



# CHAPTER 11

## Administrators and Administrative Policy

---

This chapter addresses the features in the Administration Control section of the Cisco Secure Access Control Server Release 4.2, hereafter referred to as ACS.

This chapter contains:

- [Administrator Accounts, page 11-1](#)
- [Logging In, page 11-5](#)
- [Adding, Editing, and Deleting Accounts, page 11-6](#)
- [Configuring Policy Options, page 11-8](#)
- [Administration Control Pages Reference, page 11-10](#)

### Administrator Accounts

Administrator accounts provide the only access to the ACS web interface.

This section contains:

- [About Administrator Accounts, page 11-1](#)
- [Privileges, page 11-2](#)
- [Group Access Privileges, page 11-3](#)
- [Password Expirations and Account Lockouts, page 11-3](#)
- [Support for Regulatory Compliance, page 11-4](#)

### About Administrator Accounts

From the Administration Control page, you can link to pages that establish the names, passwords, and privileges for individual administrators or groups of administrators.

ACS administrator accounts are:

- Unique to ACS and not related to other accounts, such as Windows administrator accounts, ACS TACACS+ accounts, or any other ACS user accounts.
- Unrelated to external ACS users because ACS stores ACS administrator accounts in a separate internal database.

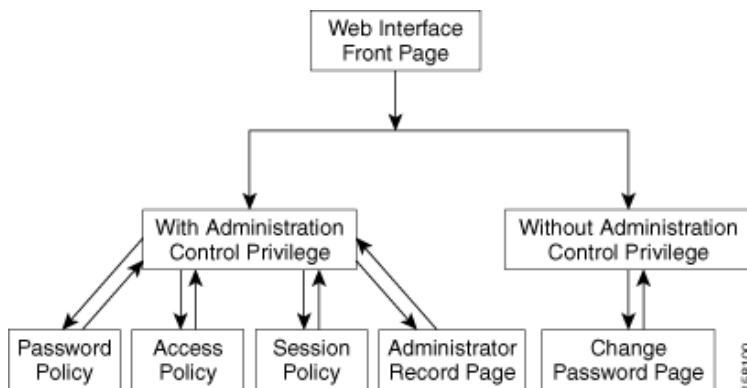
## Privileges

The privileges that you grant to each administrator determine access to areas of the web interface. By default, new administrators do not have any privileges.

### Administration Control Privilege

Administrators who have the Administration Control privilege can access the complete Administration Control page. For these administrators, this page provides management of administrators and access to pages that control administrative access policy. Restricted administrators can update their passwords. [Figure 11-1 on page 11-2](#) shows the access granted by the administration control privilege.

**Figure 11-1** The Administration Control Privilege



Examples of privileges that you can grant to administrators or groups of administrators include:

- Shared profile components
- Network, system, and interface configuration
- Administration control
- External user databases, posture validation, and network access profiles (NAPs)
- Reports and activities

For example, you are an administrator with the Administration Control privilege who wants to configure access to the Network Configuration section of the web interface for administrators whose responsibilities include network management. Therefore, you check only the Network Configuration privilege for the applicable administrator accounts.

However, you might want to configure all privileges for an administrator or an administrative group. In this case, you click the Grant All (privileges) option.

The web interface also includes a filter that can control the type of access granted to administrators. For example, you can configure an administrator for read-only access to groups of users, or you can grant them add and edit access to the same groups.



#### Note

See [Chapter 10, “Logs and Reports,”](#) for information on generating reports of privileges granted to administrators.

## The Influence of Policy

The Administration Control page also includes links to access, session, and password policy configuration pages. These policies influence all account logins and include the following configuration options:

- **Access Policy**—IP address limitations, HTTP port restrictions, and secure socket layer (SSL) setup.
- **Session Policy**—Timeouts, automatic local logins, and response to invalid IP address connections.
- **Password Policy**—Password validation, lifetime, inactivity, and incorrect attempts.

## Group Access Privileges

ACS includes options that determine the type of administrator access to groups or users in groups. When enabled, these options grant an administrator the following privileges with respect to any available group:

- Add or edit user pages
- Edit group pages
- Read access to user pages
- Read access to the group pages

Table 11-1 describes the interaction of the options:

**Table 11-1** Group Access Options

Add and Edit Access	Read Access	Result
No	No	Administrators cannot view the users in the Editable groups.
No	Yes	Administrators can view the users in the Editable groups, but Submit is not available.
Yes	No	Full access granted in either case. When enabled, Add/Edit Users in these groups overrides Read Access.
Yes	Yes	

## Password Expirations and Account Lockouts

Successful logins take administrators to the main ACS web interface page. However, all logins are subject to the restrictions that have been configured in Administration Control, including expiration, account lockout, and password configuration options.

Limits set for password lifetime and password inactivity can force password change or account lockout. In addition, the limit set for failed attempts can force password change, and privileged administrators can manually lock accounts. In the case of an account lockout, a privileged administrator must unlock the account.

ACS includes the Account Never Expires option that can globally override automatic account lockouts and password configuration options. If the Account Never Expires option is enabled for a specific administrator, all administrator lockout options are ignored.

