User Management

User Management

The user management module allows you to manage the users of Prime Service Catalog, including defining users, teams, and configuring role-based access control (RBAC). Prime Service Catalog provides role-based access to various functions. Through RBAC, Prime Service Catalog allows a user to access some resources but not others, and to perform specific tasks based on the logged-in user's roles. Authorization of tasks is controlled by roles within Prime Service Catalog and scopes within the applications.

This module is a subset of Organization Designer module and uses the existing features such as creating roles and assigning permissions. This module allows the Site Administrator to manage roles, teams, and users. The User Management module include three main tabs: Roles, Teams, Users.

- **Roles**: Role management is applicable the entire system. Roles created from this tab allows you to assign a set of capabilities and permissions to the role in one go.
- **Teams**: Team Management module introduced in 12.0 release is now merged with the User Management module under the Teams tab. For detailed information see section Setting Up Team Management.
- **Users**: The User Management module provides options to perform CRUD operations on users for the project teams.

Note Teams and Users tab are available only if Team Management is activated by the site administrator.

This chapter contains the following sections:

Managing Roles

Each role contains a group of resources such as users and services, with privileges and capabilities assigned to them. Users with the roles assigned to them can view and perform the permitted actions on the assigned services in Service Designer module. A user can be assigned more than one role. To disable the access provided to the roles, remove the role from the selected person or remove the capabilities that were assigned. For further understanding the roles and capabilities in Prime Service Catalog refer to the section Roles.

You can download the detailed list of all the out-of-box RBAC roles and capabilities Cisco Prime Service Catalog 12.1 RBAC Roles Capabilities and Permissions.

Prime Service Catalog includes a set of default roles for security and access control that allow different system functions. To create and manage roles navigate to **User Management module** > **Roles**.

Searching Roles

You can search for a role by typing all or part of its name in the Search box on the Roles tab. You can use the Show option to view the Platform or Service roles with the search criteria. All the roles that match the search criteria are displayed below.

Click the gear icon to select one of the actions from the list. The Edit Role option displays the general details of the role such as the name, description, parent role, and status.

Prime Service Catalog includes a set of default roles for security and access control that allow different system functions. To create and manage roles navigate to **User Management module** > **Roles**.

What are Platform and Service Roles?

The Show drop-down list on the Role Management Console allows you to filter the roles based on whether the roles are Platform or Service Roles:

- Platform roles are those which are created across the site for the deeper technical configuration, design, and troubleshooting tasks. These roles are created by super users like site admin or users who have permissions on Organization Designer.
- Service roles are those which are limited to the respective connections with third party applications or service groups. These are created by SOA who would provide read, write permission on the services to other users. All the users who are directly assigned the service role automatically become the member of the respective Service Design Team, if Team Management is activated.

Note The SOA can view and manage only those service roles that are associated to the integrations owned by the logged in user.

System Roles

Every SOA has the permission to access service roles tab of Role Management module. Once a connection is created in integrations a corresponding service role for SOA is created and displayed as system defined role. These system defined roles cannot be edited or deleted. See section **System-Defined Roles** of Admin guide for other system defined roles.

Note The system defined SOA roles must not be tampered with from Organization Designer module.

Managing Service Roles

A service role provides capabilities on Service Designer and Integrations modules once the role is assigned for a connection or service group.

Creating a Custom Service Role

Create a custom role when there is no system-defined role with the privilege settings that you require. If the privileges in the new role that you want to create are similar to that of an existing role, follow the procedure Cloning a Role, to copy the existing privileges into a new role that you can edit later.

Following is the high-level flow for creating a custom service role:

- Add a Name and description for the custom role.
- Add solutions and Services.
- Assign permissions on the Service.
- Associate user, group, OU, and teams.

To create service roles:

Step 1 Login as SOA and go to **Create a new role > Create a Service Role**.

Step 2 On the Create a New Service Role wizard, enter a name for the new user role. Optionally, add a Description. Click **Next Step**.

Step 3 Selected Services displays all the services assigned to this role. You may modify the permission using the toggle button or remove services on this screen.

