Getting Started

Revised: May 20, 2022

Back

Logging In and Out of the Cisco MSX Portal

To log in to the Cisco MSX user interface, enter the following URL in your web browser address field, where server-ip is the IP address or fully qualified domain name (FQDN) name of the Cisco MSX server:

https://<server-ip>Cisco MSX or https://www.example.com/

Depending on your network configuration, the first time your browser connects to the Cisco MSX web server, you may have to update your client browser to trust the security certificate of the server. This ensures the security of the connection between your client and the Cisco MSX web server.

What you can see and do in the user interface is determined by your user account privileges. For information on Cisco MSX users and the actions, they can perform, see the topic on 'Managing Users'.

To log out, select the user and click **Logout**.

Role-Based Access in Cisco MSX

In Cisco MSX, user permissions are managed using Role-Based Access Control (RBAC). RBAC restricts or authorizes the system access for users based on that user's roles. Based on the permissions that are assigned to a user by an administrator, a user can define and customize how their services are exposed to customers.

The permissions allow customizing the various aspects of a service workflow, such as managing tenants, notifications, integration with BSS systems, announcements, and so on. The role-based access permissions are categorized into:

- **Service Pack Specific Permissions**: Include permissions for controlling various settings for the service packs.
- **Services, Configurations, and Devices Specific Permissions**: Include permissions for configuring various settings for the devices and services.
- **Integrations, Settings, and Log Specific Permissions**: Include permissions for controlling integration, log, and SSO configurations.
- **Users, Roles, and Tenants-Specific Permissions**: Include permissions to configure user, remote users, tenants, roles, provider settings, and so on.

For more information on Cisco MSX out-of-the-box roles, see 'User and Role-Based Access in Cisco MSX' in *Cisco MSX Administration*. For a complete list of all the permissions available in Cisco MSX, see *Cisco MSX Platform and Service Packs Permissions Addendum*.

Managing the Managed Device-Specific User Roles

In Cisco MSX, you must create a new role (such as Managed Device Operator) and assign the permissions required to operate the platform tasks.

To create a new role and assign it to users:

Table 1: Procedure for Creating Managed Device Specific User Roles

	Task	Reference Topics
1.	Log in to the Cisco MSX Portal (as an Admin/Super user).	—
2.	Create the tenants.	For more information on creating a new tenant, see Managing Tenants.
3.	The SP_OPERATOR role available in Cisco MSX has the permissions necessary to create and manage Managed Device services. You may also create a role specifically for Managed Device and assign the permissions required to operate Managed Device.	For more information on creating a new user role, see Managing Users.
4.	Create a user (such as Tenant Operator user), assign the role that is defined in Step 3 to this user, and select all the tenants that the user must access.	For more information on creating a new user, see Managing Users.

Managing User Roles

A user is granted access to desired system resources only if the assigned role grants access privileges. For example, the user with the admin role can define a new role, create tenants, create users, and so on. For more information on assigning roles to a user, see Managing Users.

Adding User Role

To add a user role:

Procedure

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click **Roles**.

The **Manage Roles** window appears.

Step 3 Click **Add Role**.

Step 4 Enter the Role Name, Display Name, and Description.

Step 5 To assign permission for the roles, click **Category** and select the corresponding check box for the permission(s) that you must grant to the role.

The types of permission you can grant are:

Table 2: Types of Permission

Permission	Description
View	Provides read-only access to the function.
Manage	Provides access to read and manage tasks associated with the functions.

The table below lists the Managed Device category of permissions.

Table 3: Category of Permissions

Display Name	Description
Templates	Allow users to manage permission to add or modify the templates required for the Managed Device Sites. The templates can be added or modified only by using the Managed Service API. For more information on the Manage Device API, refer to the Swagger documentation accessible from the Cisco MSX Portal > User Profile icon > Account Settings > Swagger > SFI SDK > Manage Device API.
Managed Device Sites	Allow users to manage permission to add or modify sites to apply the template, remove the template or deprovision device. The templates can be added or modified only by using the Managed Service API. For more information on the Manage Device API, refer to the Swagger documentation accessible from the Cisco MSX Portal > User Profile icon > Account Settings > Swagger > SFI SDK > Manage Device API.
Templates Parameters	Allow users to manage permission to configure parameters of the uploaded templates. The templates can be added or modified only by using the Managed Service API. For more information on the Manage Device API, refer to the Swagger documentation accessible from the Cisco MSX Portal > User Profile icon > Account Settings > Swagger > SFI SDK > Manage Device API.
Metrics	Allow users to manage permission to add or modify the metrics data of the sites namely UP, DOWN, CPU, memory utilization, Uptime, Internet traffic, LAN traffic, and Status History. For more information on the Manage Device API, refer to the Swagger documentation accessible from the Cisco MSX Portal > User Profile icon > Account Settings > Swagger > SFI SDK > Manage Device API.
Running Configuration of Devices	Show running config of devices capability

