**.
 - Step 2** Click **Add Administrator**.
The Add Administrator page appears.
 - Step 3** Complete the boxes in the Administrator Details table:
 - a. In the Administrator Name box, type the login name (up to 32 characters) for the new Cisco Secure ACS administrator account.
 - b. In the Password box, type the password (up to 32 characters) for the new Cisco Secure ACS administrator account.
 - c. In the Confirm Password box, type the password a second time.
 - Step 4** To select all privileges, including user group editing privileges for all user groups, click **Grant All**.

All privilege options are selected. All user groups move to the Editable groups list.



Tip To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.

- Step 5** To grant user and user group editing privileges, follow these steps:
- Select the desired check boxes under User & Group Setup.
 - To move a user group to the Editable groups list, select the group in the Available groups list, and then click --> (right arrow button).
The selected group moves to the Editable groups list.
 - To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <-- (left arrow button).
The selected group moves to the Available groups list.
 - To move all user groups to the Editable groups list, click >>.
The user groups in the Available groups list move to the Editable groups list.
 - To remove all user groups from the Editable groups list, click <<.
The user groups in the Editable groups list move to the Available groups list.
- Step 6** To grant any of the remaining privilege options, in the Administrator Privileges table, select the applicable check boxes.
- Step 7** Click **Submit**.
- Cisco Secure ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control page.
-

Editing an Administrator Account

You can edit a Cisco Secure ACS administrator account to change the privileges granted to the administrator. You can effectively disable an administrator account by revoking all privileges.



Note You cannot change the name of an administrator account; however, you can delete an administrator account and then create an account with the new name. For information about deleting an administrator account, see [Deleting an Administrator Account, page 12-10](#). For information about creating an administrator account, see [Adding an Administrator Account, page 12-6](#).

For information about administrator privilege options, see [Administrator Privileges, page 12-3](#).

Before You Begin

For descriptions of the options available while editing an administrator account, see [Administrator Privileges, page 12-3](#).

To edit Cisco Secure ACS administrator account privileges, follow these steps:

-
- Step 1** In the navigation bar, click **Administration Control**.
Cisco Secure ACS displays the Administration Control page.
- Step 2** Click the name of the administrator account whose privileges you want to edit.
The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.
- Step 3** To change the administrator password, follow these steps:
- In the Password box, double-click the asterisks, and then type the new password (up to 32 characters) for the administrator.
The new password replaces the existing, masked password.
 - In the Confirm Password box, double-click the asterisks, and then type the new administrator password a second time.
- The new password is effective immediately after you click Submit in Step 9.
- Step 4** If the Reset current failed attempts count check box appears below the Confirm Password box and you want to allow the administrator whose account you are editing to access the Cisco Secure ACS HTML interface, select the **Reset current failed attempts count** check box.



Note If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator cannot access Cisco Secure ACS unless you complete Step 4. For more information about re-enabling an administrator account, see [Unlocking a Locked Out Administrator Account, page 12-10](#).

- Step 5** To select all privileges, including user group editing privileges for all user groups, click **Grant All**.
- All privilege options are selected. All user groups move to the Editable groups list.
- Step 6** To clear all privileges, including user group editing privileges for all user groups, click **Revoke All**.
- All privileges options are cleared. All user groups move to the Available groups list.
- Step 7** To grant user and user group editing privileges, follow these steps:
- Under User & Group Setup, select the applicable check boxes.
 - To move all user groups to the Editable groups list, click >>. The user groups in the Available groups list move to the Editable groups list.
 - To move a user group to the Editable groups list, select the group in the Available groups list, and then click --> (right arrow button). The selected group moves to the Editable groups list.
 - To remove all user groups from the Editable groups list, click <<. The user groups in the Editable groups list move to the Available groups list.
 - To remove a user group from the Editable groups list, select the group in the Editable groups list, and then click <-- (left arrow button). The selected group moves to the Available groups list.
- Step 8** To grant any remaining privilege options, select the applicable check boxes in the Administrator Privileges table.
- Step 9** To revoke any remaining privilege options, clear the applicable check boxes in the Administrator Privileges table.

