



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 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 5.8.1, 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, page 16-2](#)
- [Configuring System Administrators and Accounts, page 16-3](#)
- [Understanding Roles, page 16-3](#)
- [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#)
- [Viewing Predefined Roles, page 16-13](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)
- [Configuring Session Idle Timeout, page 16-17](#)
- [Configuring Administrator Access Settings, page 16-17](#)
- [Working with Administrative Access Control, page 16-18](#)
- [Authenticating Administrators against RADIUS Identity and RSA SecurID Servers, page 16-23](#)
- [Resetting the Administrator Password, page 16-29](#)
- [Changing the Administrator Password, page 16-30](#)

Understanding Administrator Roles and Accounts

The first time you log in to ACS 5.8.1, you are prompted for the predefined administrator username (*ACSAdmin*) and are required to change the predefined password name (*default*). The *acsadmin* account in Cisco Secure ACS, Release 5.8.1, is similar to any other administrator account with the SuperAdmin role. The default *acsadmin* account can now be disabled or deleted, provided you have another recovery administrator account with the SuperAdmin role. The account disablement criteria, such as password lifetime, account disablement, and exceeding failed authentication attempts, also apply to the default *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 SuperAdmin role is most convenient, and this role assigned to the predefined *ACSAdmin* account.

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

Step 1 Define Administrators. See [Configuring System Administrators and Accounts, page 16-3](#).

Step 2 Associate roles to administrators. See [on page 3Understanding Roles, page 16-3](#).

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 5.8.1 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 16-2](#)
- [Configuring System Administrators and Accounts, page 16-3](#)

Configuring System Administrators and Accounts

This section contains the following topics:

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#)
- [Viewing Role Properties, page 16-14](#)

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 16-8](#) for more information.

Assigning Roles

You can assign roles to the internal administrator account. ACS 5.8.1 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 5.8.1 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 5.8.1 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

ACS 5.8.1 introduces two new predefined administrator roles called Provisioning Admin and Operations Admin. You can create new administrator accounts using these two new roles. You cannot use these two administrator roles together or along with any other administrator roles while creating administrator accounts.

Table 16-1 shows the predefined roles included in ACS:

Table 16-1 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: <ul style="list-style-type: none"> • Read and write permissions on network devices • Read and write permissions on NDGs and all object types in the Network Resources drawer |
| OperationsAdmin | <p>This role is a combination of a few of the existing administrator accounts along with some extra resources and privileges.</p> <p>To view the resources and privileges of OperationsAdmin:</p> <ol style="list-style-type: none"> 1. Choose System Administration > Administrators > Roles from ACS web interface. 2. Click the radio button near OperationsAdmin. 3. Click View. <p>ACS displays the resources and privileges associated with OperationsAdmin.</p> <p>OperationsAdmin can be authenticated against external databases similar to other administrators in ACS.</p> <p>Note You cannot combine OperationsAdmin role with any other administrator role while creating administrator accounts.</p> <p>Note You can assign roles, resources, and privileges to ProvisioningAdmin similar to other administrators. But, you cannot assign the OperationsAdmin as a recovery administrator account.</p> |

Table 16-1 Predefined Role Descriptions (continued)

| Role | Privileges |
|-------------------|--|
| PolicyAdmin | <p>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:</p> <ul style="list-style-type: none"> • 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 |
| ProvisioningAdmin | <p>This role is a combination of a few of the existing administrator accounts along with some extra resources and privileges.</p> <p>To view the resources and privileges of ProvisioningAdmin:</p> <ol style="list-style-type: none"> 1. Choose System Administration > Administrators > Roles from ACS web interface. 2. Click the radio button near ProvisioningAdmin. 3. Click View. <p>ACS displays the resources and privileges associated with ProvisioningAdmin.</p> <p>ProvisioningAdmin can be authenticated against external databases similar to other administrators in ACS.</p> <p>Note You cannot combine ProvisioningAdmin role with any other administrator role while creating administrator accounts.</p> <p>Note You can assign roles, resources, and privileges to ProvisioningAdmin similar to other administrators. But, you cannot assign the ProvisioningAdmin as a recovery administrator account.</p> |
| ReadOnlyAdmin | <p>This role is intended for ACS administrators who need read-only access to all parts of the ACS user interface.</p> <p>This role has read-only access to all resources</p> |
| ReportAdmin | <p>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.</p> <p>This role has read-only access on logs.</p> |
| SecurityAdmin | <p>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:</p> <ul style="list-style-type: none"> • 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 | <p>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 <i>ACSAdmin</i> account.</p> <p>This role has Create, Read, Update, Delete, and eXecute (CRUDX) permissions on all resources.</p> |