For more information on permissions that are required for managing Meraki and other devices supported by Managed Device, see Cisco MSX Platform Addendum.

Step 6 Click **Save**.

Modifying User Role

To modify a user role:

Procedure

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click **Roles**.

The **Manage Roles** window appears.

Step 3 Select the role that you want to modify and click the **Edit** icon.

Step 4 To assign or revoke the permission for the roles, click **Category** and then select or unselect the corresponding check box for the permissions.

The table below describes the type of permissions that you can grant:

Table 4: Types of Permission

Permission	Description
View	Provides read-only access to the function.
Manage	Provides access to read and manage tasks associate with the functions.

Step 5 Click **Save**.

Managing Tenants Groups

After you create tenants, you can configure the tenant groups, which are a collection of tenants that are grouped for assigning a common list of functions such as, service extensions parameter values, and so on.

To manage tenant groups:

Procedure

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click **Tenant Groups** to view the list of tenant groups with their details in the Manage Tenant Groups window.

Step 3 Click **Add Tenant Group**.

Step 4 Enter the Name and Display Name of the new tenant group.

Step 5 (Optional) Enter the Description.

Step 6 (Optional) From the **Associate Tenants** drop-down list, choose the tenant to associate with the new tenant group.

Note A tenant can be associated with only one tenant group. The **Tenant** drop-down list displays only the tenants that are not associated with any tenant group.

Step 7 Click **Save**.

Managing Tenants

The multi-tenant architecture of Cisco MSX can segment the data stored by a tenant. When tenants are defined, data is partitioned by the tenant. Thus, provides data security and privacy for each tenant while allowing cloud or managed service providers the flexibility to consolidate many smaller customer configurations on a set of infrastructure servers.

The key points that you should know, while configuring tenants are:

- Tenant administrators are linked to their data by a tenant object.
- Tenant objects have to be consistent and unique across all clusters.
- A tenant administrator cannot view or modify the data of another tenant.

To manage tenants:

Procedure

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click **Tenants**.

The **Tenanats** window appears.

Displays the list of existing tenants with their details.

Step 3 To add a new tenant:

a) Click **Add Tenant**.
b) Enter the Name, Website URL, External ID, Parent Tenant, and Description.
c) Click **Save**.

The new tenant details appears in the Tenants window.

Step 4 To update the tenant details:

a) Select the Tenant from the list.
b) Click the **Edit** icon to edit the data in the desired field.
c) Click **Save**.

Step 5 To delete the teanant:

a) Select the Tenant from the list.
b) Click the **Delete** icon.

The **Delete Tenant** confirmation dialog box appears for you to confirm the tenant deletion.

c) Click **Delete**.

Managing Users

As an administrator, you can add new user details, assign an appropriate role to a user, and associate the new user to a tenant.

Note You can also disable the creation and modification of users, by choosing **Single Sign On** and using Identity Provider. The procedure below describes the use of local user accounts.

Before you begin

You should have administrator privilege for managing users.

Procedure

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click **Users**.

The **Users** window appears. Displays the list of users and their details.

Step 3 To add user:

a) Click **Add User**.
b) Enter details such as First Name, Last Name, User ID, and Email Address.
c) From the **Language** drop-down list, choose the desired language.
d) From the **Assign Role** drop-down list, choose the desired roles.
e) From the **Associate Tenants** drop-down list, choose one or more tenants to be associated with a user. .
f) From the **Password Policy** drop-down list, choose the desired password policy.
g) Click **Save**.

Step 4 To assign a role:

Note For more information on categories and permissions for the Managed Device service pack, see Managing Users.

a) Select the User to modify the role.
b) Click the **Edit** icon.
c) From the **Assign Role** drop-down list, choose the desired roles.
d) Click **Update**.

Back

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.