Step 10 Click **Submit**.

Cisco Secure ACS saves the changes to the administrator account.

Unlocking a Locked Out Administrator Account

Cisco Secure ACS disables the accounts of administrators who have attempted to access the Cisco Secure ACS HTML interface and have provided an incorrect password in more successive attempts than is specified on the Session Policy Setup page. Until the failed attempts counter for a disabled administrator account is reset, the administrator cannot access the HTML interface.

For more information about configuring how many successive failed login attempts can occur before Cisco Secure ACS disables an administrator account, see [Session Policy, page 12-16](#).

To reset the failed attempts count for an administrator, follow these steps:

Step 1 In the navigation bar, click **Administration Control**.

Cisco Secure ACS displays the Administration Control page.

Step 2 Click the name of the administrator account whose account you want to re-enable.

The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.

If the Reset current failed attempts count check box appears below the Confirm Password box, the administrator account cannot access the HTML interface.

Step 3 Select the **Reset current failed attempts count** check box.

Step 4 Click **Submit**.

Cisco Secure ACS saves the changes to the administrator account.

Deleting an Administrator Account

You can delete a Cisco Secure ACS administrator account when you no longer need it. We recommend deleting any unused administrator accounts.

To delete a Cisco Secure ACS administrator account, follow these steps:

-
- Step 1** In the navigation bar, click **Administration Control**.
Cisco Secure ACS displays the Administration Control page.
- Step 2** In the Administrators table, click the name of the administrator account that you want to delete.
The Edit Administrator *name* page appears, where *name* is the name of the administrator account you just selected.
- Step 3** Click **Delete**.
Cisco Secure ACS displays a confirmation dialog box.
- Step 4** Click **OK**.
Cisco Secure ACS deletes the administrator account. The Administrators table on the Administration Control page no longer lists the administrator account that you deleted.
-

Access Policy

The Access Policy feature affects access to the Cisco Secure ACS HTML interface. You can limit access by IP address and by the TCP port range used for administrative sessions. You can also enable secure socket layer (SSL) for access to the HTML interface.

This section contains the following topics:

- [Access Policy Options, page 12-12](#)
- [Setting Up Access Policy, page 12-13](#)

Access Policy Options

You can configure the following options on the Access Policy Setup page:

- **IP Address Filtering**—Contains the following IP address filtering options:
 - **Allow all IP addresses to connect**—Allow access to the HTML interface from any IP address.
 - **Allow only listed IP addresses to connect**—Allow access to the HTML interface only from IP addresses *inside* the address range(s) specified in the IP Address Ranges table.
 - **Reject connections from listed IP addresses**—Allow access to the HTML interface only from IP addresses *outside* the address range(s) specified in the IP Address Ranges table.
- **IP Address Ranges**—The IP Address Ranges table contains ten rows for configuring IP address ranges. The ranges are always inclusive; that is, the range includes the start and end IP addresses. The IP addresses entered to define a range must differ only in the last octet (Class C format).

The IP Address Ranges table contains one column of each of the following boxes:

- **Start IP Address**—Defines the lowest IP address of the range specified in the current row.
 - **End IP Address**—Defines the highest IP address of the range specified in the current row.
- **HTTP Port Allocation**—Contains the following options for configuring TCP ports used for remote access to the HTML interface.
 - **Allow any TCP ports to be used for Administration HTTP Access**—Allow the ports used by administrative HTTP sessions to include the full range of TCP ports.
 - **Restrict Administration Sessions to the following port range From Port X to Port Y**—Restrict the ports used by administrative HTTP sessions to the range specified in the *X* and *Y* boxes, inclusive. The size of the range specified determines the maximum number of concurrent administrative sessions.

Cisco Secure ACS uses port 2002 to start all administrative sessions. You do not need to include port 2002 in the port range. Also, Cisco Secure ACS does not allow you to define an HTTP port range that consists only of port 2002. Your port range must consist of at least one port other than port 2002.