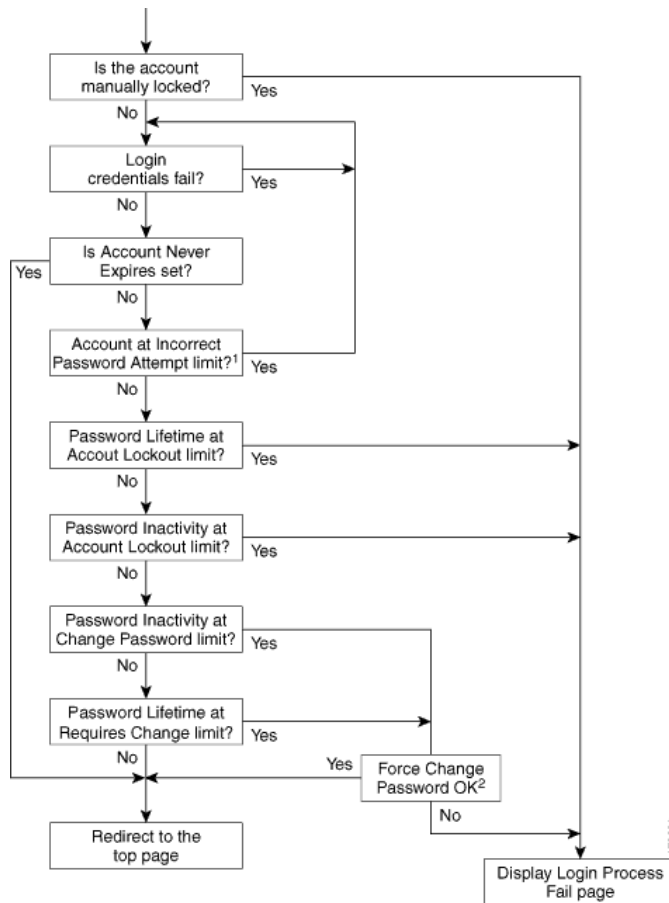
In the case of an account lockout, ACS displays the Login Process Fail page. Depending on the options, ACS displays the following pages for changing passwords:

- A password update page appears when you attempt to log in.

- The Change Password page appears when you click the Administration Control button in the navigation bar, if you do not have the Administration Control privilege. The Change Password page includes a list of the password criteria.

Figure 11-2 on page 11-4 shows the process flow at login time.

**Figure 11-2 Login Process Flow**



<sup>1</sup> When the administrator reaches the Incorrect Password Attempts limit, ACS locks the account. At this point, successful attempts will fail. However, if Account Never Expires is set, then the account cannot be locked out.

<sup>2</sup> The administrator has successfully logged in. Therefore, if only the password has been incorrectly used, ACS allows retries even though the administrator has exceeded the Incorrect Password Attempt limit.

## Support for Regulatory Compliance

ACS includes options that can support regulatory compliance. For example, an administrator with the Administration Control privilege can decide whether to grant the Administration Control privilege to other administrators. Administrators who do not have this privilege cannot access the administrator configuration details.

All administrator logins are subject to the policy that you configure for passwords and accounts, unless you check the **Account Never Expires** option. For example, ACS provides configurable limits on password lifetime, activity, and incorrect password attempts. These options can force password change and can result in automatic account lockout. Privileged administrators can also lock out an account. In addition, you can monitor the last password change and last account activity for each administrator.

In addition, you can restrict access to reports. For example, you can enable or disable an administrator's ability to change the Administration Audit report configuration.

You can also configure administrator access to user groups. You can selectively choose to allow administrators to setup groups and add or edit users. ACS also provides configuration of administrator read access to users and groups.

## Logging In

The ACS login page is the access point for the web interface. If your valid password expires, or if a change in policy affects a password, ACS forces you to change your password when you log in. If you are locked out, contact an administrator who has the Administration Control privilege.



### Note

Administrators must have a Windows domain administrator account in order to log in and manage ACS services. However, Windows domain administrators cannot log in to ACS. Only administrators with valid ACS accounts can log in to ACS. For information, see the *Installation Guide for Cisco Secure ACS for Windows Release 4.2* or the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

### ACS for Windows

To log in from a client, you must have an administrator account. However, the Session Policy includes an Allow automatic local login option. If this option is enabled, you can bypass the login page on the server that is running ACS. This option is available for unintentional lockouts. For more information about automatic local logins, see [Configuring Session Policy, page 11-8](#).

### ACS SE

To access the ACS web interface from a browser, log in to ACS by using an administrator account.

The first administrator to log in must create an administrator name and password by using the **Add ACS Admin** command in the command line interface (CLI) to create the administrator name and password for the first account. For complete information on the CLI, see the “Administering Cisco Secure ACS Solution Engine” chapter of the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

In cases where ACS has locked out all administrators, use the **Unlock** *<administrator name>* command from the CLI. Only an administrator with the Administration Control privilege can use this command. For complete information on the CLI, see the “Administering Cisco Secure ACS Solution Engine” chapter of the *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*.

To log in:

- 
- Step 1** To start ACS, click the **ACS Admin** button in the Cisco Secure ACS program group.  
The Cisco Secure ACS login page appears.
  - Step 2** Type your Username and Password.
  - Step 3** Click the **Login** button.

The Cisco Secure ACS main page appears.

---

## Adding, Editing, and Deleting Accounts

Administrators with the Administration Control privilege can add, edit, and delete administrator accounts.