Table 16-1 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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, page 16-7](#)
- [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#)

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 and external databases.

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 5.8.1 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. A recovery administrator cannot enable password hashing in ACS.

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.
- Do not enable password hash.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#)

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 16-2](#):

Table 16-2 Accounts Page

| Option | Description |
|-------------|--|
| Status | Current status of this administrator: <ul style="list-style-type: none"> Enabled—This administrator is active. Disabled—This administrator is not active. You cannot log into ACS with a disabled administrator 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 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 the account for which you want to change the password and click **Change Password**. See [Resetting Another Administrator's Password, page 16-30](#) for more information.



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

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

ACS deletes the selected administrator account only if there is at least one recovery administrator account with SuperAdmin role in the ACS database other than the selected administrator account.



Note Firefox does not display a warning message when you try to delete the last recovery administrator account from ACS web interface if you have enabled “Prevent this page from creating additional dialogs” check box.

- Step 3** Complete the Administrator Accounts Properties page fields as described in [Table 16-3](#):

Table 16-3 Administrator Accounts Properties Page

| Option | Description |
|--------------------|--|
| General | |
| Administrator 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 sends alerts to this e-mail address. ACS uses this email address to notify the internal administrators about their password expiry <i>n</i> days before their password expires. |

Table 16-3 Administrator Accounts Properties Page (continued)

| Option | Description |
|-----------------------------------|---|
| Recovery Account | <p>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 16-8 for more information.</p> <p>Note ACS does not allow you to enable password hashing for the Recovery Administrator accounts. ACS displays the following message when you set an administrator account as a recovery account:</p> <p>Please note that for a valid recovery account, you must enable the account, disable password hash, set assignment type to static, assign the SuperAdmin role, and set password type to the Internal Administrators Store.</p> |
| Account never disabled | <p>Check to ensure that your account is never disabled. Your account will not be disabled even when:</p> <ul style="list-style-type: none"> Your password expires Your account becomes inactive You exceed the specified number of login retries |
| Enable Password Hash | <p>Check this check box to enable password hashing using the PBKDF2 of Cisco SSL hashing algorithm to provide enhanced security to the administrator passwords. By default, this option is disabled. This option is applicable only for internal administrators. When you disable this option in the middle, you have to re-configure your password using the Change Password option immediately after disabling this option. For more information, see Enable and Disable Password Hashing for Internal Administrators, page 16-12.</p> <p>Note ACS runtime process must be up and running properly for this option to work properly</p> |
| Authentication Information | |
| Password Type | <p>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.</p> <p>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.</p> <p>If an external identity store is selected, you cannot configure a password for the administrator. The password edit box is disabled.</p> <p>You cannot use identity sequences as external identity stores for the password type.</p> <p>You can change the password type using the Change Password button, which is located in the System Administration > Administrators > Accounts page.</p> |
| Password | Authentication password. |
| Confirm Password | Confirmation of the authentication password. |
| Change password on next login | <p>Check to prompt the user for a new password at the next login.</p> <p>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.</p> |
| 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.

**Note**

For the administrator accounts whose password type is set as AD, ACS fails the authentication if the “User must change password at next logon” option is enabled in Active Directory.

