Managing Users, User Roles and Groups

This chapter contains the following topics:

Overview

Cisco IMC Supervisor supports the following system-defined user roles by default:

- **System Admin** — A user with all privileges including adding users. As an administrator in Cisco IMC Supervisor, you can assign users to system-provided user roles or to custom-defined user roles. In addition, at a later point, you can view information on any assigned role. You can make the following assignments:
  - Create a custom user role in the system, and create new user accounts with this role or assign the role to existing users.

    When you create a new user role, you can specify if the role is that of an administrator or an operator. For more information about creating user accounts, see Creating a User Account, on page 2. For more information about creating user roles, see Adding a User Role, on page 5.
  - Modify existing user roles, including default roles, to change menu settings and read/write permissions for users associated with that role.

    The procedure to modify menu settings and permissions for a role is the same as the procedure followed to create a user role.
- **Group Admin** — A user with all privileges. A system-defined user group **Default Group** is available by default in Cisco IMC Supervisor. As a group administrator, you can create and assign user accounts to this group or you can assign them to the groups you have created. A user can be part of multiple user groups. However, the group that the user was most recently added to is set as the default primary group for the user.

- **Operator** — Because the system administrator's role type is admin, you can modify the existing Operator role as required with any combination of access restrictions (menu settings and user permissions). By default, following menu settings and user permissions are assigned to an Operator.

Menu Settings	User Permissions
Systems : • Inventory and fault status • Physical Accounts • Firmware Management • Server Diagnostics	• Read - Physical Computing • Write - Physical Computing • Read - System Admin • Read - Users • Read - Read Tag Library • Write - Write Tag Library • Read - Orchestration • Write - Orchestration
Policies: • Manage Schedules • API and Orchestration	
Administration: • Users and Groups • Integration	

Note Reports such as **SCP User Configuration**, **Authentication Preferences** and **Password Policy** are enabled for Operator role under **Users and Groups**.

Creating a User Account

Note You cannot edit the **User Role** and **Login Name** fields in the **Edit User** dialog box.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Users**.

Step 3 Click **Add**.

Step 4 On the **Add User** page, complete the following:

Field	Description
User Role drop-down list	Choose **Group Admin**, **Operator**, or **System Admin**.

Field	Description
User Group drop-down list	Select the group that the user will have access to. You can either select a group already available, or you can add a new group. **Note** This field is visible only when you select **Group Admin** as the user role.
Login Name field	The login name for the user.
Password field	The password for the user. If the Lightweight Directory Access Protocol (LDAP) authentication is configured to the user, the password is validated only at the LDAP server, and not at the local server.
Confirm Password field	Repeat the password from the previous field.
User Contact Email field	The email address.
First Name field	(Optional) The first name of the user.
Last Name field	(Optional) The last name of the user.
Phone field	(Optional) The phone number of the user.
Address field	(Optional) The physical address of the user.

Step 5 Click **Add**.

Step 6 Click **OK**.

Viewing Online Users

Perform this procedure when you want to view users who are currently online.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Current Online Users**.
You can see the details such as username, IP address, session start time and so on of users who are currently logged on to Cisco IMC Supervisor.

Reviewing Recent Login History of Users

As an administrator in the system, you can review the recent login history for all users. The system records the following details for every login attempt:

- Login Name
- Remote Address
- Client Detail
- Client Type
- Authentication Status
- Comments
- Accessed On

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **All Users Login History**.

Step 3 Review the information displayed on the screen.

Configuring Session Limits for Users

You can configure the number of user interface sessions and REST API requests that users can initiate on the system.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 On the **Users and Groups** page, click **Session Management**.

Step 3 In the **Session Management** screen, complete the required fields, including the following:

Name	Description
Maximum Concurrent Sessions Per User field	The maximum number of concurrent GUI sessions that are supported for each user. Enter a number between 1 and 128. The default value is 16.
Maximum Concurrent REST API Requests Per User field	The maximum number of concurrent REST API requests that are supported for each user. Enter a number between 1 and 256. The default value is 128.

Step 4 Click **Submit**.

