CHAPTER 1

Managing System Administrators

System administrators are responsible for deploying, configuring, maintaining, and monitoring the ACS servers in your network. They can perform various operations in ACS through the ACS administrative interface. When you define an administrator in ACS, you assign a password and a role or set of roles that determine the access privilege the administrator has for the various operations.

When you create an administrator account, you initially assign a password, which the administrator can subsequently change through the ACS web interface. Irrespective of the roles that are assigned, the administrators can change their own passwords.

ACS provides the following configurable options to manage administrator passwords:

- Password Complexity—Required length and character types for passwords.
- Password History—Prevents repeated use of same passwords.
- Password Lifetime—Forces the administrators to change passwords after a specified time period.
- Account Inactivity—Disables the administrator account if it has not been in use for a specified time period.
- Password Failures—Disables the administrator account after a specified number of consecutive failed login attempts.

In addition, ACS provides you configurable options that determine the IP addresses from which administrators can access the ACS administrative web interface and the session duration after which idle sessions are logged out from the system.

You can use the Monitoring and Report Viewer to monitor administrator access to the system. The Administrator Access report is used to monitor the administrators who are currently accessing or attempting to access the system.

You can view the Administrator Entitlement report to view the access privileges that the administrators have, the configuration changes that are done by administrators, and the administrator access details. In addition, you can use the Configuration Change and Operational Audit reports to view details of specific operations that each of the administrators perform.

The System Administrator section of the ACS web interface allows you to:

- Create, edit, duplicate, or delete administrator accounts
- Change the password of other administrators
- View predefined roles
- Associate roles to administrators
- Configure authentication settings that include password complexity, account lifetime, and account inactivity

- Configure administrator session setting
- Configure administrator access setting

The first time you log in to ACS 5.4, you are prompted for the predefined administrator username (*ACSAdmin*) and required to change the predefined password name (*default*). After you change the password, you can start configuring the system.

The predefined administrator has super administrator permissions—Create, Read, Update, Delete, and eXecute (CRUDX)—to all ACS resources. When you register a secondary instance to a primary instance, you can use any account created on the primary instance. The credentials that you create on the primary instance apply to the secondary instance.

Note After installation, the first time you log in to ACS, you must do so through the ACS web interface and install the licenses. You cannot log in to ACS through the CLI immediately after installation.

This section contains the following topics:

Understanding Administrator Roles and Accounts

The first time you log in to ACS 5.4, you are prompted for the predefined administrator username (*ACSAdmin*) and required to change the predefined password name (*default*).

Note You cannot rename, disable, or delete the ACSAdmin account.

After you change the password, you can start configuring the system. The predefined administrator has super administrator permissions—Create, Read, Update, Delete, and eXecute (CRUDX)—to all ACS resources.

If you do not need granular access control, the Super Admin role is most convenient, and this is the role assigned to the predefined ACSAdmin account.

To create further granularity in your access control, follow these steps:

1. Define Administrators. See Configuring System Administrators and Accounts, page 1-3.
2. Associate roles to administrators. See Understanding Roles, page 1-3

When these steps are completed, defined administrators can log in and start working in the system.

Understanding Authentication

An authentication request is the first operation for every management session. If authentication fails, the management session is terminated. But if authentication passes, the management session continues until the administrator logs out or the session times out.

ACS 5.4 authenticates every login operation by using user credentials (username and password). Then, by using the administrator and role definitions, ACS fetches the appropriate permissions and answers subsequent authorization requests.

The ACS user interface displays the functions and options for which you have the necessary administrator privileges only.

Note Allow a few seconds before logging back in so that changes in the system have time to propagate.

Related Topics

- Understanding Administrator Roles and Accounts, page 1-2
- Configuring System Administrators and Accounts, page 1-3

Configuring System Administrators and Accounts

This section contains the following topics:

- Understanding Roles
- Administrator Accounts and Role Association
- Creating, Duplicating, Editing, and Deleting Administrator Accounts
- Viewing Role Properties

Understanding Roles

Roles consist of typical administrator tasks, each with an associated set of permissions. Each administrator can have more than one predefined role, and a role can apply to multiple administrators. As a result, you can configure multiple tasks for a single administrator and multiple administrators for a single task.

You use the Administrator Accounts page to assign roles. In general, a precise definition of roles is the recommended starting point. Refer to Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 1-7 for more information.