**Note**

A SuperAdmin with static role assignment can create, assign, or remove SuperAdmin roles for other administrators whereas a SuperAdmin with dynamic role assignment cannot create, assign, or remove SuperAdmin roles for other administrators.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)
- [Exporting Administrator Accounts, page 16-11](#)

Exporting Administrator Accounts

ACS 5.8.1 allows you to export the administrator accounts to a .csv file using the export option available on the Administrator Accounts page. This option exports all administrator accounts that are created and listed in the administrator accounts page to a .csv file. You can save this file to a local drive for audit purposes. You can also encrypt the exported file using an encryption password option. You need this password to decrypt the exported file. However, you cannot import the exported administrator account details back into ACS. For dynamic administrator accounts, the roles column in the exported file is empty. If you have assigned multiple roles for an administrator, a semicolon is used in between the roles. You can also export the administrator accounts from the ACS CLI, but you cannot export administrator accounts using REST PI.

**Note**

To export the administrator accounts, you must have an administrator account with SuperAdmin, SystemAdmin, or UserAdmin roles.

To export the administrator accounts from the ACS web interface:

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

The Administrators page appears with a list of configured administrators as described in [Table 16-2](#).

Step 2 Click **Export**.

The Export properties dialog box appears.

Step 3 Check the check box the **Password** field, and enter the encryption password if you want to encrypt the exported file.

Step 4 Click **Start Export**.

The Export Progress dialog box appears and displays the progress of the export operation. This dialog box also displays the export logs that helps the user to identify the errors during export operation.

**Note**

To export the administrator accounts from the ACS CLI, run the **export-data administrator <repository> <export_filename> <result_filename> <encryption_type>** command in ACS configuration mode.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)

Enable and Disable Password Hashing for Internal Administrators

You can enable password hashing to enhance security for internal administrators password. You can enable the Enable Password Hash option from ACS Administrator Account page of ACS web interface.

To enhance security of internal administrators' password, ACS 5.8.1 introduces the new feature "Enable Password Hash". If you enable this option, the administrator password is converted into hashes using the PBKDF2 of Cisco SSL hashing algorithm and is stored in the internal database. This feature is applicable only for password based authentications. ACS runtime process must be up and running properly for this option to work properly.

ACS converts the passwords to hashes and stores the same in the internal database if the Enable Password Hashing option while creating internal administrator accounts. When an administrator tries to access ACS using the login password, ACS converts that password to hashes using the PBKDF2 hashing algorithm and compares this hash entry with the entry that is stored in the internal database. ACS allows the administrator to log in only if the password hash value matches with the database hash value. ACS supports enabling password hash in distributed deployments. You cannot enable password hashing if you are a recovery administrator.

For a distributed deployment, the trust communication between ACS instances must be enabled to add a ACS instance as a secondary instance using the administrator account whose password hashing option is enabled. For information on Trust Communication, see [Trust Communication in a Distributed Deployment, page 17-31](#).

To enable password hashing for internal administrators:

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

The Internal Administrators page appears with the list of available internal administrators.

Step 2 Perform one of the following:

- Click **Create**.
- Check the check box next to the administrator account for which you want to enable password hashing and click **Edit**.

Step 3 Check the **Enable Password Hash** check box.

Step 4 Click **Submit**.

The Password hashing option is enabled for the selected internal administrator.



Note

ACS displays the following error when you enable password hashing for a recovery administrator account and click submit: For a recovery account password hash must be disabled.

To disable password hashing for internal administrators:

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

The Internal Administrators page appears with the list of available internal administrators.

Step 2 Check the check box next to administrator account for which you want to disable password hash and click **Edit**.

Step 3 Uncheck the **Enable Password Hash** check box.

Step 4 Click **Submit**.

The Password hashing option is disabled for the selected internal administrator.



Note

After disabling the **Enable Password Hash** option, you must change the user password immediately.

Step 5 Check the check box next to the administrator account for which you have disabled the password hash option and click **Change Password**.

Step 6 Enter the new password in the **Password** field.

Step 7 Reenter the new password in the **Confirm Password** field.

Step 8 Click **Submit**.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)

Viewing Predefined Roles

See [Table 16-1](#) 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 16-4](#) describes the Roles page fields.

