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 3
  - Privileges, page 4
  - User Locales, page 6
  - Configuring User Roles, page 6
  - Configuring Locales, page 8
  - Configuring User Accounts, page 10
  - Monitoring User Sessions, page 14

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 instance. 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.

**Default User Account**

Each Cisco UCS instance has a default user account, admin, which 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.

**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)
  - @

- 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 cannot start with a number.

- If an all-numeric username exists on an AAA server (RADIUS or TACACS+) and is entered during login, Cisco UCS Manager cannot log in the user.

After you create a user account, you cannot change the username. You must delete the user account and create a new one.

**Note**

You can create up to 48 user accounts in a Cisco UCS instance.

**Guidelines for Cisco UCS Manager Passwords**

For authentication purposes, a password is required for each user account. To prevent users from choosing insecure passwords, each password must be strong. Cisco UCS Manager rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters.
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.

All roles include read access to all configuration settings in the Cisco UCS instance. 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.

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.

**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.

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 cisco-av-pair vendor-specific 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.

---

**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>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>Privilege</td>
<td>Description</td>
<td>Default Role Assignment</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------------</td>
<td>-------------------------------------</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>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>
<tr>
<td>service-profile-security</td>
<td>Service profile security</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-security-policy</td>
<td>Service profile security policy</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-server</td>
<td>Service profile server management</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-server-policy</td>
<td>Service profile pool policy</td>
<td>Server Security Administrator</td>
</tr>
<tr>
<td>service-profile-storage</td>
<td>Service profile storage</td>
<td>Storage 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.

Users with AAA Administrator 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.

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Navigation pane, click the Admin tab.</td>
</tr>
<tr>
<td>Step 2</td>
<td>On the Admin tab, expand All ➤ User Management ➤ User Services.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click User Services and choose Create Role.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Create Role dialog box, complete the following fields:</td>
</tr>
</tbody>
</table>

<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 alphanumeric characters. You cannot use spaces or any special characters, and you 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 a description of that privilege. Check the check box to assign that privilege to the selected user.</td>
</tr>
</tbody>
</table>

**Help Section**
Adding Privileges to a User Role

Procedure

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

Removing Privileges from a User Role

Procedure

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

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.
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 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.

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, 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 instance.
   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, page 13.
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 instance.
   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 Cisco UCS Manager GUI displays a confirmation dialog box, click Yes.

Configuring 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.
Step 4  Complete the following fields with the required information about the user:
### Configuring User Accounts

<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)  
    - @  
    - 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 cannot start with a number.  
    - If an all-numeric username exists on an AAA server (RADIUS or TACACS+) and is entered during login, Cisco UCS Manager cannot log in the user.  
  
  After you save the user, the login ID cannot be changed. You must delete the user account and create a new one.  
  **Note** You can create up to 48 user accounts in a Cisco UCS instance. |
| **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. |
| **Password field** | The password associated with this account. To prevent users from choosing insecure passwords, each password must be strong. Cisco UCS Manager rejects any password that does not meet the following requirements:  
  - Must contain a minimum of 8 characters.  
  - Must contain at least three of the following:  
    - Lower case letters  
    - Upper case letters  
    - Digits  
    - Special characters |
### Configuring User Accounts

**Name** | **Description**
--- | ---
• Must not contain a character that is repeated more than 3 times consecutively, such as aabbb.  
• 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.
**Password Expires check box** | If checked, this password expires and must be changed on a given date.
**Expiration Date field** | If Password Expires is checked, this field specifies the date on which the password 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.

**Step 5** In the **Roles** area, check one or more boxes to assign roles and privileges to the user account.
**Step 6** (Optional) If the system includes organizations, check one or more check boxes in the **Locales** area to assign the user to the appropriate locales.
**Step 7** In the **SSH** area, complete the following fields:
  a) In the **Type** field, do the following:
    • **Password Required**—The user must enter a password when they log in.  
    • **Key**—SSH encryption is used when this user logs in.
  b) If you chose **Key**, enter the SSH key in the **SSH data** field.
**Step 8** Click **OK**.
Changing the Locales Assigned to a Locally Authenticated 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 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

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.
Deleting a Locally Authenticated 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.
Step 3 Expand the Locally Authenticated Users node.
Step 4 Right-click the user account you want to delete and choose Delete.
Step 5 In the Delete dialog box, click Yes.

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>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>
</tbody>
</table>