This section contains:

- [Adding or Editing Accounts](#)
- [Deleting an Account](#)

### Adding or Editing Accounts

To add or edit an administrator account:

---

- Step 1** In the navigation bar, click **Administration Control**.
- The [Administration Control Page](#) appears if the current account has the Administration Control privilege. Otherwise, a Change Password page appears.
- Step 2** Click **Add Administrator**, and the Add Administrator page appears; or, click the name of the administrator account that you want to edit and the Edit Administrator *administrator\_name* page appears.
- Step 3** Type the Administrator Name, Password, and Password Confirmation for new accounts. If necessary, change the Password and Password Confirmation fields for an existing account. For information about these fields, see [Add Administrator and Edit Administrator Pages, page 11-11](#).
- Step 4** Check **Account Never Expires** to prevent the account for this administrator from expiring. For information, see [Add Administrator and Edit Administrator Pages, page 11-11](#).
- Step 5** Check the **Account Locked** check box to lock this account. If the **Account Locked** check box is checked, uncheck the box to unlock the account.
- Step 6** Click **Grant All** or **Revoke All** to globally add or remove all privileges. For information on these commands, see [Add Administrator and Edit Administrator Pages, page 11-11](#). Removing privileges from an existing account disables the account.
- Step 7** Move the group names between the Available groups and Editable groups list boxes. Groups in the Editable groups list, and associated users, will be available to the current administrator according to the access options that you check.
- Step 8** Check the appropriate options to grant access privileges to the Editable groups and associated users. For information on these options, see [Add Administrator and Edit Administrator Pages, page 11-11](#).
- Step 9** Check the appropriate options in the Shared Profile Components area to grant access to specific areas of the Shared Profile Components section of the web interface. For information on these options, see [Add Administrator and Edit Administrator Pages, page 11-11](#). For information on shared profile components, see [Chapter 4, “Shared Profile Components.”](#)
- Step 10** Check **Network Configuration** to grant access to the Network Configuration section of the web interface. For information on network configuration, see [Chapter 3, “Network Configuration.”](#)

- Step 11** Check options in the System Configuration area to grant access to pages in the System Configuration section of the web interface. For information on these options, see [Add Administrator and Edit Administrator Pages, page 11-11](#). For information on system configuration, see [Chapter 7, “System Configuration: Basic,”](#) [Chapter 8, “System Configuration: Advanced,”](#) and [Chapter 10, “Logs and Reports.”](#)
- Step 12** Check the **Interface Configuration** option to grant access to the Interface Configuration section of the web interface. For information on interface configuration, see [Chapter 2, “Using the Web Interface.”](#)
- Step 13** Check the **Administration Control** option to grant access to the Administration Control section of the web interface.
- Step 14** Check the **External User Databases** option to grant access to the External User Databases section of the web interface. For information on external user databases, see [Chapter 12, “User Databases.”](#)
- Step 15** Check the **Posture Validation** option to grant access to the Posture Validation section of the web interface. For information on posture validation, see [Chapter 13, “Posture Validation.”](#)
- Step 16** Check the **Network Access Profiles** option to grant access to the Network Access Profiles section of the web interface. For information on network access profiles, see [Chapter 14, “Network Access Profiles.”](#)
- Step 17** Check options in the **Reports and Activities** area to grant access to pages in the Reports and Activities section of the web interface. For information on these options, see [Add Administrator and Edit Administrator Pages, page 11-11](#). For information on reports, see [Chapter 10, “Logs and Reports.”](#)
- Step 18** Click **Submit**.
- ACS saves the new administrator account. The new account appears in the list of administrator accounts on the Administration Control page.
- 

## Deleting an Account

You use this feature to delete administrator accounts. You can disable an account by clicking the **Revoke All** button. However, we recommend that you delete any unused administrator accounts.

To delete an account:

- 
- Step 1** In the navigation bar, click **Administration Control**.
- ACS displays the Administration Control page.
- Step 2** Click the name of the administrator account that you want to delete.
- The Edit Administrator *administrator\_name* page appears, where *administrator\_name* is the name of the administrator account that you have selected.
- Step 3** Click the **Delete** button.
- ACS displays a confirmation dialog box.
- Step 4** Click **OK**.
- ACS deletes the administrator account. The Administrators list on the Administration Control page no longer contains the administrator account.
-

# Configuring Policy Options

The options on these pages control access, session, and password policies.

This section contains the following options:

- [Configuring Access Policy, page 11-8](#)
- [Configuring Session Policy, page 11-8](#)
- [Configuring Password Policy, page 11-9](#)

## Configuring Access Policy

If you have the Administration Control privilege, you can use the Access Policy feature to limit access by IP address and by the TCP port range used for administrative sessions. You can also enable the secure socket layer (SSL) for access to the web interface.

### Before You Begin

If you want to enable the SSL for administrator access, you must have completed the steps in [Installing an ACS Server Certificate, page 9-22](#), and [Adding a Certificate Authority Certificate, page 9-26](#). After you have enabled SSL, ACS begins using the SSL at the next administrator login. This change does not affect current administrator sessions. In the absence of a certificate, ACS displays an error message when you attempt to configure SSL.