A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port a web browser must address to initiate an administrative session.

**Note**

We do not recommend allowing administration of Cisco Secure ACS from outside a firewall. If you do choose to allow access to the HTML interface from outside a firewall, keep the HTTP port range as narrow as possible. This can help prevent accidental discovery of an active administrative port by unauthorized users. An unauthorized user would have to impersonate, or “spoof,” the IP address of a legitimate host to make use of the active administrative session HTTP port.

- **Secure Socket Layer Setup**—The Use HTTPS Transport for Administration Access check box defines whether Cisco Secure ACS uses secure socket layer protocol to encrypt HTTP traffic between the CSAdmin service and a web browser used to access the HTML interface. When this option is enabled, all HTTP traffic between the browser and Cisco Secure ACS is encrypted, as reflected by the URLs, which begin with HTTPS. Additionally, most browsers include an indicator for when a connection is SSL-encrypted.

To enable SSL, you must have completed the steps in [Installing a Cisco Secure ACS Server Certificate, page 10-34](#) and [Adding a Certificate Authority Certificate, page 10-36](#).


Setting Up Access Policy

For information about access policy options, see [Access Policy Options, page 12-12](#).

Before You Begin

If you want to enable SSL for administrative access, before completing this procedure, you must have completed the steps in [Installing a Cisco Secure ACS Server Certificate, page 10-34](#), and [Adding a Certificate Authority Certificate, page 10-36](#).

To set up Cisco Secure ACS Access Policy, follow these steps:

-
- Step 1** In the navigation bar, click **Administration Control**.
Cisco Secure ACS displays the Administration Control page.
- Step 2** Click **Access Policy**.
The Access Policy Setup page appears.
- Step 3** To allow remote access to the HTML interface from any IP address, in the IP Address Filtering table, select the **Allow all IP addresses to connect** option.
- Step 4** To allow remote access to the HTML interface only from IP addresses *within* a range or ranges of IP addresses, follow these steps:
- In the IP Address Filtering table, select the **Allow only listed IP addresses to connect** option.
 - For each IP address range from within which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. In the Start IP Address box, type the lowest IP address (up to 16 characters) in the range. In the End IP Address box, type the highest IP address (up to 16 characters) in the range. Use dotted decimal format.
-  **Note** The IP addresses entered to define a range must differ only in the last octet.
-
- Step 5** To allow remote access to the HTML interface only from IP addresses *outside* a range or ranges of IP addresses, follow these steps:
- In the IP Address Filtering table, select the **Reject connections from listed IP addresses** option.

- b. For each IP address range from outside which you want to allow remote access to the HTML interface, complete one row of the IP Address Ranges table. Type the lowest IP address (up to 16 characters) in the range in the Start IP Address box. Type the highest IP address (up to 16 characters) in the range in the End IP Address box.



Note The IP addresses entered to define a range must differ only in the last octet.

- Step 6** If you want to allow Cisco Secure ACS to use any valid TCP port for administrative sessions, under HTTP Port Allocation, select the **Allow any TCP ports to be used for Administration HTTP Access** option.
- Step 7** If you want to allow Cisco Secure ACS to use only a specified range of TCP ports for administrative sessions, follow these steps:
- a. Under HTTP Port Allocation, select the **Restrict Administration Sessions to the following port range From Port X to Port Y** option.
 - b. In the *X* box type the lowest TCP port (up to 5 characters) in the range.
 - c. In the *Y* box type the highest TCP port (up to 5 characters) in the range.
- Step 8** If you want to enable SSL encryption of administrator access to the HTML interface, under Secure Socket Layer Setup, select the **Use HTTPS Transport for Administration Access** check box.



Note To enable SSL, you must have completed the steps in [Installing a Cisco Secure ACS Server Certificate, page 10-34](#), and [Adding a Certificate Authority Certificate, page 10-36](#).

