Configuring Role-Based Access Control

This chapter includes the following sections:

- Role-Based Access Control, page 1
- User Accounts for Cisco UCS Manager, page 1
  - User Roles, page 4
  - User Locales, page 8
  - Configuring User Roles, page 9
  - Configuring Locales, page 11
  - Configuring Locally Authenticated User Accounts, page 13
  - Password Profile for Locally Authenticated Users, page 20
  - Monitoring User Sessions, page 22

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 Manager

User accounts are used to access the system. Up to 48 user accounts can be configured in each Cisco UCS 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**

Each Cisco UCS domain 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.

**Locally Authenticated User Accounts**

A locally authenticated user account is authenticated directly through the fabric interconnect 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 user account that is authenticated through LDAP, RADIUS, or 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.

---

**Guidelines for Cisco UCS Manager Usernames**

The username is also used as the login ID for Cisco UCS Manager. When you assign usernames to Cisco UCS Manager 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 unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username.

• The unique username must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.

After you create a user account, you cannot change the username. 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 Manager.

• root
• bin
• daemon
• adm
• ip
• sync
• shutdown
• halt
• news
• uucp
• operator
• games
• gopher
• nobody
• nsed
• mailnull
• mail
• rpcuser
• rpc
• mtsuser
• ftpuser
• ftp
• man
• sys
• samdme
Guidelines for Cisco UCS Manager Passwords

A password is required for each locally authenticated user account. A user with admin or aaa privileges can configure Cisco UCS Manager 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 Manager rejects any password that does not meet the following requirements:

• Must contain a minimum of 8 characters and a maximum of 64 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 aaabb.
• 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

Web session limits are used by Cisco UCS Manager to restrict the number of web sessions (both GUI and XML) a given user account is permitted to access at any one time.

By default, the number of concurrent web sessions allowed by Cisco UCS Manager is set to 32; although this value can be configured up to the system maximum of 256.

User Roles

User roles contain one or more privileges that define the operations allowed for the user who is assigned the role. A user can be assigned one or more roles. A user assigned multiple roles has the combined privileges of all assigned roles. For example, if Role1 has storage related privileges, and Role2 has server related privileges, users who are assigned to both Role1 and Role2 have storage and server related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles.
All roles include read access to all configuration settings in the Cisco UCS domain. The difference between the read-only role and other roles is that a user who is only assigned the read-only role cannot modify the system state. A user assigned another role can modify the system state in that user's assigned area or areas.

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 assigned to 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 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.

---

**Note**
If a local user account and a remote user account have the same username, any roles assigned to the remote user are overridden by those assigned to the local user.

---

### 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 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 Manager.

• 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

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>Default Role Assignment</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>System security and AAA</td>
<td>AAA Administrator</td>
</tr>
<tr>
<td>admin</td>
<td>System administration</td>
<td>Administrator</td>
</tr>
<tr>
<td>ext-lan-config</td>
<td>External LAN configuration</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>ext-lan-policy</td>
<td>External LAN policy</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>ext-lan-qos</td>
<td>External LAN QoS</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>ext-lan-security</td>
<td>External LAN security</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>ext-san-config</td>
<td>External SAN configuration</td>
<td>Storage Administrator</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
<td>Default Role Assignment</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>ext-san-policy</td>
<td>External SAN policy</td>
<td>Storage Administrator</td>
</tr>
<tr>
<td>ext-san-qos</td>
<td>External SAN QoS</td>
<td>Storage Administrator</td>
</tr>
<tr>
<td>ext-san-security</td>
<td>External SAN security</td>
<td>Storage Administrator</td>
</tr>
<tr>
<td>fault</td>
<td>Alarms and alarm policies</td>
<td>Operations</td>
</tr>
<tr>
<td>operations</td>
<td>Logs and Smart Call Home</td>
<td>Operations</td>
</tr>
<tr>
<td>pod-config</td>
<td>Pod configuration</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>pod-policy</td>
<td>Pod policy</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>pod-qos</td>
<td>Pod QoS</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>pod-security</td>
<td>Pod security</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>power-mgmt</td>
<td>Read-and-write access to power management operations</td>
<td>Facility Manager</td>
</tr>
<tr>
<td>read-only</td>
<td>Read-only access</td>
<td>Read-Only</td>
</tr>
<tr>
<td>server-equipment</td>
<td>Server hardware management</td>
<td>Server Equipment Administrator</td>
</tr>
<tr>
<td>server-maintenance</td>
<td>Server maintenance</td>
<td>Server Equipment Administrator</td>
</tr>
<tr>
<td>server-policy</td>
<td>Server policy</td>
<td>Server Equipment Administrator</td>
</tr>
<tr>
<td>server-security</td>
<td>Server security</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-config</td>
<td>Service profile configuration</td>
<td>Server Profile Administrator</td>
</tr>
<tr>
<td>service-profile-config-policy</td>
<td>Service profile configuration policy</td>
<td>Server Profile Administrator</td>
</tr>
<tr>
<td>service-profile-ext-access</td>
<td>Service profile end point access</td>
<td>Server Profile Administrator</td>
</tr>
<tr>
<td>service-profile-network</td>
<td>Service profile network</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>service-profile-network-policy</td>
<td>Service profile network policy</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>service-profile-qos</td>
<td>Service profile QoS</td>
<td>Network Administrator</td>
</tr>
<tr>
<td>service-profile-qos-policy</td>
<td>Service profile QoS policy</td>
<td>Network Administrator</td>
</tr>
</tbody>
</table>
### 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.