Assigning Roles

You can assign roles to the internal administrator account. ACS 5.4 provides two methods to assign roles to internal administrators:

- Static Role assignment—Roles are assigned manually to the internal administrator account.

- Dynamic Role assignment—Roles are assigned based on the rules in the AAC authorization policy.

Assigning Static Roles

ACS 5.4 allows you to assign the administrator roles statically to an internal administrator account. This is applicable only for the internal administrator accounts. If you choose this static option, then you must select the administrator roles for each internal administrator account manually. When an administrator is trying to access the account, if that administrator is configured in an administrator internal identity store with a static role assignment, only the identity policy is executed for authentication. The authorization policy is skipped. After successful execution of the identity policy, the administrator is assigned with the selected role for the administrator account.

Assigning Dynamic Roles

ACS 5.4 allows you to assign the administrator roles statically to an internal administrator account.

If the administrator account is configured in an external or internal identity store and has a dynamic role assignment, ACS evaluates the authorization policy and gets a list of administrator roles and use it dynamically or Deny Access as the result. If the super admin assigns a dynamic role for an administrator and does not configure the authorization policy, then authorization of that administrator account uses the default value “deny access”. As a result, the authorization for this administrator account is denied. But, if you assign a static role for an administrator, then the authorization policy does not have any impact on authorizing that administrator.

Based on the selected role, ACS authenticates and manages the administrator access restrictions and authentications. If Deny Access is the result of the evaluation, then ACS denies access to the administrator and logs the reason for failure in the customer logs.

Note The ACS web interface displays only the functions for which you have privileges. For example, if your role is Network Device Admin, the System Administration drawer does not appear because you do not have permissions for the functions in that drawer.

Permissions

A permission is an access right that applies to a specific administrative task. Permissions consist of:

- **A Resource** – The list of ACS components that an administrator can access, such as network resources, or policy elements.
- **Privileges** – The privileges are Create, Read, Update, Delete, and eXecute (CRUDX). Some privileges cannot apply to a given resource. For example, the user resource cannot be executed.

A resource given to an administrator without any privileges means that the administrator has no access to resources. In addition, the permissions are discrete. If the privileges create, update, and delete apply to a resource, the read privilege is not available.

If no permission is defined for an object, the administrator cannot access this object, not even for reading.

Note You cannot make permission changes.

Predefined Roles

Table 1-1 shows the predefined roles included in ACS:

Table 1-1 Predefined Role Descriptions

Role	Privileges
ChangeAdminPassword	This role is intended for ACS administrators who manage other administrator accounts. This role entitles the administrator to change the password of other administrators.
ChangeUserPassword	This role is intended for ACS administrators who manage internal user accounts. This role entitles the administrator to change the password of internal users.
NetworkDeviceAdmin	This role is intended for ACS administrators who need to manage the ACS network device repository only, such as adding, updating, or deleting devices. This role has the following permissions: • Read and write permissions on network devices • Read and write permissions on NDGs and all object types in the Network Resources drawer
PolicyAdmin	This role is intended for the ACS policy administrator responsible for creating and managing ACS access services and access policy rules, and the policy elements referenced by the policy rules. This role has the following permissions: • Read and write permissions on all the elements used in policies, such as authorization profile, NDGs, IDGs, conditions, and so on • Read and write permissions on services policy
ReadOnlyAdmin	This role is intended for ACS administrators who need read-only access to all parts of the ACS user interface. This role has read-only access to all resources
ReportAdmin	This role is intended for administrators who need access to the ACS Monitoring and Report Viewer to generate and view reports or monitoring data only. This role has read-only access on logs.
SecurityAdmin	This role is required in order to create, update, or delete ACS administrator accounts, to assign administrative roles, and to change the ACS password policy. This role has the following permissions: • Read and write permissions on internal protocol users and administrator password policies • Read and write permissions on administrator account settings • Read and write permissions on administrator access settings
SuperAdmin	The Super Admin role has complete access to every ACS administrative function. If you do not need granular access control, this role is most convenient, and this is the role assigned to the predefined *ACSAdmin* account. This role has Create, Read, Update, Delete, and eXecute (CRUDX) permissions on all resources.

Table 1-1 Predefined Role Descriptions (continued)

Role	Privileges
SystemAdmin	This role is intended for administrators responsible for ACS system configuration and operations. This role has the following permissions: • Read and write permissions on all system administration activities except for account definition • Read and write permissions on ACS instances
UserAdmin	This role is intended for administrators who are responsible for adding, updating, or deleting entries in the internal ACS identity stores, which includes internal users and internal hosts. This role has the following permissions: • Read and write permissions on users and hosts • Read permission on IDGs

Note At first login, only the Super Admin is assigned to a specific administrator.

