Configuring Role-Based Access Control

This chapter includes the following sections:

- Role-Based Access Control, page 1
- User Accounts for Cisco UCS , page 1
- Configuring User Roles, page 5
- Configuring Locally Authenticated User Accounts, page 11
- Configuring User Locales, page 17
- Configuring User Domain Groups, page 21
- Configuring User Organizations, page 22
- Configuring Passwords, page 24
- Monitoring User Sessions, page 27

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Accounts for Cisco UCS

User accounts are used to access the system. Up to 128 user accounts can be configured in each Cisco UCS Central domain. Each user account must have a unique username and password.

A user account can be set with a SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Admin Account

Cisco UCS Central has an admin account. The admin account is a default user account and cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

The local admin user is able to login for fail over, even when authentication is set to remote.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated through the Cisco UCS Central user database, and can be enabled or disabled by anyone with admin or aaa privileges. Once a local user account is disabled, the user cannot log in. Configuration details for disabled local user accounts are not deleted by the database. If you re-enable a disabled local user account, the account becomes active again with the existing configuration, including username and password.

Remotely Authenticated User Accounts

A remotely authenticated user account is any Cisco UCS Central user account that is authenticated through LDAP. Cisco UCS domainssupport LDAP, RADIUS and TACACS+.

If a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

Note After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available.

Guidelines for Cisco UCS Usernames

The username is also used as the login ID for Cisco UCS Central. When you assign login IDs to Cisco UCS user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)

    - . (dot)

- The login ID must be unique within Cisco UCS Central.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Reserved Words: Locally Authenticated User Accounts

The following words cannot be used when creating a local user account in Cisco UCS and Cisco UCS Central.

- root
- bin
- daemon
- adm
- ip
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp

- man
- sys
- samdme
- debug

Guidelines for Cisco UCS Passwords

A password is required for each locally authenticated user account. A user with admin, aaa, or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

Cisco recommends that each user have a strong password. If you enable the password strength check for locally authenticated users, Cisco UCS Central rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

Web Session Limits for User Accounts

Cisco UCS Central does not support managing a number of concurrent web sessions at this time. We do support 32 concurrent web sessions for Cisco UCS Central users and a total of 256 concurrent sessions for all users.

Configuring User Roles

User Roles

User roles contain one or more privileges that define the operations that are allowed for a user. One or more roles can be assigned to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role2 has server-related privileges, users with Role1 and Role2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Each domain group in Cisco UCS Central can contain 48 user roles, including the user roles that are inherited from the parent domain group. When user roles are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 roles will be active. Any user roles after the first 48 will be inactive with faults raised.

All roles include read access to all configuration settings in the Cisco UCS domain. Users with read-only roles cannot modify the system state.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users that have that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have a different set of privileges, but a new Server and Storage Administrator role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

User profiles on AAA servers (RADIUS or TACACS+) should be modified to add the roles corresponding to the privileges granted to that user. The attribute is used to store the role information. The AAA servers return this attribute with the request and parse it to get the roles. LDAP servers return the roles in the user profile attributes.

Default User Roles

The system contains the following default user roles:

AAA Administrator

Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

Administrator

Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.

Facility Manager

Read-and-write access to power management operations through the power-mgmt privilege. Read access to the rest of the system.

Network Administrator

Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the rest of the system.

Operations

Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the rest of the system.

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Server Compute

Read and write access to most aspects of service profiles. However the user cannot create, modify or delete vNICs or vHBAs.

Server Equipment Administrator

Read-and-write access to physical server related operations. Read access to the rest of the system.

Server Profile Administrator

Read-and-write access to logical server related operations. Read access to the rest of the system.

Server Security Administrator

Read-and-write access to server security related operations. Read access to the rest of the system.

Storage Administrator

Read-and-write access to storage operations. Read access to the rest of the system.

Reserved Words: User Roles

The following words cannot be used when creating custom roles in Cisco UCS.

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Table 1: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator

Privilege	Description	Default Role Assignment
admin	System administration	Administrator
domain-group-management	Domain Group Management	Domain Group Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator

Privilege	Description	Default Role Assignment
server-security	Server security	Server Security Administrator
service-profile-compute	Service profile compute	Server Compute Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile end point access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Security Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator

Creating a User Role

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the user role.

a) Expand the **Domain Groups** node.

b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following choices:

- Click **Operational Policies**.

- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane navigate to **Roles**.
a) Click **Security**.
b) Expand the **User Services** node.
c) Click **Roles**.

Step 5 Click **Create Role**.
You can also right-click **Roles** to access that option.