To set up an ACS Access Policy:

- 
- Step 1** In the navigation bar, click **Administration Control**.  
ACS displays the Administration Control page.
  - Step 2** Click **Access Policy**.  
The Access Policy Setup page appears.
  - Step 3** Click the appropriate **IP Address Filtering** option. For information on these options, see [Access Policy Setup Page, page 11-18](#).
  - Step 4** Type the appropriate IP address ranges in accordance with the IP Address Filtering option.
  - Step 5** Click the appropriate HTTP Port Allocation option to allow all ports or restrict access to certain ports. If you restrict access, type the range of the restricted ports. For information on these options, see [Access Policy Setup Page, page 11-18](#).
  - Step 6** Check this option if you want ACS to use the SSL. For information on this option, see [Access Policy Setup Page, page 11-18](#).
  - Step 7** Click **Submit**.  
ACS saves and begins enforcing the access policy settings.
- 

## Configuring Session Policy

If you have the Administration Control privilege, you can use the Session Policy controls that enable or disable:

- Local logins
- Responses to invalid IP address connections

To set up ACS session policy:

- 
- Step 1** In the navigation bar, click **Administration Control**.  
ACS displays the Administration Control page.
- Step 2** Click **Session Policy**.  
The Session Policy Setup page appears.
- Step 3** Click the appropriate policies and type the appropriate information to set up the policy. For information on these options and fields, see [Session Policy Setup Page, page 11-20](#).
- Step 4** Click **Submit**.  
ACS saves and begins enforcing the session policy settings.
- 

## Configuring Password Policy

You can access the Administrator Password Policy page from the Password Policy button on the Add Administrator page. If you do not configure the password policy, any administrator can log in, create administrators, and assign privileges.

The Administrator Password Policy provides controls that:

- Constrain complexity
- Restrict lifetime
- Restrict inactive accounts
- Limit incorrect login attempts

To set up a password policy:

- 
- Step 1** In the navigation bar, click **Administration Control**.  
ACS displays the Administration Control page.
- Step 2** Click **Password Policy**.  
The Administrator Password Policy page appears.
- Step 3** Click the appropriate options and type the appropriate values. For information on these options and fields, see [Administrator Password Policy Page, page 11-16](#).
- Step 4** Click **Submit**.  
ACS saves and begins enforcing the password policy settings at the next login.
-

# Administration Control Pages Reference

The following topics describe the pages accessed from the **Administration Control** button on the navigation bar:

- [Administration Control Page, page 11-10](#)
- [Add Administrator and Edit Administrator Pages, page 11-11](#)
- [Administrator Password Policy Page, page 11-16](#)
- [Access Policy Setup Page, page 11-18](#)
- [Session Policy Setup Page, page 11-20](#)

## Administration Control Page

The Administration Control page is the starting point for configuring administrator accounts and policies. Only administrators with the Administration Control privilege can access this page.

To open this page, click the **Administration Control** button in the navigation bar.

**Table 11-2 Administration Control (Privileged Administrator)**

Option	Description
Administrators	Lists all configured administrators.
<administrator_name>	Opens the Edit Administrator <administrator_name> page. For information, see the <a href="#">Add Administrator and Edit Administrator Pages, page 11-11</a> .
Add Administrator	Opens the Add Administrator page. For information, see the <a href="#">Add Administrator and Edit Administrator Pages, page 11-11</a> .
Access Policy	Opens the Access Policy Setup page, which controls network access for browsers. For information, see the <a href="#">Administrator Password Policy Page, page 11-16</a> .
Session Policy	Opens the Session Policy Setup page, which provides configuration details for HTTP sessions. For information, see the <a href="#">Session Policy Setup Page, page 11-20</a> .
Password Policy	Opens the Administrator Password Policy page. For information, see the <a href="#">Administrator Password Policy Page, page 11-16</a> .

### Related Topics

- [Adding or Editing Accounts, page 11-6](#)
- [Deleting an Account, page 11-7](#)
- [Configuring Access Policy, page 11-8](#)
- [Configuring Session Policy, page 11-8](#)
- [Configuring Password Policy, page 11-9](#)

## Add Administrator and Edit Administrator Pages

Use the areas on the Add Administrator and Edit Administrator pages to:

- Add an administrator (Add Administrator page only)
- Add, edit, and monitor passwords
- Monitor and re-enable locked out accounts
- Enable or disable privileges

To open these pages, click **Administration Control**, and then click **Add Administrator** or click `<administrator_name>` to edit an administrator.

Table 11-3 describes the following options:

- [Administrator Details, page 11-11](#)
- [Administrator Privileges, page 11-12](#)
- [User & Group Setup, page 11-12](#)
- [Shared Profile Components, page 11-13](#)
- [Network Configuration, page 11-14](#)
- [System Configuration, page 11-14](#)
- [Interface Configuration, page 11-15](#)
- [Administration Control, page 11-15](#)
- [External User Databases, page 11-15](#)
- [Posture Validation, page 11-15](#)
- [Network Access Profiles, page 11-15](#)
- [Reports & Activity, page 11-15](#)