Related Topics

- Administrator Accounts and Role Association
- Creating, Duplicating, Editing, and Deleting Administrator Accounts

Changing Role Associations

By design, all roles in ACS are predefined and cannot be changed. ACS allows you to only change role associations. Owing to the potential ramifications on the system's entire authorization status, the ACS Super Admin and SecurityAdmin roles alone have the privilege to change role associations.

Changes in role associations take effect only after the affected administrators log out and log in again. At the new login, ACS reads and applies the role association changes.

Note You must be careful in assigning the ACS Super Admin and SecurityAdmin roles because of the global ramifications of role association changes.

Administrator Accounts and Role Association

Administrator account definitions consist of a name, status, description, e-mail address, password, and role assignment.

Note It is recommended that you create a unique administrator for each person. In this way, operations are clearly recorded in the audit log.

Administrators are authenticated against the internal database only.

You can edit and delete existing accounts. However, the web interface displays an error message if you attempt to delete or disable the last super administrator.

Only appropriate administrators can configure identities and certificates. The identities configured in the System Administration drawer are available in the Users and Identity Stores drawer, but they cannot be modified there.

When you create a new administrator, you have an option to choose the type of identity store for the password type. The new administrator is authenticated based on this password type. The password type can be internal administrator, AD, or LDAP. The default value of all the existing administrators is **`AdminsIDStore`**. The password type has a new association defined to create an association between the administrator account and the identity store. During the internal administrator authentication, if the administrator is present in the internal database, then the value in the password type field is read and populated in the attribute list.If this attribute value is not equal to **`AdminsIDStore`**, then the authentication is routed to either LDAP or an AD identity store, based on the value that is configured in the password type field. ACS use PAP authentication to authenticate administrators against AD and LDAP.

Recovery Administrator Account

ACS 5.4 requires the system administrator to keep at least one administrator account as a recovery account. If an account is configured as a recovery account, then ACS bypasses the administrator identity policy and authorization policy to authenticate that particular administrator. This recovery administrator account is authenticated against the administrator internal identity store. If you try to access ACS using the recovery account, you are authenticated against internal administrator users, and roles are assigned statically. You can have more than one recovery account. By default, the Super Admin account is set as a recovery account. When you create a new administrator account, ACS does not set that account as a recovery account, but you need to configure it as a recovery account in account settings.

To configure an administrator account as a recovery account, you need to perform the following actions:

- Assign a static role to the administrator account.
- Assign the Super Admin role to the administrator account.
- Do not use the password type to set an external identity store to the administrator account.

Related Topics

- Understanding Roles
- Creating, Duplicating, Editing, and Deleting Administrator Accounts

Creating, Duplicating, Editing, and Deleting Administrator Accounts

To create, duplicate, edit, or delete an administrator account:

Step 1 Choose **System Administration > Administrators > Accounts**.

The Administrators page appears with a list of configured administrators as described in Table 1-2:

Table 1-2 Accounts Page

Option	Description
Status	Current status of this administrator: • Enabled—This administrator is active. • Disabled—This administrator is not active. You cannot log into ACS with a disabled admin account.
Name	Name of the administrator.
Role(s)	Roles assigned to the administrator.
Description	Description of this administrator.

Step 2 Do any of the following:

- Click **Create**.
- Check the check box next to the account that you want to duplicate and click **Duplicate**.
- Click the account that you want to modify; or, check the check box for the Name and click **Edit**.
- Check the check box next to the account for which you want to change the password and click **Change Password**. See Resetting Another Administrator's Password, page 1-23 for more information.

Note On the Duplicate page, you must change at least the Admin Name.

- Check one or more check boxes next to the accounts that you want to delete and click **Delete**.

Note Firefox does not display a warning message when you try to delete the last recovery admin account from ACS web interface if you have enabled "Prevent this page from creating additional dialogs" checkbox.

Step 3 Complete the Administrator Accounts Properties page fields as described in Table 1-3:

Table 1-3 Administrator Accounts Properties Page

Option	Description
General	
Admin Name	Configured name of this administrator. If you are duplicating a rule, be sure to enter a unique name.
Status	From the Status drop-down menu, select whether the account is enabled or disabled. This option is disabled if you check the Account never disabled check box.
Description	A description of this administrator.
Email Address	Administrator e-mail address. ACS View will direct alerts to this e-mail address.
Recovery Account	Check this option to configure an account as a recovery account. ACS bypasses the administrator identity policies and authorization policies to authenticate the administrators when you use this option. See Recovery Administrator Account, page 1-7 for more information.