What to do next

When users initiate a GUI session or a REST API request to exceed the limit specified on this screen, an error message is displayed in the **System Messages** screen. In this scenario, either users should clear their sessions and API requests, or as an administrator, you can use the Shell utility and clear the sessions and requests for a user. For more information, see the *Cisco IMC Supervisor Shell Guide*.

Adding a User Role

On a newly installed Cisco IMC Supervisor appliance, by default, a **GroupAdmin** role and an **Operator** role are available. Because the group admin's role type is admin, you can modify the existing **Operator** role as required with any combination of access restrictions (menu settings and user permissions). Similarly, you can create new roles, as in the following procedure, and assign users to them.

Procedure

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

Step 2 Click **User Roles**.

Step 3 Click **Add**.

Step 4 On the **Add User Role** page, complete the following for the **User Role** pane:

Field	Description
User Role field	A descriptive name for the user role.
Role Type drop-down list	Choose **Admin**.
Description field	(Optional) A description of the user role.

Step 5 Click **Next**.

Step 6 In the **Menu Settings** pane, select the required menu options.

To choose the menu option, check the checkbox for the menu setting field.

Step 7 Click **Next**.

Step 8 In the **User Permissions** pane, select the required operations.

To choose the operation, check the checkbox for the operation.

Step 9 Click **Submit**.

Note You can also, edit, clone, or delete user roles.

Adding a User Group

Perform this procedure when you want to add a new user group.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **User Groups**.

Step 3 Click **Add**.

Step 4 On the **Add User Group** page, complete the following:

Field	Description
Name field	A name of the user group.
Description field	(Optional) A description of the user group.
Code field	(Optional) A shorter name or code name for the group.
Cost Center field	(Optional) The cost center name or number if required. This name or number represents a cost center that a group is associated with.
Contact Email field	The email used to notify the group owner about the status of service requests and request approvals if necessary.
First Name field	(Optional) The contact's first name.
Last Name field	(Optional) The contact's last name.
Phone field	(Optional) The contact's phone number.
Address field	(Optional) The contact's address.
Group Share Policy drop-down list	(Optional) Choose the group share policy for the users in this group. This drop-down list is populated only when you have created group share policies.
Allow Resource Assignment To Users checkbox	(Optional) If checked, the users of this group can have resources assigned to them and can own these resources. Also, these users can view resources belonging to the group. However, the resources among these users cannot be shared.

Step 5 Click **Add**.

Step 6 Click **OK**.

Note You can select these user groups and manage them by viewing, editing, deleting, enabling, and disabling them. You can also manage tags from the **User Groups** tab.

Branding a User Group

Perform the following procedure when you want to customize the Cisco IMC Supervisor application for a group of users. When users who belong to a selected group login to the system, they will see the customized page.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **User Groups**.

Step 3 Select a user group.

Step 4 Click **Branding**.

Step 5 On the **Group Branding** page, complete the following:

Field	Description
Logo Image checkbox	If checked, the logo appears on the top left corner of the application .
Application Labels checkbox	If checked, the application labels appear on top header section of the application.
URL Forwarding on Logout checkbox	If checked, user will be forwarded to the provided URL on logout.
Custom Links checkbox	If checked, custom links will appear on the top right corner of the application.

Step 6 Click **Submit**.

Group Share Policy

A group share policy provides more control to the users on the resources and what they can share with other users. With this policy, users can view resources that are currently assigned only to them or can view resources that are assigned to all groups that the users are part of.

While you are creating a group, you can define a group share policy and determine which groups have read/write permissions. Later on, when users are added to this group, their access to resources is defined by the group share policy that is applied to the group.

Adding Group Share Policy

Perform this procedure when you want to add a policy and share it with a user group.

Procedure

Step 1 Choose **Administration** > **Users and Groups**.

Step 2 Click **Group Share Policy**.

Step 3 Click **Add**.

Step 4 On the **Add Group Share Policy** page, complete the following fields:

Field	Description
Policy Name field	The name of the group share policy.
Policy Description field	The description of the policy.
Select Groups drop-down list	Choose the groups to share the policy you have created.

Step 5 Click **Submit**.

Step 6 Click **OK** in the **Submit Result** dialog box.

Note You can also select an existing policy to view, edit, delete, and clone them.