**Table 11-3** Add Administrator and Edit Administrator Pages

Option	Description
<b>Administrator Details</b>	
Administrator Name (appears only on the Add Administrator page)	<p>The login name for the ACS administrator account. Administrator names can contain 1 to 32 characters, excluding the left angle bracket (&lt;), the right angle bracket (&gt;), and the backslash (\). An ACS administrator name does not have to match a network user name.</p> <p>The administrator name does not appear on the Edit Administrator page because ACS does not allow name changes for previously configured administrators. To change names, delete the account and configure an account with a new name. To disable an account, revoke all privileges.</p>
Password	<p>The password can match the password that the administrator uses for dial-in authentication, or it can be a different password. ACS enforces the options in the Password Validation Options section on the Administrator Password Policy page.</p> <p>Passwords must be at least four characters long and contain at least one numeric character. The password cannot include the username or the reverse username, must not match any of the previous four passwords. and must be in ASCII characters. For errors in passwords, ACS displays the password criteria.</p> <p>If the password policy changes and the password does not change, the administrator remains logged in. ACS enforces the new password policy at the next login.</p>

Table 11-3 Add Administrator and Edit Administrator Pages (continued)

Option	Description
Confirm Password	Verifies the password in the Password field. For errors in password typing, ACS displays an error message.
Last Password Change (Edit Administrator page only)	Displays the date of the change on which a password changes through administrative action on this page or through expiration of a password during login. (Read-only) Always displays the change date, not the expiration date. Does not appear until a new account has been submitted.
Last Activity (Edit Administrator page only)	Displays the date of the last successful login. (Read-only) Does not appear until a new account has been submitted.
Account Never Expires	Prevents account lockout by overriding the lockout options on the Administrator Password Policy page with the exception of manual lockout. Therefore, the account never expires but password change policy remains in effect. The default value is unchecked (disabled).
Account Locked	<p>Prevents an administrator, who was locked out due to the lockout options on the Password Policy page, from logging in. When unchecked (disabled), this option unlocks an administrator who was locked out.</p> <p>Administrators who have the Administration Control privilege can use this option to manually lock out an account or reset locked accounts. The system displays a message that explains the reason for a lockout.</p> <p>When an administrator unlocks an account, ACS resets the Last Password Change and the Last Activity fields to the day on which the administrator unlocks the account.</p> <p>The reset of a locked account does not affect the configuration of the lockout and unlock mechanisms for failed attempts.</p>
<b>Administrator Privileges</b>	<p>Contains the privilege options for the User Setup and Group Setup sections of the web interface.</p> <p>By default, a remote administrator does not have privileges.</p>
Grant All	<p>Enables all privileges. ACS moves all user groups to the Editable Groups list. A privileged administrator can also grant privileges to each ACS administrator by assigning privileges on an individual basis. In either case, the administrator can individually override options enabled by Grant All.</p> <p>By default, ACS restricts all privileges for new administrator accounts.</p>
Revoke All	<p>Clears (restricts) all privileges. ACS removes all user groups from the Editable Groups list. Revoking all privileges for an existing account effectively disables the account. The administrator can individually override options disabled by Revoke All.</p> <p>You can also disable an account by revoking all privileges.</p>
<b>User &amp; Group Setup</b>	
Add/Edit users in these groups	<p>Enables an administrator to add or edit users, and to assign users to the groups in the Editable groups list.</p> <p>When enabled, this setting overrides the settings in the Read access to users in these groups option.</p>
Setup of these groups	<p>Enables an administrator to edit the settings for the groups in the Editable groups list.</p> <p>When enabled, this setting overrides the settings in the Read access of these groups option.</p>

Table 11-3 Add Administrator and Edit Administrator Pages (continued)

Option	Description
Read access to users in these groups	<p>Enables read-only access to users in the Editable groups.</p> <p>When the Add/Edit users in these groups option is enabled, it overrides the settings in the Read access to users in these groups option.</p> <p>If the Add/Edit users in these groups option is checked (enabled), it does not matter if this setting is enabled or disabled. The Add/Edit users in these groups setting overrides this setting, and the administrator can edit all users in the Editable groups.</p> <p>If the Add/Edit users in these groups option is unchecked (disabled):</p> <ul style="list-style-type: none"> <li>• Check this check box to grant the administrator read access to the users in the Editable groups. In this case, the administrator cannot submit changes.</li> <li>• When unchecked, administrators cannot view users.</li> </ul>
Read access of these groups	<p>Enables read-only access to users in the Editable groups.</p> <p>When the Add/Edit users in these groups option is enabled, it overrides the settings in the Read access to users in these groups option.</p> <p>If the Add/Edit users in these groups option is checked (enabled), it does not matter if this setting is enabled or disabled. The Add/Edit users in these groups setting overrides this setting, and the administrator can edit the Editable groups.</p> <p>If the Add/Edit users in these groups option is unchecked (disabled):</p> <ul style="list-style-type: none"> <li>• Check this check box to grant the administrator read access to the Editable groups list. In this case, the administrator cannot submit changes.</li> <li>• When unchecked, administrators cannot view groups.</li> </ul>
Available groups	Lists all user groups. Administrators do not have access to the groups in this list.
Editable groups	<p>Lists the user groups to which administrators have access. Other options in the User &amp; Group Setup area determine the limits on administrator access to these groups and associated users in this list.</p> <p>Click &gt;&gt; to add all groups, or click &lt;&lt; to remove all groups. Click &gt; to add a single group, or click &lt; to remove a single group.</p> <p><b>Note</b> The access settings in this section do not apply to group mappings for external authenticators.</p>
<b>Shared Profile Components</b>	
Network Access Restriction Sets	Enables full access to the Network Access Restriction Sets feature.
Network Access Filtering Sets	Enables full access to the Network Access Filtering Sets feature.
Downloadable ACLs	Enables full access to the Downloadable PIX ACLs feature.
RADIUS Authorization Components	Enables full access to RACs.
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 ACS by using this privilege appear in the Shared Profile Components section of the web interface.