Table 1-3 Administrator Accounts Properties Page (continued)

Option	Description
Account never disabled	Check to ensure that your account is never disabled. Your account will not be disabled even when: • Your password expires • Your account becomes inactive • You exceed the specified number of login retries
Authentication Information	
Password Type	Displays (only AD and LDAP) configured external identity store names, along with internal administrator, which is the default password type. You can choose any identity store from the list. During administrator authentication, if an external identity store is configured for the administrator, then the internal identity store forwards the authentication request to the configured external identity store. If an external identity store is selected, you cannot configure a password for the administrator. The password edit box is disabled. You cannot use identity sequences as external identity stores for the password type. You can change the password type using the **Change Password** button, which is located in the **System Administration > Administrators > Accounts** page.
Password	Authentication password.
Confirm Password	Confirmation of the authentication password.
Change password on next login	Check to prompt the user for a new password at the next login. **Note** If you enable Change password on next login option for an administrator account, then the administrator cannot add ACS instances to a distributed deployment.
Role Assignment	
Available Roles	List of all configured roles. Select the roles that you want to assign for this administrator and click >. Click >> to assign all the roles for this administrator.
Assigned Roles	Roles that apply to this administrator.

Step 4 Click **Submit**.

The new account is saved. The Administrators page appears, with the new account that you created or duplicated.

Related Topics

- Understanding Roles, page 1-3
- Administrator Accounts and Role Association, page 1-6
- Viewing Predefined Roles, page 1-9
- Configuring Authentication Settings for Administrators, page 1-10

Viewing Predefined Roles

See Table 1-1 for description of the predefined roles included in ACS.

To view predefined roles:

Choose **System Administration > Administrators > Roles**.

The Roles page appears with a list of predefined roles. Table 1-4 describes the Roles page fields.

Table 1-4 Roles Page

Field	Description
Name	List of all configured roles. See Predefined Roles, page 1-5 for a list of predefined roles.
Description	Description of each role.

Viewing Role Properties

Use this page to view the properties of each role.

Choose **System Administration > Administrators > Roles, and click a role or choose the role's radio button and click View**.

The Roles Properties page appears as described in Table 1-5:

Table 1-5 Roles Properties Page

Field	Description
Name	Name of the role. If you are duplicating a role, you must enter a unique name as a minimum configuration; all other fields are optional. Roles cannot be created or edited. See Table 1-4 for a list of predefined roles.
Description	Description of the role. See Predefined Roles, page 1-5 for more information.
Permissions List	
Resource	List of available resources.
Privileges	Privileges that can be assigned to each resource. If a privilege does not apply, the privilege check box is dimmed (not available). Row color is irrelevant to availability of a given privilege and is determined by the explicit text in the Privileges column.

Related Topics

- Understanding Roles, page 1-3
- Administrator Accounts and Role Association, page 1-6
- Configuring Authentication Settings for Administrators, page 1-10

Configuring Authentication Settings for Administrators

Authentication settings are a set of rules that enhance security by forcing administrators to use strong passwords, regularly change their passwords, and so on. Any password policy changes that you make apply to all ACS system administrator accounts.

To configure a password policy:

Step 1 Choose **System Administration > Administrators > Settings > Authentication**.

The Password Policies page appears with the Password Complexity and Advanced tabs.

Step 2 In the **Password Complexity** tab, check each check box that you want to use to configure your administrator password.

Table 1-6 describes the fields in the Password Complexity tab.

Table 1-6 Password Complexity Tab

Option	Description
Applies to all ACS system administrator accounts	
Minimum length	Required minimum length; the valid options are 4 to 20.
Password may not contain the username or its characters in reversed order	Check to specify that the password cannot contain the username or reverse username. For example, if your username is john, your password cannot be john or nhoj.
Password may not contain 'cisco' or its characters in reversed order	Check to specify that the password cannot contain the word *cisco* or its characters in reverse order, that is, *ocsic*.
Password may not contain '' or its characters in reversed order	Check to specify that the password does not contain the string that you enter or its characters in reverse order. For example, if you specify a string, polly, your password cannot be polly or yllop.
Password may not contain repeated characters four or more times consecutively	Check to specify that the password cannot repeat characters four or more times consecutively. For example, you cannot have the string apppple as your password. The letter p appears four times consecutively.
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	Password must contain at least one lowercase alphabetic character.
Upper case alphabetic characters	Password must contain at least one uppercase alphabetic character.
Numeric characters	Password must contain at least one numeric character.
Non alphanumeric characters	Password must contain at least one nonalphanumeric character.