Table 16-4 Roles Page

| Field | Description |
|-------------|---|
| Name | List of all configured roles. See Predefined Roles, page 16-5 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 16-5](#):

Table 16-5 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 16-4 for a list of predefined roles. |
| Description | Description of the role. See Predefined Roles, page 16-5 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 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)

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 16-6 describes the fields in the Password Complexity tab.

Table 16-6 Password Complexity Tab

| Option | Description |
|---|--|
| Applies to all ACS system administrator accounts | |
| Minimum length | Required minimum length; the valid options are 4 to 127. |
| 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 <i>cisco</i> or its characters in reverse order, that is, <i>ocsic</i> . |
| 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 16-7 describes the fields in the Advanced tab.

Table 16-7 Advanced Tab

| Options | Description |
|---|---|
| Password History | |
| Password must be different from the previous <i>n</i> 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 | |
| Require a password change after <i>n</i> days | Specifies that the password must be changed after <i>n</i> days; the valid options are 1 to 365. This option, when set, ensures that you change the password after <i>n</i> days. |
| Disable administrator account after <i>n</i> days if password is not changed | Specifies that the administrator account must be disabled after <i>n</i> 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 <i>n</i> days option. |

Table 16-7 Advanced Tab

| Options | Description |
|--|---|
| Send Email for password expiry before n days | Specifies that an email notification a day must be sent to the internal administrators starting from n th day before their password expires if the password is not changed; the valid options are 1 to 365. The default value is 5 days. This option, when set, ensures that an email notification is sent to the internal administrator accounts n days before their password expires. ACS does not allow you to configure this option without configuring the Disable administrator account after n days if password is not changed. |
| 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. |
| 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 ACS 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 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)

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. The session timeout option is not applicable for the Active Directory and Distributed System Management pages. The AD page is automatically refreshed to verify the AD connectivity status based on the refresh interval that is defined in the application. The Distributed System Management page is automatically refreshed for the configured interval of time. You can configure the refresh interval from the Distributed System Management page of ACS web interface.

To configure the timeout period:

-
- Step 1** Choose **System Administration > Administrators > Settings > Session**.
 - Step 2** The GUI Session page appears.
 - Step 3** Enter the Session Idle Timeout value in minutes. Valid values are 5 to 90 minutes.
 - Step 4** 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 5.8.1 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 16-17](#)
- [Allow Remote Administration from a Select List of IP Addresses, page 16-17](#)
- [Reject Remote Administration from a Select List of IP Addresses, page 16-18](#)

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:

```
access-setting accept-all
```

For more information on this command, see [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#) for more information.

Working with Administrative Access Control

ACS 5.8.1 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 5.8.1, 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 5.8.1, 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 5.8.1 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 16-19](#)
- [Administrator Authorization Policy, page 16-26](#)

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
- RSA SecurID store
- RADIUS Identity 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 16-8](#).

Table 16-8 *Simple Identity Policy Page*

| Option | Description |
|-----------------|---|
| Policy type | <p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> • Simple—Specifies the result to apply to all requests. • Rule-based—Configures rules to apply different results, depending on the request. <p>If you switch between policy types, you will lose your previously saved policy configuration.</p> |
| 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 16-8](#). If it is configured, the Rule-Based Identity Policy page appears with the fields as described in [Table 16-9](#):

Table 16-9 *Rule-Based Identity Policy Page*



| Option | Description |
|--------------|--|
| Policy type | <p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> Simple—Specifies the results to apply to all requests. Rule-based—Configures rules to apply different results depending on the request. <p> Caution If you switch between policy types, you will lose your previously saved policy configuration.</p> |
| Status | <p>The current status of the rule. The rule statuses are:</p> <ul style="list-style-type: none"> 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 | <p>ACS applies the Default rule when:</p> <ul style="list-style-type: none"> Enabled rules are not matched. No other rules are defined. <p>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.</p> |

Table 16-9 Rule-Based Identity Policy Page (continued)

| Option | Description |
|------------------|--|
| Customize button | <p>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.</p> <p> Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p> |
| Hit Count button | <p>Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.</p> |

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

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)

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**.
4. Complete the fields as shown in the Identity Rule Properties page, as described in [Table 16-10](#).