Table 11-3 Add Administrator and Edit Administrator Pages (continued)

Option	Description
Shell Command Authorization Sets	Enables full access to the Shell Command Authorization Sets feature.
PIX/ASA Command Authorization Sets	Enables full access to the PIX/ASA Command Authorization Sets feature. <b>Note</b> Additional command authorization set privilege options can appear if other Cisco network management applications, such as CiscoWorks, have updated the configuration of ACS.
<b>Network Configuration</b>	Enables full access to the features in the Network Configuration section of the web interface.
<b>System Configuration</b>	Contains the privilege options for the features in the System Configuration section of the web interface. For each of the features, enabling the option grants full access to the feature.
Service Control	Enables access to configuration of the service log files, and stop and restart of ACS services.
Date/Time Format Control	Enables access to control of date formats.
Logging Control	Enables access to report options associated with the Logging Configuration page. To access the Logging Configuration page, click <b>System Configuration</b> , then click <b>Logging</b> .
Administration Audit Configuration	Enables this administrator to change the Administration Audit report configuration.
Password Change Configuration	Enables this administrator to change the Password Change report configuration.
Password Validation	Enables access to validation parameters for user passwords.
DB Replication	Enables access to ACS internal database replication.
RDBMS Synchronization	Enables access to RDBMS synchronization.
IP Pool Address Recovery	Enables access to IP pool address recovery.
IP Pool Server Configuration	Enables access to the configuration of IP pools.
ACS Backup	Enables access to ACS backup.
ACS Restore	Enables access to ACS restore.
ACS Service Management	Enables access to system monitoring and event logging.
VoIP Accounting Configuration	Enables access to the VoIP accounting configuration.
ACS Certificate Setup	Enables access to ACS certificate setup.
Global Authentication Setup	Grants privilege for global authentication setup. Any administrator who requires access to the EAP-FAST Files Generation configuration page must have the Global Authentication Setup privilege enabled.
EAP-FAST PAC Files Generation (ACS SE)	Enable generation of PAC files for use with EAP-FAST authentication.
NAC Attributes management (ACS SE)	Enables access to NAC attribute management.
<b>Appliance Configuration</b> (ACS SE)	Enables access to appliance configuration.
<b>Support Operations</b> (ACS SE)	Enables access to support operations.

Table 11-3 Add Administrator and Edit Administrator Pages (continued)

Option	Description
<b>View Diagnostic Logs</b> (ACS SE)	Enables access to diagnostic logs.
<b>Appliance Upgrade Status</b> (ACS SE)	Enables access to appliance upgrade status reports.
<b>Interface Configuration</b>	Enables full access to the features in the Interface Configuration section of the web interface.
<b>Administration Control</b>	Enables full access to the features in the Administration Control section of the web interface.
<b>External User Databases</b>	Enables full access to the features in the External User Databases section of the web interface.
<b>Posture Validation</b>	Enables access to Network Admission Control (NAC) configuration.
<b>Network Access Profiles</b>	Enables access to service-based policy configuration by using NAPs.
<b>Reports &amp; Activity</b>	Click the <b>Reports and Activities</b> button in the navigation bar to access these logs.
TACACS+ Accounting	Enables access to the TACACS+ Accounting log, which includes TACACS+ session information.
TACACS+ Administration	Enables access to the TACACS+ Administration log, which lists configuration commands.
RADIUS Accounting	Enables access to the RADIUS Accounting log, which includes RADIUS session information.
VoIP Accounting	Enables access to the VoIP Accounting log, which includes VoIP session information.
Passed Authentications	Enables access to the Passed Authentications log, which lists successful authentication requests.
Failed Attempts	Enables access to the Failed Attempts log, which lists authentication and authorization failures.
Logged-in Users	Enables access to the Logged-in Users log, which lists all users that receive services from AAA clients.
Purge of Logged-in Users	If users are listed as logged in but the connection to the AAA client has been lost and the users are no longer actually logged in, click Purge and that session's activity will be terminated. Purging the user from this list does not log the user off the AAA client, but terminates the session record in accounting. To print this list, right-click anywhere in the right window and print the window from the browser.
Disabled Accounts	Enables access to the Disabled Accounts log, which lists all disabled user accounts.
ACS Backup and Restore	Enables access to the ACS Backup and Restore log, which lists backup and restore activity.
DB Replication	Enables access to the Database Replication log, which lists database replication activity.
RDBMS Synchronization	Enables access to the RDBMS Synchronization log, which lists RDBMS synchronization activity.
Administration Audit	Enables access to the Administration Audit log, which lists system administrator actions.
ACS Service Monitor	Enables access to the ACS Service Monitoring log, which lists ACS service starts and stops.
User Change Password	Enables access to the User Password Changes log, which lists user-initiated password changes.
Entitlement Reports	Enables access to reports of user and administrator entitlements.

Table 11-3 Add Administrator and Edit Administrator Pages (continued)

Option	Description
Appliance Status (ACS SE)	Enables access to the Appliance Status log, which logs resource utilization.
Appliance Administration Audit (ACS SE)	Enables access to the Appliance Administration Audit log, which lists activity on the serial console.