Step 4 To add new services, click **Select a Solution**.
All the integrations and custom integrations owned by the logged in user are displayed.

Step 5 Choose the solution and select the services you wish to assign to the role.

Step 6 Click **Next Step.**

Step 7 From the **Select Permissions** pop-up select the appropriate permission for the services and **Add.**

Step 8 You may add more services to this list by repeating the steps 2 -5.

Step 9 Click **Nest Step**.

Step 10 From the Add Members screen, select the required users, group, Organizations, and teams to add to the role. The selected entries will remain even if you navigate from one tab to other.

Note The user must have read/write permission on all the users, group, organizations, and teams. Only then the user can assign the role on them.

Note Only the users who are directly assigned the service role automatically become the member of the respective Service Design Team. This means that the users who inherit the service role assigned to teams, group, or organizational unit are not added as members to the Service Design Teams. However, these users can access to the system and have permissions to perform actions as defined in the Service Role.

Step 11 Click **Create** to create the Custom role.

Step 12 Click **Done** to exit the wizard.

Editing a Service Role

The Edit Role option allows you to view and edit the general details of the role, and assign members and services to the role.

Assigning Members

Members of a role consist of individual users, teams, groups, and organizational units that have been assigned the role. If teams, groups, or organizational units are assigned, all members of the group, team, or org unit inherit the role. In addition, sub teams, suborganizational units and subgroups inherit roles from their parent. The **Show Inheriting Members** option allows you to choose whether to show those members who have inherited his role. If not checked, only teams, organizational units, and groups directly assigned to the role appear. Before you can assign users, teams, group, or organizational unit to the role, you must first make sure the entity exists. There are two ways to create a role/member association:

- Go to the individual user, team, group, or organizational unit, and assign the role.
- Go to the role and add members.

Note The user must have read/write permission on all the users, group, organizations, and teams i.e., write permission on Person "All Objects". Only then the user can assign the role on them.

Important Only those users who are directly assigned the service role automatically become the member of the respective Service Design Team. This means that the users who inherit the service role assigned to teams, group, or organizational unit do not become members of the Service Design Teams. However, these users can access to the system and have permissions to perform actions as defined in the Service Role.

The Members panel of the Role Details page displays all the members who have been assigned this role. Click **Add Members** option to assign this role to new teams, organizations or groups. To delete existing members, select the members from the list and click **Remove**.

Assigning Services

The Services panel is used to manage the permissions of this role on the assigned services. You can add new services to the role, update the permissions of the service, and remove the chosen service from the role. For the assigned services the role can have permission to view, edit, or restrict access to the service.

To add new services to the role:

Step 1 From the Services panel click **Add Services**.

Step 2 On the Selected Services pop-up click **Select a Solution**.

All the integrations and custom integrations owned by the logged in user are displayed.

Step 3 Choose the solution and select the services you wish to assign to the role.

Step 4 Click **Next.**

Step 5 From the **Select Permissions** pop-up select the appropriate permission for the services and **Add**.

Step 6 You may add more services to this list by repeating the steps 2 - step 5.

Step 7 Click **Submit**.

To unassign services from the role, choose the service from the Services panel and click remove.

Cloning a Role

Clone a Role option copies a role as is, including the members and assigned services. Once the clone is created you can make changes to this role using the Edit Role. This option works well when you can use a role as a base and want to make minor modifications on the existing role.

To create a clone of an existing role, select the role which you want to clone and choose **Clone Role** from the settings. You may add a different description and select different parent.

If a system defined role is cloned, the new role becomes a user defined role. This role can be deactivated or deleted if required.

Deactivating/Activating and Deleting Role

Roles must be active to have access privileges, that is, inactive roles do not have privileges. Deactivating a role removes that role and all associated permissions from any user to whom the role is assigned. At any time you can choose to deactivate or activate a role. Before deleting a role you must first deactivate the role.

Note System defined roles cannot be deactivated or deleted.

Managing Platform Roles

Only the Site Administrator or any user who has Organization Designer role can access, create or modify platform roles. The out of box platform roles cannot be edited or deleted.