Step 3 In the **Advanced** tab, enter the values for the criteria that you want to configure for your administrator authentication process.

Table 1-7 describes the fields in the Advanced tab.

Table 1-7 Advanced Tab

Options	Description
Password History	
Password must be different from the previous *n* versions	Specifies the number of previous passwords for this administrator to be compared against. This option prevents the administrators from setting a password that was recently used. Valid options are 1 to 99.
Password Lifetime: Administrators are required to periodically change password	
Display reminder after *n* days	Displays a reminder after *n* days to change password; the valid options are 1 to 365. This option, when set, only displays a reminder. It does not prompt you for a new password.

Table 1-7 Advanced Tab

Options	Description
Require a password change after *n* days	Specifies that the password must be changed after *n* days; the valid options are 1 to 365. This option, when set, ensures that you change the password after n days.
Disable administrator account after *n* days if password is not changed	Specifies that the administrator account must be disabled after *n* days if the password is not changed; the valid options are 1 to 365. ACS does not allow you to configure this option without configuring the Display reminder after *n* days option.
Account Inactivity	
Inactive accounts are disabled	
Require a password change after *n* days of inactivity	Specifies that the password must be changed after *n* days of inactivity; the valid options are 1 to 365. This option, when set, ensures that you change the password after *n* days. ACS does not allow you to configure this option without configuring the Display reminder after *n* days option.
Disable administrator account after *n* days of inactivity	Specifies that the administrator account must be disabled after *n* days of inactivity; the valid options are 1 to 365. ACS does not allow you to configure this option without configuring the Display reminder after *n* days option.
Incorrect Password Attempts	
Disable account after *n* successive failed attempts	Specifies the maximum number of login retries after which the account is disabled; the valid options are 1 to 10.

Note ACS automatically deactivates or disables your account based on your last login, last password change, or number of login retries. The CLI and PI user accounts are blocked and they receive a notification that they can change the password through the web interface. If your account is disabled, contact another administrator to enable your account.

Step 4 Click **Submit**.

The administrator password is configured with the defined criteria. These criteria will apply only for future logins.

Related Topics

- Understanding Roles, page 1-3
- Administrator Accounts and Role Association, page 1-6
- Viewing Predefined Roles, page 1-9

Configuring Session Idle Timeout

A GUI session, by default, is assigned a timeout period of 30 minutes. You can configure a timeout period for anywhere from 5 to 90 minutes.

To configure the timeout period:

Step 1 Choose **System Administration > Administrators > Settings > Session**.

The GUI Session page appears.

Step 2 Enter the Session Idle Timeout value in minutes. Valid values are 5 to 90 minutes.

Step 3 Click **Submit**.

Note The CLI client interface has a default session timeout value of 6 hours. You cannot configure the session timeout period in the CLI client interface.

Configuring Administrator Access Settings

ACS 5.4 allows you to restrict administrative access to ACS based on the IP address of the remote client. You can filter IP addresses in any one of the following ways:

- Allow All IP Addresses to Connect, page 1-13
- Allow Remote Administration from a Select List of IP Addresses, page 1-13
- Reject Remote Administration from a Select List of IP Addresses, page 1-14

Allow All IP Addresses to Connect

You can choose the Allow all IP addresses to connect option to allow all connections; this is the default option.

Allow Remote Administration from a Select List of IP Addresses

To allow administrators to access ACS remotely:

Step 1 Choose **System Administration > Administrators > Settings > Access**.

The IP Addresses Filtering page appears.

Step 2 Click Allow only listed IP addresses to connect radio button.

The IP Range(s) area appears.

Step 3 Click **Create** in the IP Range(s) area.

A new window appears. Enter the IPv4 or IPv6 address of the machine from which you want to allow remote access to ACS. Enter a subnet mask for an entire IP address range. ACS checks if the address that is entered is in a format that is supported by IPv4 or IPv6.

Step 4 Click **OK.**

The IP Range(s) area is populated with the IP addresses. Repeat Step 3 to add other IP addresses or ranges for which you want to provide remote access.