**Related Topics**

- [Service Control, page 7-1](#)
- [Date and Time Format Control, page 7-3](#)
- [Local Password Management, page 7-4](#)
- [ACS Backup, page 7-8](#)
- [ACS System Restore, page 7-14](#)
- [ACS Active Service Management, page 7-18](#)
- [VoIP Accounting Configuration, page 7-21](#)
- [Appliance Configuration \(ACS SE Only\), page 7-22](#)
- [Support Page, page 7-25](#)
- [Viewing or Downloading Diagnostic Logs \(ACS SE Only\), page 7-27](#)
- [ACS Internal Database Replication, page 8-1](#)
- [RDBMS Synchronization, page 8-17](#)
- [IP Pools Server, page 8-39](#)
- [IP Pools Address Recovery, page 8-44](#)
- [Global Authentication Setup, page 9-21](#)
- [ACS Certificate Setup, page 9-22](#)
- [NAC Attribute Management \(ACS SE Only\), page 8-44](#)
- [Appliance Configuration \(ACS SE Only\), page 7-22](#)
- [About ACS Logs and Reports, page 10-1](#)
- [Password Expirations and Account Lockouts, page 11-3](#)
- [Adding, Editing, and Deleting Accounts, page 11-6](#)

## Administrator Password Policy Page

Use the Administrator Password Policy page to set password validation, lifetime, inactivity, and incorrect attempt options. If you do not configure the password policy, any administrator can log in, create administrators, and assign privileges.

To open this page, click **Administration Control** and then click **Password Policy**.

ACS returns an error when:

- The specification is out of range.

- Users do not meet the criteria on this page.

Table 11-4 describes the following options:

- [Password Validation Options](#), page 11-17
- [Password Lifetime Options](#), page 11-17
- [Password Inactivity Options](#), page 11-17
- [Incorrect Password Attempt Options](#), page 11-18

**Table 11-4 Administrator Password Policy**

Option	Description
<b>Password Validation Options</b>	
Password may not contain the username	If enabled, the password cannot contain the username or the reverse username.
Minimum length $n$ characters	$n$ specifies the minimum length of the password (the default is 4, the range is 4 to 20).
Password must contain:	Use these options to determine password complexity constraints.
upper case alphabetic characters	If enabled, the password must contain uppercase alphabetic characters.
lower case alphabetic characters	If enabled, the password must contain lowercase alphabetic characters.
numeric characters	If enabled, the password must contain numeric characters.
non alphanumeric characters	If enabled, the password must contain nonalphanumeric characters (for example, @).
Password must be different from the previous $n$ versions	If enabled, the password must be different from the previous $n$ versions (the default is 1, the range is 1 to 99).
<b>Password Lifetime Options</b>	
Following a change of password:	Use these options to set restrictions on the lifetime of administrator passwords. The value $n$ represents the number of days that passed since the last time the password was changed.
The password will require change after $n$ days	Following a change of password, if enabled, $n$ specifies the number of days before ACS requires a change of password due to password age (the default is 30). The range is 1 to 365. When checked (enabled), The Administrator will be locked after $n$ days option, causes ACS to compare the two Password Lifetime Options and take the greater value.
The Administrator will be locked out after $n$ days	Following a change of password, if enabled, $n$ specifies the number of days before ACS locks out the associated administrator account due to password age (the default is 60, the range is 1 to 365).
<b>Password Inactivity Options</b>	
Following last account activity:	Use these options to place restrictions on the use of inactive administrator accounts. The value $n$ represents the number of days that passed since the activity (administrator login).

Table 11-4 Administrator Password Policy (continued)

Option	Description
The password will require change after $n$ days	<p>Following the last account activity, if enabled, <math>n</math> specifies the number of days before ACS requires a change of password due to password inactivity (the default is 30). The range is 1 to 365. When checked (enabled), The Administrator will be locked after <math>n</math> days option causes ACS to compare the two Password Inactivity Options and take the greater value.</p> <p><b>Note</b> For additional security, ACS does not warn users who are approaching the limit for password inactivity.</p>
The Administrator will be locked out after $n$ days	<p>Following the last account activity, if enabled, <math>n</math> specifies the number of days before ACS locks out the associated administrator account due to password inactivity (the default is 60, the range is 1 to 365).</p> <p><b>Note</b> For additional security, ACS does not warn users who are approaching the limit for account inactivity.</p>
<b>Incorrect Password Attempt Options</b>	
Lock out Administrator after $n$ successive failed attempts	<p><b>If enabled, <math>n</math> specifies the allowable number of incorrect password attempts. When checked, <math>n</math> cannot be set to zero. If disabled (not checked), ACS allows unlimited successive failed login attempts (the default is 3, the range is 1 to 98).</b></p> <p><b>Note</b> For additional security, ACS does not warn users who are approaching the limit for failed attempts. If the <b>Account Never Expires</b> option is enabled for a specific administrator, this option is ignored.</p>

## Access Policy Setup Page

Use the Access Policy Setup page to configure access for IP addresses and ranges, to configure HTTP access, and to set up the Secure Sockets Layer (SSL).

To open the Access Policy Setup page, click **Administration Control**, and then click **Access Policy**.