Step 6 In the **Create Role** dialog box, enter the **Name** to assign the role.

Step 7 Select all **Privileges** for the role.

Step 8 Click **OK**.

Deleting a User Role

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the user role.
a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following choices:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all roles.
a) Click **Security**.
b) Expand the **User Services** node.
c) Expand the **Roles** node.

Step 5 Click the role which you want to delete.

Step 6 Click **Delete**.
You can also right-click a **Role** to access that option.

Step 7 In the **Confirm** dialog box, click **Yes**.

Adding Privileges to a User Role

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the user role.

a) Expand the **Domain Groups** node.

b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following choices:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all roles.

a) Click **Security**.

b) Expand the **User Services** node.

c) Expand the **Roles** node.

Step 5 Choose the role to which you want to add privileges.

Step 6 Click **Properties**.
You can also right-click a **Role** to access that option.

Step 7 In the **Properties** dialog box, check the boxes for the privileges you want to add to the role.

Step 8 Click **Save Changes**.

Removing Privileges from a User Role

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the user role.

a) Expand the **Domain Groups** node.

b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following choices:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all roles.

a) Click **Security**.

b) Expand the **User Services** node.
c) Expand the **Roles** node.

Step 5 Choose the role from which you want to remove privileges.

Step 6 Click **Properties**.
You can also right-click a **Role** to access that option.

Step 7 In the **Properties** dialog box, uncheck the boxes for the privileges you want to remove from the role.

Step 8 Click **Save Changes**.

Configuring Locally Authenticated User Accounts

Creating a Locally Authenticated User Account

At a minimum, we recommend that you create the following users:

- Server administrator account
- Network administrator account
- Storage administrator

Before You Begin

Perform the following tasks, if the system includes any of the following:

- Remote authentication services, ensure the users exist in the remote authentication server with the appropriate roles and privileges.
- Multi-tenancy with organizations, create one or more locales. If you do not have any locales, all users are created in root and are assigned roles and privileges in all organizations.
- SSH authentication, obtain the SSH key.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 Click **Create Locally Authenticated User**.

Step 5 In the **Create Locally Authenticated User** dialog box, complete the following fields:

Name	Description
Login ID field	The username for the local Cisco UCS Central user. Login IDs must meet the following the following restrictions: • The login ID can contain between 1 and 32 characters, including the following: ◦ Any alphabetic character ◦ Any digit ◦ _ (underscore) ◦ - (dash) ◦ . (dot) • The login ID must be unique within Cisco UCS Central. • The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore. • The login ID is case-sensitive. • You cannot create an all-numeric login ID. • After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.
Description field	The description of the user account. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote).
First Name field	The first name of the user. Enter up to 32 characters or spaces.
Last Name field	The last name of the user. Enter up to 32 characters or spaces.
Email field	The email address for the user.
Phone field	The telephone number for the user.

Name	Description
Password field	The password associated with this account. If password strength check is enabled, a user's password must be strong. Strong passwords must meet the following requirements: • Must contain a minimum of 8 characters and a maximum of 80 characters. • Must contain at least three of the following: ◦ Lower case letters ◦ Upper case letters ◦ Digits ◦ Special characters • Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb. • Must not be identical to the username or the reverse of the username. • Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word. • Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign). • Should not be blank for local user and admin accounts.
Set field	Whether the password has been set for this user.
Confirm Password field	The password a second time for confirmation purposes.
Account Expiration check box	If checked, this account expires and cannot be used after the date specified in the **Expiration Date** field.
Account Status drop-down list	If the status is set to **Active**, a user can log into Cisco UCS Central with this login ID and password.
Expiration Date field	The date on which the account expires. The date should be in the format mm/dd/yyyy. Click the calendar icon at the end of this field to view a calendar that you can use to select the expiration date.

Step 6 In the **Create Locally Authenticated User** dialog box, click the **Roles/Locales** tab and complete the following fields:

Name	Description
Assigned Roles list box	A list of the user roles defined in Cisco UCS Central. If the associated check box is checked, the selected user has been assigned that user role.
Assigned Locales list box	A list of the locales defined in Cisco UCS Central. If the associated check box is checked, the selected user has been assigned that locale.

Step 7 (Optional) If the system includes organizations, check one or more check boxes in the **Assigned Role(s)** pane to assign the user to the appropriate locales.

Note Do not assign locales to users with an admin role.

Step 8 In the **Create Locally Authenticated User** dialog box, click the **SSH** tab and complete the following fields:

Name	Description
Type field	This can be one of the following: • **Key**—SSH encryption is used when this user logs in. • **Password**—The user must enter a password when they log in.
SSH Data field	If **Type** is set to **Key**, this field contains the associated SSH key.