Users with AAA privileges (AAA Administrator role) can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization then a user assigned that locale can only assign the Engineering organization to other users.

**Note**

You cannot assign a locale to users with one or more of the following privileges:

- `aaa`
- `admin`
- `operations`

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.
Configuring User Roles

Creating a User Role

Procedure

Step 1  In the Navigation pane, click the Admin tab.
Step 2  On the Admin tab, expand All > User Management > User Services.
Step 3  Right-click User Services and choose Create Role.
         You can also right-click Roles to access that option.
Step 4  In the Create Role dialog box, complete the following fields:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name field</td>
<td>A user-defined name for this user role. This name can be between 1 and 16</td>
</tr>
<tr>
<td></td>
<td>alphanumeric characters. You cannot use spaces or any special characters</td>
</tr>
<tr>
<td></td>
<td>other than - (hyphen), _ (underscore), : (colon), and . (period), and you</td>
</tr>
<tr>
<td></td>
<td>cannot change this name after the object has been saved.</td>
</tr>
<tr>
<td>Privileges list box</td>
<td>A list of the privileges defined in the system. Click a privilege to view</td>
</tr>
<tr>
<td></td>
<td>a description of that privilege. Check the check box to assign that</td>
</tr>
<tr>
<td></td>
<td>privilege to the selected user.</td>
</tr>
<tr>
<td>Help Section</td>
<td></td>
</tr>
<tr>
<td>Description field</td>
<td>A description of the most recent privilege you clicked in the Privileges</td>
</tr>
<tr>
<td></td>
<td>list box.</td>
</tr>
</tbody>
</table>

Step 5  Click OK.
Adding Privileges to a User Role

Procedure

Step 1  In the Navigation pane, click the Admin tab.
Step 2  On the Admin tab, expand All > User Management > User Services.
Step 3  Expand the Roles node.
Step 4  Choose the role to which you want to add privileges.
Step 5  In the General tab, check the boxes for the privileges you want to add to the role.
Step 6  Click Save Changes.

Removing Privileges from a User Role

Procedure

Step 1  In the Navigation pane, click the Admin tab.
Step 2  On the Admin tab, expand All > User Management > User Services.
Step 3  Expand the Roles node.
Step 4  Choose the role from which you want to remove privileges.
Step 5  In the General tab, uncheck the boxes for the privileges you want to remove from the role.
Step 6  Click Save Changes.

Deleting a User Role

When you delete a user role, Cisco UCS Manager removes that role from all user accounts to which the role has been assigned.

Procedure

Step 1  In the Navigation pane, click the Admin tab.
Step 2  On the Admin tab, expand All > User Management > User Services.
Step 3  Expand the Roles node.
Step 4  Right-click the role you want to delete and choose Delete.
Step 5  In the Delete dialog box, click Yes.
Configuring Locales

Creating a Locale

Before You Begin

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

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services.
Step 3 Right-click Locales and choose Create a Locale.
Step 4 In the Create Locale page, do the following:
   a) In the Name field, enter a unique name for the locale.
      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) Click Next.
Step 5 In the Assign Organizations dialog box, do the following:
   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 6 Click Finish.

What to Do Next

Add the locale to one or more user accounts. For more information, see Changing the Locales Assigned to a
Locally Authenticated User Account, on page 17.
Assigning an Organization to a Locale

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services.
Step 3 Expand the Locales node and click the locale to which you want to add an organization.
Step 4 In the Work pane, click the General tab.
Step 5 In the Organizations area, click + on the table icon bar.
Step 6 In the Assign Organizations dialog box, do the following:
   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 7 Click OK.

