



CHAPTER 5

Password Policy Configuration Scenario

Cisco Secure ACS, hereafter referred to as ACS, provides new password features to support corporate requirements mandated by the Sarbanes-Oxley Act of 2002. Sarbanes-Oxley (SOX) requires stricter enforcement of password restrictions.

ACS provides SOX support, which includes:

- Enforcement of password lifetime policy
- Enforcement of inactivity limits
- Improved password constraints

To enable password configuration that includes these new features, ACS provides a new password policy page.

All administrator logins are subject to the policy that you configure for passwords and accounts, unless you check the Account Never Expires check box. For example, ACS provides configurable limits on password lifetime and 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.

Limitation on Ability of the Administrator to Change Passwords

If an administrator is not granted full administrative access, the only action the administrator can take is to change his or her own password.

Summary of Configuration Steps

To configure password policy in ACS:

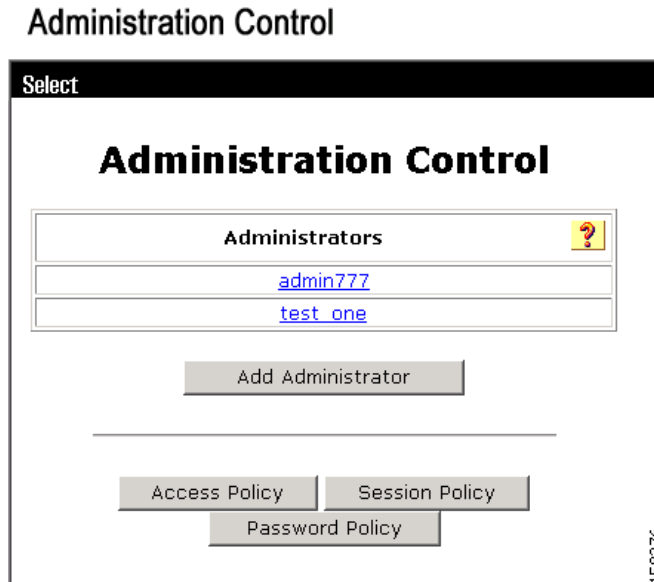
-
- Step 1** Add a new administrator account.
Add a new administrator account, specify the administrator name and password, and grant access privileges. See [Step 1: Add and Edit a New Administrator Account, page 5-2](#) for details.
- Step 2** Configure password policy.
Configure restrictions on the admin user password. See [Step 2: Configure Password Policy, page 5-4](#) for details.
- Step 3** Configure session policy.
Configure restrictions on the admin user's session. See [Step 3: Configure Session Policy, page 5-7](#) for details.
- Step 4** Configure access policy.
Configure restrictions on admin access, such as the IP addresses from which administrators can log in. See [Step 4: Configure Access Policy, page 5-9](#) for details.
-

Step 1: Add and Edit a New Administrator Account

To add a new administrator account:

-
- Step 1** In the navigation bar, click **Administration Control**.
The Administration Control page appears, as shown in [Figure 5-1](#).

Figure 5-1 Administration Control Page



The Administration Control page initially lists no administrators. If administrators have been configured, the page lists the configured administrators.

Step 2 To add an administrator, click **Add Administrator**.

The Add Administrator page opens.

Step 3 In the Administrator Details area, enter:

Option	Description
Administrator Name	Enter the login name for the ACS administrator account. Administrator names can contain 1 to 32 characters, excluding the left angle bracket (<), the right angle bracket (>), and the backslash (\). An ACS administrator name does not have to match a network user name.
Password	<p>Enter the password for the administrator to access the ACS web interface.</p> <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 4 characters long and contain at least 1 numeric character. The password cannot include the username or the reverse username, must not match any of the previous 4 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>
Confirm Password	Reenter the password that you entered in the password field.

Option	Description
Account Never Expires	If you want to override the lockout options set up on the Administrator Password Policy page (with the exception of manual lockout), check the check box next to Account Never Expires. If you check this option, the account never expires but password change policy remains in effect. The default value is unchecked (disabled).
Account Locked	<p>If you want to lock out an administrator who is denied access due to the account policy options specified on the Password Policy page, check the check box for Account Locked. 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>

Step 4 Click **Grant All** or **Revoke All** to globally add or remove all privileges,

Step 5 If you want to grant specific privileges to the administrator, check the check boxes that correspond to the privileges that you want to grant.