Step 9 Click **OK**.

Deleting a Locally Authenticated User Account

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.

Step 4 Right-click the **User** you want to delete, and choose **Delete**.

Step 5 In the **Confirm** dialog box, click **Yes**.

Changing the Roles Assigned to a Locally Authenticated User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.

Step 4 Click the user account that you want to modify.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Work** pane, click the **Roles/Locales** tab.

Step 7 In the **Assigned Role(s)** area, assign and remove roles.

- To assign a new role to the user account, check the appropriate check boxes.
- To remove a role from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Enabling the Password Strength Check for Locally Authenticated Users

You must be a user with admin, aaa, or domain-group-management privileges to enable the password strength check. If the password strength check is enabled, Cisco UCS Central does not permit a user to choose a password that does not meet the guidelines for a strong password.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Work** pane, check the **Password Strength Check** check box in the **Properties** area.

Step 5 Click **Save**.

Clearing the Password History for a Locally Authenticated User

You must have admin, aaa, or domain-group-management privileges to change the password profile properties.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Password Profile** area, enter 0 for the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password in the **History Count** field.
Setting the **History Count** field to 0 (the default setting) disables the history count and allows users to reuse previously used passwords at any time.

Step 5 Click **Save**.

Enabling a Locally Authenticated User Account

You must be a user with admin, aaa, or domain-group-management privileges to enable or disable a local user account.

Before You Begin

Create a local user account.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.

Step 4 Click the user account that you want to modify.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Account Status** field, click the **active** radio button.

Step 7 Click **Save**.

Disabling a Locally Authenticated User Account

You must be a user with admin, aaa, or domain-group-management privileges to enable or disable a local user account.

Note If you change the password on a disabled account through the Cisco UCS Central GUI, the user cannot use this changed password after you enable the account and make it active. The user must enter the required password again after the account is enabled and made active.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.

Step 4 Click the user account that you want to modify.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Account Status** field, click the **inactive** radio button.
The admin user account is always set to active. It cannot be modified.

Step 7 Click **Save**.

Configuring User Locales

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) the user is allowed access, and access would be limited to the organizations specified in the locale. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Each domain group in Cisco UCS Central can contain 48 user locales, including the user locales that are inherited from the parent domain group. When user locales are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 locales will be active. Any user locales after the first 48 will be inactive with faults raised.

Users with admin, aaa, or domain-group-management privileges can assign organizations to the locale of other users.

Note You cannot assign a locale to users with the admin privilege.

You can hierarchically manage organizations. A user that is assigned at a top level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

Creating a User Locale

Before You Begin

One or more organizations must exist before you create a locale.

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the locale.

a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane navigate to **Locales**.

a) Click **Security**.
b) Expand the **User Services** node.
c) Click **Locales**.

Step 5 Click **Create Locales**.
You can also right-click **Locales** to access that option.

Step 6 In the **Create Locale** dialog box enter requested information.

a) In the **Name** field, enter a unique name for the locale.
This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
b) In the **Description** field, enter a description for the locale.

Step 7 Click **Filter**.

Step 8 In the **Table Filter** dialog box enter requested information.

a) Choose the **Assigned Organization** filter.
b) Enter the **Assigned Organization** filter value.

Step 9 Click **OK**.

Step 10 Click **Assign Organization**.

Step 11 In the **Assign Organizations** dialog box assign the organization to the locale.

a) Expand the **Organizations** area to view the organizations in the Cisco UCS domain.
b) Expand the **root** node to see the sub-organizations.
c) Click an organization that you want to assign to the locale.
d) Drag the organization from the **Organizations** area and drop it into the design area on the right.
e) Repeat Steps b and c until you have assigned all desired organizations to the locale.

Step 12 Click **OK** to assign organization.

Step 13 Click **OK** to create locale.

Deleting a User Locale

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the locale.

a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all locales.

a) Click **Security**.
b) Expand the **User Services** node.
c) Expand the **Locales** node.

Step 5 Click the locale which you want to delete.

Step 6 Click **Delete**.
You can also right-click a **Locale** you want to delete to access that option.

Step 7 In the **Confirm** dialog box, click **Yes**.

Assigning an Organization to a User Locale

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the locale.

a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane select a locale.

a) Click **Security**.
b) Expand the **User Services** node.

c) Expand the **Locales** node.

Step 5 Click the locale to which you want to add an organization.