Deleting an Organization from a Locale

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services.
Step 3 Expand the Locales node and click the locale from which you want to delete an organization.
Step 4 In the Work pane, click the General tab.
Step 5 In the Organizations area, right-click the organization that you want to delete from the locale and choose Delete.
Step 6 Click Save Changes.
Deleting a Locale

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services.
Step 3 Expand the Locales node.
Step 4 Right-click the locale you want to delete and choose Delete.
Step 5 If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes.

Configuring Locally Authenticated User Accounts

Creating a 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 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services.
Step 3 Right-click User Services and choose Create User to open the User Properties dialog box. You can also right-click Locally Authenticated Users to access that option.
Step 4 Complete the following fields with the required information about the user:
### Creating a User Account

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Login ID field** | The account name that is used when logging into this account. This account must be unique and meet the guidelines and restrictions for Cisco UCS Manager user accounts.  
  - The login ID can contain between 1 and 32 characters, including the following:  
    - Any alphabetic character  
    - Any digit  
    - _ (underscore)  
    - - (dash)  
    - . (dot)  
  - The unique username for each user account cannot be all-numeric. You cannot create a local user with an all-numeric username.  
  - The unique username must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.  
  After you save the user, the login ID cannot be changed. You must delete the user account and create a new one. |
| **First Name field** | The first name of the user. This field can contain up to 32 characters.  

| **Last Name field** | The last name of the user. This field can contain up to 32 characters. |
| **Email field** | The email address for the user. |
| **Phone field** | The telephone number for the user. |
The password associated with this account. If password strength check is enabled, a user’s password must be strong and Cisco UCS Manager rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 64 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 aaaa.
- 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.

The password a second time for confirmation purposes.

If the status is set to Active, a user can log into Cisco UCS Manager with this login ID and password.

If checked, this account expires and cannot be used after the date specified in the Expiration Date field.

The date on which the account expires. The date should be in the format yyyy-mm-dd.

Click the down arrow at the end of this field to view a calendar that you can use to select the expiration date.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Password** field  | The password associated with this account. If password strength check is enabled, a user’s password must be strong and Cisco UCS Manager rejects any password that does not meet the following requirements:  
  - Must contain a minimum of 8 characters and a maximum of 64 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 aaaa.  
  - 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. |
| **Confirm Password** field | The password a second time for confirmation purposes.                                                                                     |
| **Account Status** field | If the status is set to Active, a user can log into Cisco UCS Manager with this login ID and password.                                   |
| **Account Expires** check box | If checked, this account expires and cannot be used after the date specified in the Expiration Date field.                       |
| **Expiration Date** field | The date on which the account expires. The date should be in the format yyyy-mm-dd.  
  Click the down arrow at the end of this field to view a calendar that you can use to select the expiration date. |
| **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.  
  Cisco UCS Manager GUI displays this field when you check the Account Expires check box. |
Enabling the Password Strength Check for Locally Authenticated Users

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

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services.
Step 3 Click the Locally Authenticated Users node.
Step 4 In the Work pane, check the Password Strength Check check box in the Properties area.
Step 5 Click Save Changes.

Setting the Web Session Limits for Cisco UCS Manager GUI Users

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > Communication Management > Communication Services.
Step 3 Click the Communication Services tab.
Step 4 In the Web Session Limits area, complete the following fields:
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Sessions Per User field</td>
<td>The maximum number of concurrent HTTP and HTTPS sessions allowed for each user. Enter an integer between 1 and 256.</td>
</tr>
<tr>
<td>Maximum Sessions field</td>
<td>The maximum number of concurrent HTTP and HTTPS sessions allowed for all users within the system. Enter an integer between 1 and 256.</td>
</tr>
</tbody>
</table>

**Step 5** Click **Save Changes**.

## Changing the Locales Assigned to a Locally Authenticated User Account

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

**Procedure**

**Step 1** In the **Navigation** pane, click the **Admin** tab.

**Step 2** On the **Admin** tab, expand **All > User Management > User Services > Locally Authenticated Users**.

**Step 3** Click the user account that you want to modify.

**Step 4** In the **Work** pane, click the **General** tab.

**Step 5** In the **Locales** area, do the following:

- 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 6** Click **Save Changes**.