Note For more information on administrative privileges, see the “Add Administrator and Edit Administrator Pages” section in Chapter 11 of the *User Guide for Cisco Secure Access Control Server 4.2*, “Administrators and Administrative Policy.”

Step 6 Go to [Step 2: Configure Password Policy, page 5-4](#) (the next section of this chapter) and follow the steps to specify password restrictions.


Step 2: Configure Password Policy


To configure password policy:


Step 1 On the Administration Control page, click **Password Policy**.
The Administrator Password Policy Setup page appears, shown in [Figure 5-2](#).


Figure 5-2 The Administrator Password Policy Setup Page

Administrator Password Policy Setup

Password Validation Options 	
<input type="checkbox"/>	Password may not contain the username
Minimum length	<input type="text" value="4"/> characters
Password must contain:	
<input type="checkbox"/>	lower case alphabetic characters
<input type="checkbox"/>	upper case alphabetic characters
<input type="checkbox"/>	numeric characters
<input type="checkbox"/>	non alphanumeric characters
<hr/>	
<input type="checkbox"/>	Password must be different from the previous:
<input type="text" value="10"/>	versions

Password Lifetime Options 	
Following a change of password:	
<input type="checkbox"/>	The password will require change after <input type="text" value="30"/> days
<input type="checkbox"/>	The Administrator will be locked out after <input type="text" value="60"/> days

Password Inactivity Options 	
Following last account activity:	
<input type="checkbox"/>	The password will require change after <input type="text" value="30"/> days
<input type="checkbox"/>	The Administrator will be locked out after <input type="text" value="60"/> days

Incorrect Password Attempt Options 	
<input type="checkbox"/>	Lock out Administrator after <input type="text" value="3"/> successive failed attempts

158377

- Step 2** On the Password Policy Setup Page, specify:
- Password Validation Options
See [Specify Password Validation Options, page 5-6](#).
 - Password Lifetime Options
See [Specify Password Lifetime Options, page 5-6](#).
 - Password Inactivity Options
See [Specify Password Inactivity Options, page 5-7](#).
 - Incorrect Password Attempt Option
See [Specify Incorrect Password Attempt Options, page 5-7](#).
-

Specify Password Validation Options

In the Password Validation Options section, configure:

- **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 (default = 4, range = 4 to 20).
- **Uppercase alphabetic characters**—If enabled, the password must contain uppercase alphabetic characters.
- **Lowercase 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, the at symbol (@).
- **Password must be different from the previous n versions**—If enabled, the password must be different from the previous n versions (default = 10, range = 0 to 99).

Specify Password Lifetime Options

In the Password Lifetime Options section, configure:

- **The password will require change after n days**—Following a change of password, if this option is enabled, n specifies the number of days before ACS requires a change of password due to password age (the default value is 30 days). 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 use the greater value of the two.
- **The Administrator will be locked out after n days**—Following a change of password, if this option is enabled, n specifies the number of days before ACS locks out the associated administrator account due to password age. The default value is 30 days; the range is 1 to 365 days.

Specify Password Inactivity Options

In the Password Inactivity Options section, configure:

- **The password will require change after n days**—Following the last account activity, if enabled, n specifies the number of days before ACS requires a change of password due to password inactivity. The default value is 30 days; the range is 1 to 365 days. When checked (enabled), the Administrator will be locked after n days option causes ACS to compare the two Password Inactivity Options and use the greater value of the two.

**Note**

For additional security, ACS does not warn users who are approaching the limit for password inactivity.

- **The Administrator will be locked out after n days**—Following the last account activity, if enabled, n specifies the number of days before ACS locks out the associated administrator account due to password inactivity (default = 30, range = 1 to 365).

**Note**

For additional security, ACS does not warn users who are approaching the limit for account inactivity.

Specify Incorrect Password Attempt Options

In the Incorrect Password Attempt Options section, configure:

Lock out Administrator after n successive failed attempts—If checked (enabled), n specifies the allowable number of incorrect password attempts. When checked, n cannot be set to zero (0). If not checked (disabled), ACS allows unlimited successive failed login attempts. The default value is 3 days; the range = 1 to 98 days.