Step 6 Click **Assign Organization**.
You can also right-click the **Locale** to access that option.

Step 7 In the **Assign Organizations** dialog box enter the **Organization**.

Step 8 Click **OK**.

Deleting an Organization from a User Locale

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane select a domain group for the locale.

a) Expand the **Domain Groups** node.
b) Expand the **Domain Groups root** node.

Step 3 Under the **Domain Groups** node, do one of the following:

- Click **Operational Policies**.
- Expand a **Domain Group** node and click **Operational Policies**.

Step 4 In the **Work** pane display all locales.

a) Click **Security**.
b) Expand the **User Services** node.
c) Expand the **Locales** node.

Step 5 Click the locale with an assigned organization you want to delete.

Step 6 Click **Properties**.

Step 7 In the **Work** pane, click the **Organization** you want to delete.

Step 8 Click **Delete**.
You can also right-click an **Organization** you want to delete to access that option.

Step 9 In the **Confirm** dialog box, click **Yes**.

Changing the Locales Assigned to a Locally Authenticated User Account

Note Do not assign locales to users with an admin role.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, expand **Locally Authenticated Users**.

Step 4 Click the user account that you want to modify.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Work** pane, click the **Roles/Locales** tab.

Step 7 In the **Assigned Locale(s)** area, assign and remove locales.

- To assign a new locale to the user account, check the appropriate check boxes.
- To remove a locale from the user account, uncheck the appropriate check boxes.

Step 8 Click **Save**.

Configuring User Domain Groups

Creating a User Domain Group

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, click **Domain Groups** and do one of the following choices:

- In the **Domain Groups** pane under the **Name** column, click a **Domain Group** and click **Create Domain Group**.
- In the **Navigation** pane, click **Domain Groups root** and click **Create Domain Group**.
- In the **Navigation** pane, expand the **Domain Groups root** node, click a **Domain Group** and click **Create Domain Group**.

Step 3 In the **Create Domain Group** dialog box enter requested information.

a) In the **Name** field, enter a unique name for the domain group.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

b) In the **Description** field, enter a description for the domain group.

Step 4 Click **OK** to create domain group.

Deleting a User Domain Group

Procedure

Step 1 On the menu bar, click **Operations Management**.

Step 2 In the **Navigation** pane, click **Domain Groups**.

Step 3 In the **Domain Groups** pane under the **Name** column, click the **Domain Group** you want to delete.

Step 4 Click **Delete**.
You can also right-click the **Domain Group** you want to delete to access that option.

Note You cannot delete the domain group root.

Step 5 In the **Confirm** dialog box, click **Yes**.

Configuring User Organizations

User Organizations

A user can create one or more organizations. Each organization defines sub-organizations, faults, events, UUID suffix pools and blocks of UUIDs.

Cisco UCS organizations are hierarchically managed by users. A user that is assigned at the root level organization has automatic access to all organizations and domain groups under it.

Creating a User Organization

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane create an organization.

a) Expand the **Pools** node.
b) Click **root**.
c) In the **Work** pane, click **Create Organization**.

Step 3 In the **Create Organization** dialog box enter requested information.

a) In the **Name** field, enter a unique name for the organization.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

b) In the **Description** field, enter a description for the organization.

Step 4 Click **OK** to create an organization.

Deleting a User Organization

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane select an organization.

a) Expand the **Pools** node.
b) Expand the **root** node.
c) Click **Sub-Organizations**.
d) In the **Sub-Organizations** pane, click the **Organization** you want to delete.

Step 3 Click **Delete**.
You can also right-click the **Organization** you want to delete to access that option.

Step 4 In the **Confirm** dialog box, click **Yes**.

Creating a User Sub-Organization

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane create a sub-organization.

a) Expand the **Pools** node.
b) Expand the **root** node.
c) Click **Sub-Organizations**.

Step 3 In the **Sub-Organizations** pane, click applicable assigned organization name.

Step 4 In the **Work** pane, click **Create Organization**.

Step 5 In the **Create Organization** dialog box enter requested information.

a) In the **Name** field, enter a unique name for the organization.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

b) In the **Description** field, enter a description for the organization.

Step 6 Click **OK** to create a sub-organization.

Deleting a User Sub-Organization

Procedure

Step 1 On the menu bar, click **Servers**.

Step 2 In the **Navigation** pane select an organization.

a) Expand the **Pools** node.
b) Expand the **root** node.
c) Click **Sub-Organizations**.
d) In the **Sub-Organizations** pane, expand applicable assigned organization node.
e) In the **Sub-Organizations** pane, click the **Organization** you want to delete.
Expand applicable assigned organization nodes until reaching the applicable organization name.