Creating a Custom Platform Role

Only those users who have the **Access role configuration** and **Access User Management** capability and permission on all the Roles can create and manage Platform roles. Any user who has capability to access the platform role, can view all the roles even the ones that are not created by the logged in user.

Following is the high-level flow for creating a custom Platform role:

- Add a Name and description for the custom role.
- Add capability.
- Assign permissions on Object type.

- Associate user, group, OU, and teams.

To create platform roles:

Step 1 Login as Site Administrator and go to **Create a new role > Create a Platform Role**.

Step 2 On the Create a New Platform Role wizard, enter a name for the new role. Optionally, add a Description or a Parent Role. Click **Next Step**.

Step 3 (Optional) To add capability to the role:

a) Choose the module from the left hand side. Automatically all available capabilities within the chosen module are displayed in the Add Capabilities area. For detailed list of capabilities within the system see section Assigning Role Capabilities.

b) From the Add Capabilities area select the specific capability for the role. All selected capabilities are displayed in the Selected Capabilities area.
Similarly, you can navigate to any other module and select capabilities. The Selected Capabilities area remembers your selection from all the modules. You can delete the capabilities by clicking on the cross mark next to the capability.

c) Once done, Click **Next Step**.

Step 4 (Optional) Configure permissions for the role:

a) Choose the Object Type from the left hand side and click **Add**.

b) Choose the permission type from the **Permissions for this type** drop-down list. The permissions displayed depend on the object selected.

c) Choose the appropriate option from **Assign permission to** list.

d) If you chose Selected Objects, from the list below select the objects on which the role must have permissions from the list below and Click **Add.**
Similarly, you can navigate to any Object Type and configure permissions. The right pane remembers your selection from all the Object types. You can delete the capabilities by clicking on the cross mark next to the permission.

e) Once done, Click **Next Step**.

Step 5 From the Add Members screen, select the required users, group, Organizations, and teams to add to the role. The selected entries will remain even if you navigate from one tab to other.
At any point of time you can navigate to the capability, permissions, or members tabs to modify the selections.

Step 6 Click **Create** to create the Custom role.

Step 7 Click **Done** to exit the wizard.

Editing a Platform Role

Associating Roles

You can assign any system roles to the platform role using the Associated Roles panel. These roles behave as sub roles for the platform role. This panel displays all the assigned roles to the platform role.

To add new roles:

Step 1 On the Associated Roles panel, click **Add Roles**.

Step 2 Search for the role name you want to assign to the platform role.

Step 3 Choose the roles to be assigned from the options displayed below and click **Add Roles**
To delete a role, select the roles to be deleted from the panel and click **Remove.**

Managing Capabilities

A capability is the ability to perform certain functions within Prime Service Catalog. You can manage capabilities of the Platform role from the Capabilities panel. For detailed list of capabilities within the system see section Assigning Role Capabilities.

If a role has been assigned a parent role, the sub role inherits the capabilities from the parent role. The **Show inherited capabilities** option allows you to choose whether to show these inherited capabilities from a parent role. If not checked, only the capabilities directly assigned to the role appear.

To add new capabilities:

Step 1 On the Capabilities panel, click **Add Capabilities.**

Step 2 Choose the module from the drop-down list and select the capabilities. Click **Add capabilities**.
To add capabilities from another module repeat the procedure.

To remove capabilities, select the capabilities from the panel and click **Remove**. The inherited capabilities cannot be removed.

Managing Permissions

Permissions grant rights to a role to act upon an object. Permissions determine if a role with granted capabilities allows the user to operate on all entities (objects) of a particular type, or restricted to a set of named entities. The Permission panel allows you to manage the permissions for the role.

If a role has a parent role assigned, this role inherits the permissions granted to the parent role. These in permissions can be viewed by clicking on the **Show Inherited Permissions** option. By default only the directly assigned permissions are displayed in the panel below.

To add additional permissions for the role:

Step 1 On the Permissions panel, click **Add Permissions**.

Step 2 Choose the Object Type from the left hand side.