Step 5 Click **Submit**.

Reject Remote Administration from a Select List of IP Addresses

To reject administrators from accessing ACS remotely:

Step 1 Choose **System Administration > Administrators > Settings > Access**.

The IP Addresses Filtering page appears.

Step 2 Click **Reject connections** from listed IP addresses radio button.

The IP Range(s) area appears.

Step 3 Click **Create** in the IP Range(s) area.

A new window appears.

Step 4 Enter the IP address of the machine that you do not want to access ACS remotely. Enter a subnet mask for an entire IP address range.

Step 5 Click **OK**.

The IP Range(s) area is populated with the IP addresses. Repeat Step 3 to add other IP addresses or ranges that you want to reject.

Step 6 Click **Submit**.

Note It is possible to reject connection from all IP addresses. You cannot reset this condition through the ACS web interface. However, you can use the following CLI command:

```
acs reset-password
```

Refer to the *CLI Reference Guide for Cisco Secure Access Control System 5.4* for more information.

Working with Administrative Access Control

ACS 5.4 introduces a new service type called the Administrative Access Control (AAC) service. The AAC service handles the authentications and authorization of the ACS administrators.

The enhanced AAC web interface includes:

- Policy-based authentication and authorization
- Authentication against an external database is feasible by:
  - Password type on administrator accounts in the Internal Administrators ID store.
  - Configuring the identity policy (the authentication policy) against an external database.

This AAC service is automatically created at the time of installation. You cannot remove or add a new AAC service. AAC is not available under the service selection policy and is automatically selected upon administrator login.

The AAC service identifies a set of policies for administrator login. The policies that are provided within the AAC service are these:

- The Administrator identity policy determines the identity database that is used to authenticate the administrator and also retrieves attributes for the administrator that may be used in subsequent authorization policy.
- The Administrator authorization policy determines the role of the administrator for the session in ACS. The assigned role determines the permission of the administrator. Each role has a predefined list of permissions, and it can be viewed in the roles page.

The AAC service processes these two policies in a sequence. You need to configure both the Administrator identity policy and the Administrator authorization policy. The default for both the policies are:

Identity policy—The default is Internal Identity Store.

Authorization policy—The default is Deny Access.

The AAC service supports only the PAP authentication type. Only the Super Admin is permitted to configure administrator access control.

While upgrading the ACS application to ACS 5.4, AAC undergoes the following changes:

- Single AAC service is automatically created during upgrade.
- The identity policy in AAC service is set to Administrators Internal Identity Store.
- All existing administrators are validated with a static role assignment.
- All administrators with the Super Admin role are automatically set as the recovery account.

After upgrading the ACS application to 5.4, if the administrator accounts are not updated, the upgraded administrator accounts are authenticated against the administrator internal identity store and get their roles through static assignment. While restoring the backup when upgrading, ACS 5.4 takes care of upgrading the schema files as well as the data.

Note Administrator accounts created in external identity stores cannot access CARS mode of ACS CLI. But, they can access acs-config mode of ACS CLI.

This section contains the following topics:

- Administrator Identity Policy, page 1-15
- Administrator Authorization Policy, page 1-19

Administrator Identity Policy

The identity policy in administrative access control defines the identity source that ACS uses for authentication and attribute retrieval. The attributes and groups can be retrieved only from the external database. ACS can use the retrieved attributes only in subsequent authorization policies.

The AAC service supports two types of identity policies. They are:

- Single result selection
- Rule-based result selection

Super Admin can configure and modify this policy. You can configure a simple policy, which applies the same identity source for authentication of all requests, or you can configure a rule-based identity policy.

The supported identity methods for a simple policy are:

- Deny Access—Access to the user is denied and no authentication is performed.

- Identity Store—A single identity store.

  You can select any one of the following identity stores:

  - Internal Administrator ID store
  - Active Directory ID store
  - LDAP ID store

In cases where Deny Access is selected as the result, the access of the administrator is denied.

In a rule-based policy, each rule contains one or more conditions and a result, which is the identity source to use for authentication.

The supported conditions are these:

- System username
- System time and date
- Administrator client IP address

An identity policy in the AAC service does not support the identity store sequence as a result. You can create, duplicate, edit, and delete rules within the identity policy, and you can enable and disable them.

Caution If you switch between the simple policy and the rule-based policy pages, you will lose your previously saved policy configuration.