Step 3 Click **Delete**.
You can also expand the **Organizations** until reaching the target you want to delete, and right-click an **Organization** to access that option.

Step 4 In the **Confirm** dialog box, click **Yes**.

Configuring Passwords

Password Profile for Locally Authenticated Users

The password profile contains the password history and password change interval properties for all locally authenticated users of Cisco UCS Central. You cannot specify a different password profile for each locally authenticated user.

Note You must have admin, aaa, or domain-group-management privileges to change the password profile properties. Except for password history, these properties do not apply to users with these administrative privileges.

Password History Count

The password history count allows you to prevent locally authenticated users from reusing the same password over and over again. When this property is configured, Cisco UCS Central stores passwords that were previously used by locally authenticated users up to a maximum of 15 passwords. The passwords are stored in reverse chronological order with the most recent password first to ensure that the only the oldest password can be reused when the history count threshold is reached.

A user must create and use the number of passwords configured in the password history count before being able to reuse one. For example, if you set the password history count to 8, a locally authenticated user cannot reuse the first password until after the ninth password has expired.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously passwords at any time.

If necessary, you can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

The password change interval enables you to restrict the number of password changes a locally authenticated user can make within a given number of hours. The following table describes the two configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	This option does not allow passwords for locally authenticated users to be changed within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.	For example, to prevent passwords from being changed within 48 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to disable • No change interval to 48
Password changes allowed within change interval	This option specifies the maximum number of times that passwords for locally authenticated users can be changed within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of 2 password changes within a 48 hour interval.	For example, to allow to be changed a maximum of once within 24 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to enable • Change count to 1 • Change interval to 24

Configuring the Maximum Number of Password Changes for a Change Interval

You must have admin or aaa privileges to change the password profile properties. Except for password history, these properties do not apply to users with admin or aaa privileges.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Password Profile** area complete all fields.

a) In the **Change During Interval** field, click **Enable**.

b) In the **Change Interval** field, enter the maximum number of hours over which the number of password changes specified in the **Change Count** field are enforced.
This value can be anywhere from 1 to 745 hours.

For example, if this field is set to 48 and the**Change Count** field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.

c) In the **Change Count** field, enter the maximum number of times a locally authenticated user can change his or her password during the Change Interval.
This value can be anywhere from 0 to 10.

Step 5 Click **Save**.

Configuring a No Change Interval for Passwords

You must have admin or aaa privileges to change the password profile properties. Except for password history, these properties do not apply to users with admin or aaa privileges.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Password Profile** area complete all fields.

a) In the **Change During Interval** field, click **Disable**.

b) In the **No Change Interval** field, enter the minimum number of hours that a locally authenticated user must wait before changing a newly created password.
This value can be anywhere from 1 to 745 hours.

This interval is ignored if the **Change During Interval** property is not set to **Disable**.

Step 5 Click **Save**.

Configuring the Password History Count

You must have admin or aaa privileges to change the password profile properties.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 In the **Navigation** pane, click the **Access Control** tab.

Step 3 On the **Access Control** tab, click **Locally Authenticated Users**.

Step 4 In the **Password Profile** area, enter the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password in the **History Count** field.
This value can be anywhere from 0 to 15.

By default, the **History Count** field is set to 0, which disables the history count and allows users to reuse previously used passwords at any time.

Step 5 Click **Save**.

Monitoring User Sessions

You can monitor Cisco UCS Central sessions for both locally authenticated users and remotely authenticated users, whether they logged in through the CLI or the GUI.

Procedure

Step 1 On the menu bar, click **Administration**.

Step 2 On the **Access Control** tab, click **Locally Authenticated Users** or **Remotely Authenticated Users**.

Step 3 In the **Navigation** pane, user sessions are monitored under **Locally Authenticated Users** for all users or each user.

- In the **Navigation** pane, click **Locally Authenticated Users** to monitor all user sessions.
- In the **Navigation** pane, expand the **Locally Authenticated Users** node and click a user name to monitor that individual user.

Step 4 In the **Work** pane, click the **Sessions** tab.
The tab displays the following details of user sessions:

Name	Description
Filter button	Allows you to filter the data in the table. When you apply a filter, this button name changes to **Filter (on)**.
Terminate Session button	Ends the selected user session.

Name	Description
Host column	The IP address from which the user logged in.
Login Time column	The date and time at which the user logged in.
Terminal Type column	The type of terminal from which the user logged in.
Current Session column	Whether the session is currently active.