- Step 9** Click **Submit**.
- Cisco Secure ACS saves and begins enforcing the access policy settings.
- If you have enabled SSL, at the next administrator login, Cisco Secure ACS begins using HTTPS. Any current administrator sessions are unaffected.
-

Session Policy

The Session Policy feature controls various aspects of Cisco Secure ACS administrative sessions.

This section contains the following topics:

- [Session Policy Options, page 12-16](#)
- [Setting Up Session Policy, page 12-17](#)

Session Policy Options

You can configure the following options on the Session Policy Setup page:

- **Session idle timeout (minutes)**—Defines the time in minutes that an administrative session, local or remote, must remain idle before Cisco Secure ACS terminates the connection. This parameter applies to the Cisco Secure ACS administrative session in the browser only. It does not apply to an administrative dial-up session.

An administrator whose administrative session is terminated receives a dialog box asking whether or not the administrator wants to continue. If the administrator chooses to continue, Cisco Secure ACS starts a new administrative session.

- **Allow Automatic Local Login**—Enables administrators to start an administrative session without logging in if they are using a browser on the computer running Cisco Secure ACS. Such administrative sessions are conducted using a default administrator account named “local_login”. The local_login administrator account has all privileges. Local administrative sessions with automatic local login are recorded in the Administrative Audit report under the local_login administrator name.



Note

If there are no administrator accounts defined, no administrator name and password are required to access Cisco Secure ACS locally. This prevents you from accidentally locking yourself out of Cisco Secure ACS.

- **Respond to Invalid IP Address Connections**—Enables an error message in response to attempts to start a remote administrative session using an IP address that is invalid according to the IP address ranges configured in Access Policy. Disabling this option can help prevent unauthorized users from discovering Cisco Secure ACS.
- **Lock out Administrator after X successive failed attempts**—Enables Cisco Secure ACS to lock out an administrator after a number of successive failed attempts to log in to the HTML interface. The number of successive attempts is specified in the X box. If this check box is selected, the X box cannot be set to zero. If this check box is not selected, Cisco Secure ACS allows unlimited successive failed login attempts by an administrator.

Setting Up Session Policy

For information about session policy options, see [Session Policy Options, page 12-16](#).

To setup Cisco Secure ACS Session Policy, follow these steps:

-
- Step 1** In the navigation bar, click **Administration Control**.
Cisco Secure ACS displays the Administration Control page.
 - Step 2** Click **Session Policy**.
The Session Policy Setup page appears.
 - Step 3** To define the number of minutes of inactivity after which Cisco Secure ACS ends an administrative session, in the Session idle timeout (minutes) box, type the number of minutes (up to 4 characters).
 - Step 4** Set the automatic local login policy:
 - To allow administrators to log in to Cisco Secure ACS locally without using their administrator names and passwords, select the **Allow Automatic Local Login** check box.
 - To require administrators to log in to Cisco Secure ACS locally using their administrator names and passwords, clear the **Allow Automatic Local Login** check box.

- Step 5** Set the invalid IP address response policy:
- To configure Cisco Secure ACS to respond with a message when an administrative session is requested from an invalid IP address, select the **Respond to invalid IP address connections** check box.
 - To configure Cisco Secure ACS to send no message when an administrative session is requested from an invalid IP address, clear the **Respond to invalid IP address connections** check box.
- Step 6** Set the failed administrative login attempts policy:
- To enable Cisco Secure ACS to lock out an administrator after a specified number of successive failed administrative login attempts, select the **Lock out Administrator after X successive failed attempts** check box.
 - In the *X* box, type the number of successive failed login attempts after which Cisco Secure ACS locks out an administrator. The *X* box accepts up to 4 characters.
- Step 7** Click **Submit**.
- Cisco Secure ACS saves and begins enforcing the session policy settings you made.
-

Audit Policy

The Audit Policy feature controls the generation of the Administrative Audit log. For more information about enabling, viewing, or configuring the Administrative Audit log, see [Cisco Secure ACS System Logs, page 11-11](#).