To configure a simple identity policy, complete the following steps:

Step 1 Select **System Administration > Administrative Access Control > Identity**.

By default, the Simple Identity Policy page appears with the fields as described in Table 1-8.

Table 1-8 Simple Identity Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the result to apply to all requests. • Rule-based—Configures rules to apply different results, depending on the request. If you switch between policy types, you will lose your previously saved policy configuration.
Identity Source	Identity source to apply to all requests. The default is Deny Access. For password-based authentication, choose a single identity store or an identity store sequence.

Step 2 Select an identity source for authentication; or, choose **Deny Access**.

Step 3 Click **Save Changes** to save the policy.

Viewing Rule-Based Identity Policies

Select **System Administration > Administrative Access Control > Identity.**

By default, the Simple Identity Policy page appears with the fields as described in Table 1-8. If it is configured, the Rule-Based Identity Policy page appears with the fields as described in Table 1-9:

Table 1-9 Rule-Based Identity Policy Page

Option	Description
Policy type	Defines the type of policy to configure: • Simple—Specifies the results to apply to all requests. • Rule-based—Configures rules to apply different results depending on the request. **Caution** If you switch between policy types, you will lose your previously saved policy configuration.
Status	The current status of the rule. The rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Name	Rule name.
Conditions	Conditions that determine the scope of the policy. This column displays all current conditions in sub columns.
Results	Identity source that is used for authentication as a result of the evaluation of the rule.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 1-10.

To configure a rule-based policy, see these topics:

- Creating Policy Rules, page 1-38
- Duplicating a Rule, page 1-39
- Editing Policy Rules, page 1-39
- Deleting Policy Rules, page 1-40

Configuring Identity Policy Rule Properties

You can create, duplicate, or edit an identity policy rule to determine the identity databases that are used to authenticate the administrator and retrieve attributes for the administrator. The retrieval of attributes is possible only if you use an external database.

To display this page, complete the following steps:

Step 1 Choose **System Administration > Administrative Access Control > Identity,** then do one of the following:

- Click **Create**.
- Check a rule check box, and click **Duplicate**.
- Click a rule name or check a rule check box, then click **Edit**.

Step 2 Complete the fields as shown in the Identity Rule Properties page, as described in Table 1-10.

Table 1-10 Identity Rule Properties Page

Option	Description
General	
Rule Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Rule Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	Conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is *ANY*. To change the value for a condition, check the condition check box, then specify the value. If you check **Compound Condition**, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 1-41.
Results	
Identity Source	Identity source to apply to requests. The default is Administrators Internal Identity store. For password-based authentication, choose a single identity store or an identity store sequence.

Administrator Authorization Policy

The authorization policy in the Administrative Access Control is used for dynamically assigning roles to administrators upon login. The role of the administrator is set according to the rules that are defined in the policy. According to the rules that are defined in the policy, the condition can include attributes and groups if authenticated with an external database. ACS can use the retrieved attributes in subsequent policies.

The authorization policy-based role assignment is applicable for both internal and external administrator accounts. This is the only method that is available to assign roles to the external administrator accounts.

In the administrator authorization policy, each rule contains one or more conditions that are used for authentication and a result.

The supported conditions are:

- System username
- System time and date
- Administrator client IP address
- AD dictionary or LDAP dictionary (external groups and attributes)

The administrator identity policy and the password type feature enable administrators to authenticate the requests in external identity stores like Active Directory or LDAP identity stores and to retrieve the administrator groups and attributes. The administrator authorization policy rules can be configured based on these retrieved groups and attributes.

You can configure the administrator authorization policy results with a set of administrator roles that are to be assigned to the administrators.

The supported authorization policy results are:

- Administrator Role Result—One or more administrator roles
- Deny Access—Failed authorization

You can create, duplicate, edit, and delete rules within the authorization policy, and you can enable and disable rules.

Configuring Administrator Authorization Policies

The administrator authorization policy determines the role for ACS administrators.

See Configuring General Access Service Properties, page 1-13 for a description of the AAC Access Service properties page.

Use this page to do the following:

- View rules.
- Delete rules.
- Open pages that enable you to create, duplicate, edit, and customize rules.

Select **System Administration > Administrative Access Control > Authorization > Standard Policy**.

The Administrator Authorization Policy page appears as described in Table 1-11.