Table 16-10 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. |

Table 16-10 (continued) Identity Rule Properties Page (continued)

| Option | Description |
|-------------------|---|
| Rule Status | <p>Rule statuses are:</p> <ul style="list-style-type: none"> • 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 | <p>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.</p> <p>The default value for each condition is <i>ANY</i>. To change the value for a condition, check the condition check box, then specify the value.</p> <p>If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.</p> |
| 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. |

Authenticating Administrators against RADIUS Identity and RSA SecurID Servers

ACS 5.8.1 supports authenticating administrators against RADIUS Identity and RSA SecurID servers. This feature is available in both the ACS web interface and the ACS configuration mode of ACS CLI. This feature enhances security for administrator authentications by using an One Time Password (OTP) that the RADIUS Identity or RSA SecurID server generates. ACS has the following two use cases for authenticating administrators against external identity sources:

- Administrator account is in ACS. Password type is set as External Identity source. The password type is set as external identity source under **System Administration > Administrators > Accounts**. Therefore, the authentication password for the administrator account must be retrieved from the specified external identity source.
- Administrator account is in external identity source. Therefore, ACS uses the external identity source to verify both the administrator account and its password to authenticate the administrator against the external identity source.

This section contains the following topics:

- [Authenticating Administrators against RADIUS Identity Server, page 16-24](#)
- [Authenticating Administrators against RSA SecurID Server, page 16-24](#)

Authenticating Administrators against RADIUS Identity Server

To authenticate administrators against RADIUS Identity server:

-
- Step 1** Add the RADIUS Identity server in ACS. See [Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90](#) for more information.
 - Step 2** Add ACS and administrator account in RADIUS Identity server. Refer to the RADIUS Identity server documentation for information on how to perform these operations.
 - Step 3** Choose **System Administration > Administrative Access Control > Identity** in the ACS web interface.
 - Step 4** Click **Single result selection** radio button.
 - Step 5** Select the RADIUS Identity server as Identity Source and click **Save Changes**.
 - Step 6** Log out from the ACS web interface.
 - Step 7** Launch ACS web interface to authenticate the administrator account against RADIUS Identity server for the first time.
 - Step 8** Enter the username in the **Username** field, password set in the RADIUS Identity server in the **Password** field, and click **Login**.

Based on the RADIUS Identity server configuration, ACS might display different messages to the administrators before authenticating them.

ACS allows the administrator to log in to the web interface using the password set in the RADIUS Identity server.



Note

To authenticate ACS administrators against RADIUS Identity server from ACS CLI, use the same procedure discussed above in **acs-config** mode of ACS CLI.

Related Topics

- [Authenticating Administrators against RSA SecurID Server, page 16-24](#)

Authenticating Administrators against RSA SecurID Server

To authenticate administrators against RSA SecurID server as an external identity source:

Setting RSA SecurID Server as external identity source for ACS administrator authentications

- Step 1** Add the RSA SecurID server in ACS. See [Configuring RSA SecurID Agents, page 8-80](#) for more information.
- Step 2** Add ACS and administrator account in RSA SecurID server. See *RSA Authentication Manager Administrator's Guide* for more information.
- Step 3** Choose **System Administration > Administrative Access Control > Identity** in ACS web interface.
- Step 4** Click **Single result selection** radio button.
- Step 5** Select the RSA SecurID server as Identity Source and click **Save Changes**.

You have now configured RSA SecurID server as the external identity source for authenticating administrators.

Performing First ACS administrator authentication using RSA SecurID Server

- Step 1** Launch ACS web interface.
- Step 2** Enter the username in the **Username** field.
- Step 3** Generate a **Token code** using RSA SecurID device and enter the token code in the **Password** field of ACS web interface and click **Login**.

Based on the RSA SecurID server configuration, ACS may display the following message with a system generated PIN:

```
PIN: <XXXXXXX> Please remember your new PIN then press Return to continue.
```



Note Copy the PIN displayed in the above message and store it in your system. You have to use this PIN to generate the subsequent token codes for logging in to the ACS web interface.