Table 11-5 describes the following options:

- [IP Address Filtering, page 11-18](#)
- [IP Address Ranges, page 11-19](#)
- [HTTP Configuration, page 11-19](#)
- [Secure Socket Layer Setup, page 11-20](#)

Table 11-5 Access Policy Options

Option	Description
<b>IP Address Filtering</b>	
Allow all IP addresses to connect	Enables remote access to the web interface from any IP address.
Allow only listed IP addresses to connect	Restricts remote access to the web interface to IP addresses within the specified IP Address Ranges.

Table 11-5 Access Policy Options (continued)

Option	Description
Reject connections from listed IP addresses	<p>Restricts remote access to the web interface to IP addresses outside of the specified IP Address Ranges.</p> <p>IP filtering operates on the IP address received in an HTTP request from a remote administrator's web browser. If the browser is configured to use an HTTP proxy server or the browser runs on a workstation behind a network device performing network address translation, IP filtering applies only to the IP address of the HTTP proxy server or the NAT device.</p>
<b>IP Address Ranges</b>	<p>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.</p> <p>Use dotted-decimal format. The IP addresses that define a range must differ only in the last octet (Class C format).</p>
Start IP Address	Defines the lowest included IP address in the specified range (up to 16 characters).
End IP Address	Defines the highest included IP address in the specified range (up to 16 characters).
<b>HTTP Configuration</b>	
<b>HTTP Port Allocation</b>	
Allow any TCP ports to be used for Administration HTTP Access	Enables ACS to use any valid TCP port for remote access to the web interface.
Restrict Administration Sessions to the following port range From Port <i>n</i> to Port <i>n</i>	<p>Restricts the ports that ACS can use for remote access to the web interface. Use the boxes to specify the port range (up to five digits per box). The range is always inclusive; that is, the range includes the start and end port numbers. The size of the specified range determines the maximum number of concurrent administrative sessions.</p> <p>ACS uses port 2002 to start all administrative sessions. Port 2002 does not need to be in the port range. Also, ACS does not allow definition of an HTTP port range that consists only of port 2002. The port range must consist of at least one port other than port 2002.</p> <p>A firewall configured to permit HTTP traffic over the ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port that a web browser must address to initiate an administrative session.</p> <p>We do not recommend allowing administration of ACS from outside a firewall. If access to the web interface from outside a firewall is necessary, keep the HTTP port range as narrow as possible. A narrow range can help to 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.</p>

Table 11-5 Access Policy Options (continued)

Option	Description
<b>Secure Socket Layer Setup</b>	
Use HTTPS Transport for Administration Access	<p>Enables ACS to use the secure socket layer (SSL) protocol to encrypt HTTP traffic between the <b>CSAdmin</b> service and the web browser that accesses the web interface. This option enables encryption of all HTTP traffic between the browser and ACS, as reflected by the URLs, that begin with HTTPS. Most browsers include an indicator for SSL-encrypted connections.</p> <p>To enable SSL, first install an a server certificate and a certification authority certificate. Choose <b>System Configuration &gt; ACS Certificate Setup</b> to access the installation process. With SSL enabled, ACS begins using HTTPS at the next administrator login. Current administrator sessions are unaffected. In the absence of a certificate, ACS displays an error.</p>

**Related Topics**

- [Installing an ACS Server Certificate, page 9-22](#)
- [Adding a Certificate Authority Certificate, page 9-26](#)

## Session Policy Setup Page

Use the Session Policy Setup page to configure session attributes that include timeout, automatic local logins (ACS for Windows only), and response to invalid IP address connections.

To open this page, click **Administration Control**, and then click **Session Policy**.

[Table 11-6](#) describes the session configuration options.

Table 11-6 Session Policy

Option	Description
<b>Session Configuration</b>	
Session idle timeout (minutes)	<p>Specifies the time, in minutes, that an administrative session must remain idle before ACS terminates the connection (four-digit maximum, 5 to 1439).</p> <p>When an administrative session terminates, ACS displays a dialog box asking whether the administrator wants to continue. If the administrator chooses to continue, ACS starts a new administrative session.</p> <p>This parameter only applies to the ACS administrative session in the browser. It does not apply to an administrative dial-up session.</p>

Table 11-6 Session Policy (continued)

Option	Description
<p><b>Allow Automatic Local Login</b> (ACS for Windows)</p>	<p>Enables administrators to start an administrative session without logging in, if they are using a browser on the computer that runs ACS. ACS uses a default administrator account named <code>local_login</code> to <i>conduct these sessions</i>.</p> <p>When unchecked (disabled), administrators must log in using administrator names and passwords.</p> <p><b>Note</b> To prevent accidental lockout when there are no defined administrator accounts, ACS does not require an administrator name and password for local access to ACS.</p> <p>The <code>local_login</code> administrator account requires the Administration Control privilege. ACS records administrative sessions that use the <code>local_login</code> account in the Administrative Audit report under the <code>local_login</code> administrator name.</p>
<p>Respond to invalid IP address connections</p>	<p>Enables ACS to send an error message in response to attempts to start a remote administrative session by using an IP address that is invalid according to the IP address Range settings in the Access Policy. If this check box is clear, ACS does not display an error message when an invalid remote connection attempt is made. (the default is Enabled)</p> <p>Disabling this option can help to prevent unauthorized users from discovering ACS.</p>