Table 1-11 Administrators Authorization Policy Page

Option	Description
Status	Rule statuses are: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor-only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the administrator roles that are applied when the corresponding rule is matched. You can customize rule results; a rule can apply administrator roles. The columns that appear reflect the customization settings.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions and results to use in policy rules. The Conditions and Results columns reflect your customized settings. **Caution** If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 1-10.

Configuring Administrator Authorization Rule Properties

Use this page to create, duplicate, and edit the rules to determine administrator roles in the AAC access service.

Select **System Administration > Administrative Access Control > Authorization > Standard Policy**, and click **Create, Edit,** or **Duplicate**.

The Administrator Authorization Rule Properties page appears as described in Table 1-12.

Table 1-12 Administrators Authorization Rule Properties Page

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are as follows: • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor-only. The monitor option is especially useful for viewing watching the results of a new rule.
Conditions	
conditions	These are conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value. If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 1-41.
Results	
Roles	Roles to apply for the rule.

Administrator Login Process

When an administrator logs in to the ACS web interface, ACS 5.4 performs the authentication as given below.

If an administrator account is configured as a recovery account in the administrator internal identity store, then ACS bypasses the identity and authorization policies, authenticates the administrator against the administrator internal identity store, and assigns the role statically. If an administrator account is not a recovery account, then ACS proceeds with policy-based authentication.

As a part of policy-based authentication, ACS fetches the AAC service with identity policy and authorization policy configuration. ACS evaluates the identity policy and gets the identity store as a result. If the identity policy result is the administrator internal identity store, then ACS evaluates the password type and retrieves the identity store as the result.

ACS authenticates the administrator against the selected identity store, and retrieves the user groups and user attributes, if the administrator account is configured in an external identity store.

If the administrator account is configured in the internal identity store, and it has a static role assignment, then ACS extracts the list of administrator roles.

If the administrator account is configured in an external or internal identity store and has a dynamic role assignment, ACS evaluates the authorization policy, gets a list of administrator roles, and uses it dynamically, or gets Deny Access as the result.

Based on the selected role, ACS authenticates and manages the administrator access restrictions and authentications. If Deny Access is the result of the evaluation, then ACS denies access to the administrator and logs the reason for failure in the customer logs.

Note If the administrator password on the AD or LDAP server is expired or reset, then ACS denies the administrator access to the web interface.

Resetting the Administrator Password

While configuring administrator access settings, it is possible for all administrator accounts to get locked out, with none of the administrators able to access ACS from any IP address in your enterprise. If this happens, you must reset the administrator password from the ACS Config CLI. You must use the following command to reset all administrator passwords:

access-setting accept-all

For more information on this command, refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/command/reference/cli_app_a.html#wp1893005.

Note You cannot reset the administrator password through the ACS web interface.

Changing the Administrator Password

ACS 5.4 introduces a new role Change Admin Password that entitles an administrator to change another administrator's password. If an administrator's account is disabled, any other administrator who is assigned the Change Admin Password role can reset the disabled account through the ACS web interface. This section contains the following topics:

- Changing Your Own Administrator Password, page 1-22
- Resetting Another Administrator's Password, page 1-23

Changing Your Own Administrator Password

Note All administrators can change their own passwords. You do not need any special roles to perform this operation.

To change your password:

Step 1 Choose **My Workspace > My Account**.

The My Account page appears. See My Account Page, page 1-2 for valid values.

Step 2 In the **Password field** section, enter the current administrator password.

Step 3 In the New Password field, enter a new administrator password.

Step 4 In the Confirm Password field, re-enter the new administration password.

Step 5 Click **Submit**.

The administrator password is created.

You can also use the **acs reset-password** command to reset your ACSAdmin account password. For more information on this command, refer to

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.4/command/reference/cli_app_a.html#wp1887660.

Resetting Another Administrator's Password

To reset another administrator's password:

Step 1 Choose **System Administration > Administrators > Accounts**.

The Accounts page appears with a list of administrator accounts.

Step 2 Check the check box next to the administrator account for which you want to change the password and click **Change Password**.

The Authentication Information page appears, listing the date when the administrator's password was last changed.

Step 3 In the Password field, enter a new administrator password.

Step 4 In the Confirm Password field, re-enter the new administrator password.

Step 5 Check the **Change password on next login** check box for the other administrator to change password at first login.

Step 6 Click **Submit**.

The administrator password is reset.

Related Topics

- Configuring Authentication Settings for Administrators, page 1-10
- Understanding Roles, page 1-3
- Administrator Accounts and Role Association, page 1-6
- Viewing Predefined Roles, page 1-9