**Note**

For additional security, ACS does not warn users who are approaching the limit for failed attempts. If the **Account Never Expires** option is checked (enabled) for a specific administrator, this option is ignored.

Step 3: Configure Session Policy

To configure session policy:

- Step 1** On the Administration Control page, click **Session Policy**.
The Session Policy Setup page opens, as shown in [Figure 5-3](#).

Figure 5-3 The Session Policy Setup Page

Session Policy Setup

Session Configuration ?

Session idle timeout (minutes)

Allow automatic local login

Respond to invalid IP address connections

158387

Step 2 On the Session Policy Setup page, set session options as required.

You can specify:

- **Session idle timeout (minutes)**—Specifies the time, in minutes, that an administrative session must remain idle before ACS terminates the connection (4-character maximum).

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.

This parameter only applies to the ACS administrative session in the browser. It does not apply to an administrative dial-up session.

- **Allow Automatic Local Login (ACS for Windows Only)**—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 *local_login* to conduct these sessions.

When unchecked (disabled), administrators must log in by using administrator names and passwords.



Note

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.

The *local_login* administrator account requires the Administration Control privilege. ACS records administrative sessions that use the *local_login* account in the Administrative Audit report under the *local_login* administrator name.

- **Respond to invalid IP address connections**—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 unchecked, ACS does not display an error message when a user makes an invalid remote connection attempt. This option is checked (enabled) by default.

Disabling this option can help to prevent unauthorized users from discovering ACS.

Step 4: Configure Access Policy

This section describes how to configure administrative access policy.

Before You Begin

If you want to enable the SSL for administrator access, you must have completed the steps in [Install the CA Certificate, page 7-4](#), and [Add a Trusted Certificate, page 7-4](#). 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, as shown in [Figure 5-4](#).

Figure 5-4 Access Policy Setup Page

IP Address Filtering

Allow all IP addresses to connect

Allow only listed IP addresses to connect

Reject connections from listed IP addresses

IP Address Ranges

	Start IP Address	End IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>

HTTP Configuration

HTTP Port Allocation

Allow any TCP ports to be used for Administration HTTP Access

Restrict Administration Sessions to the following port range From Port to Port

Secure Socket Layer Setup

Use HTTPS Transport for Administration Access

Back to Help

210086

Step 3 Click the appropriate **IP Address Filtering** option

Table 5-1 Access Policy Options

Option	Description
IP Address Filtering	
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 5-1 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>
IP Address Ranges	<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).
HTTP Configuration	
HTTP Port Allocation	
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 5-1 Access Policy Options (continued)

Option	Description
Secure Socket Layer Setup	
Use HTTPS Transport for Administration Access	<p>Enables ACS to use the secure socket layer (SSL) protocol to encrypt HTTP traffic between the CSAdmin 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 System Configuration > ACS Certificate Setup 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>

- 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.
- Step 6** Check this option if you want ACS to use the SSL.
- Step 7** Click **Submit**.
ACS saves and begins enforcing the access policy settings.

Viewing Administrator Entitlement Reports

To assist in SOX compliance, ACS produces entitlement report, which contain data extracted from the ACS configuration and formatted into text based files.

ACS produces entitlement reports for administrators and users. The reports that you can generate are:

- **Privilege**—The privileges granted to a selected administrator.
- **Combined Privilege**—The privileges granted to all administrators.
- **Users to Groups Mapping**—The group membership of every user.

View Privilege Reports

To view privilege reports:

-
- Step 1** In the navigation bar, click **Reports and Activity**.
The Reports page opens.
- Step 2** Click **Entitlement Reports**.
A list of the available entitlement reports appears. [Figure 5-5](#) shows an example list.

Figure 5-5 *List of Entitlement Reports*

User Entitlement Reports
Download Report for mapping of Users to Groups

Administrator Entitlement Reports
Download Privilege Report for All Administrators
Privilege Report for admin777
Privilege Report for test_one

158379

- Step 3** To view a report, click the report name.
Each report is downloaded to the local computer in the form of an Excel spreadsheet.
-