Step 3 Choose the permission type from the **Permissions for this type** drop-down list. The permissions displayed depend on the object selected.

The options displayed for field **Permissions for this type** and **Assign permission to** depend on the Object Type chosen.

Step 4 Choose the appropriate option from **Assign permission to** list.

Step 5 If you chose Selected Objects, from the list below select the objects on which the role must have permissions from the list below and Click **Add.**
Similarly, you can navigate to any Object Type and configure permissions. The Selected Permissions pane displays your selection from all the Object types. You can delete the capabilities by clicking on the cross mark next to the permission.

Step 6 Click **Add Permissions**.

Managing Members

Adding members to a Platform role is same as adding members to service roles. For detailed information see section Assigning Members to a Role.

Cloning a Platform Role

Cloning a Platform role is similar to the cloning a Service role. Refer to section XXX.

Deactivating/Activating and Deleting Role

Deactivating/Activating and Deleting Platform Role concepts are similar to Service roles. See section.

Managing Users

The User management console is a new interface which provides enhanced user experience to manage the users in system. From this console you can perform CRUD operations on the user and also assign roles to individual users. The Users tab of User Management module is accessible only to the Site Administrator. For detailed information see section Adding a Person.

Creating a New User

Service Catalog provides four mechanisms for adding people:

- User Management allows administrators to create a person interactively, using the pages described in this section.
- Organization Designer allows administrators to create a person. For detailed information refer to section People.
- The Import Person event in Directory Integration can create a person and his/her home OU. For more information, see the Cisco Prime Service Catalog Integration Guide.
- The Directory Task available in the service workflow (delivery plan) can create a person based on service form data. For more information, see the Cisco Prime Service Catalog Designer Guide.

When creating a new user, you must assign a default, or Home, organizational unit to the person. Therefore make sure you create the organizational unit before you create the new person.

To add a new person:

Step 1 Go to User Management > Users.

Step 2 Click **Create New User**.
Enter all the necessary information about the user, the fields with an asterisk (*)): are mandatory. For reference see table 53 Table 1

Edit User Details

You can add additional information for the user using the Edit user details option. For reference see table Table 53 Table 1 and Table 54 Table 1.

To edit user details:

Step 1 From the settings icon of the user, select the option **View User Details**.

Step 2 Click **Edit** on the User Details panel and edit the user info.

Step 3 Click **Update** to save changes.

Assigning User to a Team

In case Tenant Management is turned on, users need to belong to at least one team to be able to order services. From this panel the administrator can assign users to teams.

To assign user to a project team:

Step 1 From the settings icon of the user, select the option **View User Teams**.

Step 2 Click **Join Team** on the Team Membership panel assign the user to a team.

Step 3 To unassign the user from the team, click on the delete icon beside the team name.

Assigning Role to a User

This option allows you to configure roles for a user. A role is a combination of access to a module with one or more capabilities, and in some cases, one or more object-level permissions. The Roles panel displays all the roles assigned to the user. All users inherit roles that are assigned to teams, groups, or organizational units. The **Show inheriting Roles** option allows you to choose whether to show those roles which have been inherited. If not checked, only roles directly assigned to the users appear.

Important Only those users who are directly assigned the service role automatically become the member of the respective Service Design Team. This means that the users who inherit the service role assigned to teams, group, or organizational unit do not become members of the Service Design Teams. However, these users can access to the system and have permissions to perform actions as defined in the Service Role.

To add new roles, click **Assign Role** option to assign this role to users. Search for the desired role and click **Use selected.** To unassign existing roles, select the roles from the list and click the delete icon. Only the directly assigned roles can be deleted.

Deactivating a User

Once a person has performed any activities within Prime Service Catalog, the person entry cannot be deleted. The person can be made Inactive to prevent them from logging on or performing further activities. For more details see section **Deactivating a Person.** To deactivate a user, select **Deactivate User** from the settings icon of the user.

Adding Additional User Information

You can add additional information of the user from the respective panels of the Manage User page. For further information on other tasks see the following sections:

- Address Information
- Contact Information
- Adding Additional Information using Extensions
- Configuring a Person's Calendar