Role-Based Access Configuration

Role-Based Access Control Overview

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 a locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, you can manage individual user privileges by assigning the appropriate roles and locales.

A user is granted write access to the required 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 can update server configurations in the Engineering organization. They cannot, however, 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 access the system. You can configure up to 48 local user accounts in each Cisco UCS Manager domain. Each user account requires a unique username and password.

You can set user accounts with an SSH public key. The public key can be set in either of the two formats: OpenSSH or SECSH.

Admin Account

An admin account comes with each Cisco UCS domain. The admin account is a default user account and cannot be modified or deleted. This account is the system administrator or superuser account s 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. After a local user account is disabled, the user cannot log in. The database does not delete the configuration details for disabled local user accounts. If you re-enable a disabled local user account, the account becomes active with the existing configuration, including the 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

You can configure user accounts 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. However, you can configure the account to use the latest expiration date available.

Reserved Words: Locally Authenticated User Accounts

You cannot use the following words when creating a local user account in Cisco UCS.

- root
- bin
- daemon
- adm
- lp
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher

- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

Web Session Limits for User Accounts

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

Each Cisco UCS Manager domain supports a maximum of 32 concurrent web sessions per user and 256 total user sessions. By default, the number of concurrent web sessions allowed by Cisco UCS Manager is set to 32 per user, but you can configure this value up to the system maximum of 256.

User Roles

User roles contain one or more privileges that define the operations that are allowed for a user. You can assign one or more roles to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role 2 has server-related privileges, users with Role1 and Role 2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Any user roles configured after the first 48 are accepted, but they are 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.

You can create, modify or remove existing privileges, and delete roles. When you modify a role, the new privileges apply to all users with that role. Privilege assignment is not restricted to the privileges defined for the default roles. Meaning, 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. However, you can create a Server and Storage Administrator role that combines the privileges of both roles.

Note If you delete a role after it was assigned to users, it is also deleted from those user accounts.

Modify the user profiles on AAA servers (RADIUS or TACACS+) to add the roles corresponding to the privileges granted to that user. The attribute stores the role information. The AAA servers return this attribute with the request and parse it to obtain the roles. LDAP servers return the roles in the user profile attributes.

Note If a local and a remote user account have the same username, Cisco UCS Manager overrides any roles assigned to the remote user with 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 remaining system.

Administrator

Complete read-and-write access to the entire system. Assigns this role to the default administrator account by default. You cannot change it.

Facility Manager

Read-and-write access to power management operations through the power management privilege. Read access to the remaining system.

Network Administrator

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

Operations

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

Server Profile Administrator

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

Server Security Administrator

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

Storage Administrator

Read-and-write access to storage operations. Read access to the remaining system.

Reserved Words: User Roles

You cannot use the following words 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.

Tip Detailed information about these privileges and the tasks that they enable users to perform is available in *Privileges in Cisco UCS* available at the following URL: http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html.

Table 1: User Privileges

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

Privilege	Description	Default Role Assignment
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
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 endpoint 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

Privilege	Description	Default Role Assignment
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 In the **Navigation** pane, click **Admin**.

Step 2 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:

Name	Description
Name field	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 other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Privileges list box	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.
Help Section	
Description field	A description of the most recent privilege you clicked in the **Privileges** list box.

Step 5 Click **OK**.

Adding Privileges to a User Role

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 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 **Admin**.
Step 2 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 was assigned.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 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**.

Locales

User Locales

You can assign a user to one or more locales. Each locale defines one or more organizations (domains) to which a user can access. Access is usually limited to the organizations specified in the locale. An exception is a locale without any organizations. It provides unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Any user locales configured after the first 48 are accepted, but are inactive with faults raised.

Users with admin or aaa privileges 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, a user assigned to 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
- fault
- operations

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations below 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.

Assigning an Organization to a Locale

Procedure

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

Step 2 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**.

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 **Admin**.
Step 2 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 is 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 15.

Deleting an Organization from a Locale

Procedure

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

Step 2 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 **Admin**.

Step 2 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 a confirmation dialog box displays, click **Yes**.

Locally Authenticated User Accounts

Creating a User Account

At a minimum, Cisco recommends that you create the following users:

- Server administrator account
- Network administrator account
- Storage administrator

Note After you create the user account, if you make any changes to any of the user account fields from the Cisco UCS Manager GUI, make sure to enter the password again.

Before you begin

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

- Remote authentication services—Ensures that the users exist in the remote authentication server with the appropriate roles and privileges.
- Multitenancy with organizations—Creates 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—Obtains the SSH key.

Procedure

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

Step 2 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:

Name	Description

Login ID field	The account name that is used when logging into this account. This account must be unique and meet the following 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 login ID must be unique within Cisco UCS Manager.
	• 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.
	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.

Name	Description

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 eight characters and a maximum of 80 characters.
	• If the password strength check is turned on, the minimum password length is variable and can be set from a minimum of 6 to a maximum of 80 characters.
	Note The default is 8 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 three 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.

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

Name	Description
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** Cisco UCS Manager GUI displays this field when you check the **Account Expires** check box.

Step 5 In the **Roles** area, check one or more boxes to assign roles and privileges to the user account.

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

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, click 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**.

Enabling the Password Strength Check for Locally Authenticated Users

You must have admin or aaa privileges to enable the password strength check. If 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 **Admin**.

Step 2 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

Procedure

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

Step 2 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:

Note The HTML-5 Interface supports one user session per browser.

Name	Description
Maximum Sessions Per User	The maximum number of concurrent HTTP and HTTPS sessions allowed for each user. Enter an integer between 1 and 256.
Maximum Sessions	The maximum number of concurrent HTTP and HTTPS sessions allowed for all users within the system. Enter an integer between 1 and 256.
Maximum Event Interval (in seconds)	The maximum time interval between two events. Tracks various types of event change notifications, such as responses to any user requests from the UI. If the interval expires, the UI session is terminated. Enter and integer between 120-3600

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 **Admin**.

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 **Admin**.

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 have 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 **Admin**.

Step 2 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 have 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.

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.

Step 3 Click the user that you want to disable.

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

Step 5 In the **Account Status** field, click the **inactive** radio button.

The admin user account is always set to active. It cannot be modified.

Step 6 Click **Save Changes**.

Clearing the Password History for a Locally Authenticated User

Procedure

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

Step 2 Expand **All** > **User Management** > **User Services** > **Locally Authenticated Users**.

Step 3 Click the user for whom you want to clear the password history.

Step 4 In the **Actions** area, click **Clear Password History**.

Step 5 If a confirmation dialog box displays, click **Yes**.

Deleting a Locally Authenticated User Account

Procedure

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

Step 2 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

Procedure

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

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:

Name	Description
Name column	The name for the session.
User column	The username that is involved in the session.
Fabric ID column	The fabric interconnect that the user logged in to for the session.
Login Time column	The date and time the session started.
Refresh Period column	When a web client connects to Cisco UCS Manager, the client must 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 inactive, but it does not terminate the session.
Session Timeout column	The maximum amount of time that can elapse after the last refresh request before Cisco UCS Manager considers a web session as inactive. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session.
Terminal Type column	The kind of terminal the user is logged in through.
Host column	The IP address from which the user is logged in.
Current Session column	If this column displays **Y**, the associated user session is currently active.