## 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 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services > Locally Authenticated Users.
Step 3 Click the user account that you want to modify.
Step 4 In the Work pane, click the General tab.
Step 5 In the Roles area, do the following:
   • 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 6 Click Save Changes.

Enabling a User Account

You must be a user with admin or aaa privileges to enable or disable a local user account.

Before You Begin
Create a local user account.

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services > Locally Authenticated Users.
Step 3 Click the user that you want to enable.
Step 4 In the Work pane, click the General tab.
Step 5 In the Account Status field, click the active radio button.
Step 6 Click Save Changes.

Disabling a User Account

You must be a user with admin or aaa privileges to enable or disable a local user account.

Note
If you change the password on a disabled account through the Cisco UCS Manager 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.
Clearing the Password History for a Locally Authenticated User

Procedure

1. In the Navigation pane, click the Admin tab.
2. On the Admin tab, expand All > User Management > User Services > Locally Authenticated Users.
3. Click the user for whom you want to clear the password history.
4. In the Actions area, click Clear Password History.
5. If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes.

Deleting a Locally Authenticated User Account

Procedure

1. In the Navigation pane, click the Admin tab.
2. On the Admin tab, expand All > User Management > User Services.
3. Expand the Locally Authenticated Users node.
4. Right-click the user account you want to delete and choose Delete.
5. In the Delete dialog box, click Yes.
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 Manager. You cannot specify a different password profile for each locally authenticated user.

**Note**
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.

**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 Manager 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.

<table>
<thead>
<tr>
<th>Interval Configuration</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| No password change allowed | This option does not 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 |
**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** In the **Navigation** pane, click the **Admin** tab.

**Step 2** On the **Admin** tab, expand **All > User Management > User Services**.

**Step 3** Click the **Locally Authenticated Users** node.

**Step 4** In the **Password Profile** area, do the following:

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

b) 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.

c) 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.

**Step 5** Click **Save Changes**.

**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.

### Interval Configuration

<table>
<thead>
<tr>
<th>Interval Configuration</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
</table>
| 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 Password History Count

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

Procedure

Step 1 In the Navigation pane, click the Admin tab.
Step 2 On the Admin tab, expand All > User Management > User Services.
Step 3 Click the Locally Authenticated Users node.
Step 4 In the Password Profile area, do the following:
   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 Changes.

Monitoring User Sessions

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

Step 1  In the Navigation pane, click the Admin tab.
Step 2  In the Admin tab, expand All > User Management.
Step 3  Click the User Services node.
Step 4  In the Work pane, click the Sessions tab.

The tab displays the following details of user sessions:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name column</td>
<td>The name for the session.</td>
</tr>
<tr>
<td>User column</td>
<td>The username that is involved in the session.</td>
</tr>
<tr>
<td>Fabric ID column</td>
<td>The fabric interconnect that the user logged in to for the session.</td>
</tr>
<tr>
<td>Login Time column</td>
<td>The date and time the session started.</td>
</tr>
<tr>
<td>Refresh Period column</td>
<td>When a web client connects to Cisco UCS Manager, the client needs to send</td>
</tr>
<tr>
<td></td>
<td>refresh requests to Cisco UCS Manager to keep the web session active.</td>
</tr>
<tr>
<td></td>
<td>This option specifies the maximum amount of time allowed between refresh</td>
</tr>
<tr>
<td></td>
<td>requests for a user in this domain.</td>
</tr>
<tr>
<td></td>
<td>If this time limit is exceeded, Cisco UCS Manager considers the web session</td>
</tr>
<tr>
<td></td>
<td>to be inactive, but it does not terminate the session.</td>
</tr>
<tr>
<td>Session Timeout column</td>
<td>The maximum amount of time that can elapse after the last refresh request</td>
</tr>
<tr>
<td></td>
<td>before Cisco UCS Manager considers a web session to have ended.</td>
</tr>
<tr>
<td></td>
<td>If this time limit is exceeded, Cisco UCS Manager automatically</td>
</tr>
<tr>
<td></td>
<td>terminates the web session.</td>
</tr>
<tr>
<td>Terminal Type column</td>
<td>The kind of terminal the user is logged in through.</td>
</tr>
<tr>
<td>Host column</td>
<td>The IP address from which the user is logged in.</td>
</tr>
<tr>
<td>Current Session column</td>
<td>If this column displays Y, the associated user session is currently active.</td>
</tr>
</tbody>
</table>

When a web client connects to Cisco UCS Manager, the client needs to send refresh requests to Cisco UCS Manager to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Manager considers the web session to be inactive, but it does not terminate the session.