- Step 4** Click **Login**.
- ACS allows the administrator to log in to the web interface. The first administrator authentication against RSA SecurID server is successful.
-

When you use RSA SecurID server to authenticate administrator account for the first time:

- If you click **Cancel** when ACS displays the challenge message, you must start the authentication procedure from the beginning.
- If you click **Cancel** after ACS displays a system generated PIN, it means that you have canceled the first authentication and you can use the system generated PIN to perform the subsequent authentications.

When you use RSA SecurID server for subsequent administrator authentications, if you enter the wrong passcode, ACS prompts for the correct password. If you enter the correct password now and click **Login**, ACS prompts for the next token code to ensure security.

Performing Subsequent ACS administrator authentications using RSA SecurID Server.

- Step 1** Launch ACS web interface.
- Step 2** Enter the username in the **Username** field.
- Step 3** Enter the system generated PIN that ACS has displayed in the RSA SecurID device and click the arrow icon.
- RSA SecurID device displays a passcode.
- Step 4** Copy the passcode from RSA SecurID device and enter the same in the password field of ACS web interface and click **Login**.

ACS allows the administrator to log in to the web interface. The subsequent administrator authentication against RSA SecurID server is successful.

You can find the administrator authentication related logs in **Monitoring and Reports > Reports > ACS Reports > ACS Instance > ACS Administrator Logins** page.

**Note**

To authenticate ACS administrators against RSA SecurID server from ACS CLI, use the same procedure discussed above in **acs-config** mode of ACS CLI. When you authenticate administrator against RSA SecurID server from ACS CLI, you can see two log entries for a single CLI authentication. One entry is logged against ACS web interface and another one is logged against CLI. Both the entries list the IP address as loop back address (127.0.0.1). The ACS web interface log entry displays the authentication summary and the detailed steps whereas the CLI entry only lists the authentication summary, but not the detailed steps.

**Note**

You can download the RSA SecurID software token from the following link:
<http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/ms-windows.htm>

Related Topics

- [Authenticating Administrators against RADIUS Identity Server, page 16-24](#)

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)

Generally, we have also added the possibility to configure authorization policy based on the attributes returned by the RADIUS Identity server.

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 10-13](#) 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 16-11](#).

Table 16-11 Administrators Authorization Policy Page

| Option | Description |
|--------------|--|
| Status | <p>Rule statuses are:</p> <ul style="list-style-type: none"> • 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 | <p>Displays the administrator roles that are applied when the corresponding rule is matched.</p> <p>You can customize rule results; a rule can apply administrator roles. The columns that appear reflect the customization settings.</p> |
| Hit Count | Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column. |
| Default Rule | <p>ACS applies the Default rule when:</p> <ul style="list-style-type: none"> • Enabled rules are not matched. • No other rules are defined. <p>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.</p> |

Table 16-11 Administrators Authorization Policy Page (continued)

| Option | Description |
|------------------|---|
| Customize button | <p>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.</p> <p> Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p> |
| 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 10-10 . |

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 16-12](#).

Table 16-12 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 | <p>Rule statuses are as follows:</p> <ul style="list-style-type: none"> • 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 | <p>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.</p> <p>The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value.</p> <p>If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.</p> |
| Results | |
| Roles | Roles to apply for the rule. |

Administrator Login Process

When an administrator logs in to the ACS web interface, ACS 5.8.1 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

An administrator with Super Admin role has the rights to change the roles and privileges of other administrators.



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 *CLI Reference Guide for Cisco Secure Access Control System 5.8.1*.



Note

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

Changing the Administrator Password

ACS 5.8.1 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 16-30](#)
- [Resetting Another Administrator's Password, page 16-30](#)

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 5-2](#) 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 ACS Administrator account password. For more information on this command, refer to [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#).

Resetting Another Administrator's Password

An internal web administrator who has the Super Admin role or ChangeAdminPassword role can reset or change the passwords for other administrators. 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 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 16-14](#)
- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)

