Managing Roles in Cisco MSX

In Cisco Managed Services Accelerator (MSX), user permissions are managed using Role-Based Access Control (RBAC). RBAC restricts or authorizes system access for users based on their user 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 users to customize various aspects of a service workflow, such as managing tenants, notifications, integration with BSS systems, announcements, and so on.

In MSX, you need to create a new role (such as an SD-WAN Operator) and assign the permissions required to order, operate, and view service pack-related services. MSX provides five out-of-box roles. For more information on MSX out-of-box roles, see the *Cisco Managed Services Accelerator (MSX) Platform User Guide*.

To create the SD-WAN role and assign it to users:

Table 1: Procedure for Creating SD-WAN Service Pack-Specific User Roles

	Procedure	References
1	Log in to the Cisco MSX portal (Admin/Super user)	
2	Create the tenants.	For more information on creating a new tenant, see Managing Tenants .
3	Create a new role if you want to perform specific tasks on SD-WAN. **Note** By default, MSX provides five out-of-the-box (OOB) roles that have permissions applied. In these OOB roles, Service Operator role has permissions required to create and manage SD-WAN service. To see the default permissions applied on a service provider operator role: In the main menu of the MSX Portal, click Roles and select Service Provider Operator. Expand the various categories to see the default permissions applied on this role.	For more information on basic permissions that are required to perform the documented tasks for the MSX platform and the service packs, see Cisco Managed Services Accelerator (MSX) Platform and Service Pack Permissions Addendum. For more information on creating a new user role, see Managing User Roles .

	Procedure	References
4	Create users (such as SD-WAN User), and assign the role that is defined in Step 3 to the user, and select all the tenants that the user needs to access.	For more information on creating a new user, see Managing Users

Managing User Roles

Your user account privileges determine, what you can see and do in the MSX user interface. In MSX, the permissions are managed using Role-Based Access Control (RBAC). RBAC restricts or authorizes system access for users based on their user roles. A role defines the privileges of a user in the system. Since users are not directly assigned with privileges, management of individual user privileges is simply a matter of assigning the appropriate roles.

A user is granted access to desired system resources only if the assigned role grants the access privileges. For example, a user with the Service Extension permissions can import service extension templates, define service extension parameters, define default parameter values, and so on. For more information on assigning roles to a user with appropriate permissions, see Managing Users .

SD-WAN-Specific Permissions

The table below lists the Cisco SD-WAN and SD-Branch category of permissions:

Table 2: Cisco SD-WAN and SD-Branch Category of Permissions

SD-WAN Service	SD-WAN Data Plane	Allows users with manage permissions to add, edit, or delete sites (data plane). View permission allows you to view sites (Data Plane) and the status of the sites.
	SD-WAN Maintenance	Allows users with manage permission to debug and access SD-WAN GET APIs. Using these APIs, users can query SD-WAN databases, or query Cisco SD-WAN to check on status of various components.
	SD-WAN Control Plane	Allows users with manage permissions to create, attach, delete, detach Control Plane. View permission allows users to view a control plane that is already created or attached and see the status of the Control Plane components.
	SD-WAN Orchestrator Settings	Allows users with manage permission to configure orchestrator settings to spin up a new Control Plane. For more information, see #unique_23
	SD-WAN Traffic Policy	Allows users with manage permission to add and modify Application Relevance policy or Path Preference policy to the Cisco SD-WAN fabric. For more information on how to configure these traffic policies for Cisco SD-WAN, see Configuring SD-WAN Traffic Policies. This permission along with **Service Configuration Application** manage permission is also required to configure application relevance for various applications across MSX managed sites that have MX device models (Meraki SD-WAN appliance).
	SD-WAN Bulk Site	

		Allows users to download the template to their local machine and to view or manage the template.
Cisco MSX SD-Branch Operations	Template Data Operations	Allows users with manage permissions to manage predefined data for Cisco MSX SD-Branch service templates.
	Template Operations	Allows users with manage permissions to add, edit, or delete Cisco MSX SD-Branch service templates and edit tenant access to SD-Branch service templates
	SD-Branch Settings Operations	Allows users with manage permissions to manage Cisco MSX SD-Branch settings.
	SD-Branch Sites Operations	Allows users with manage permissions to add, edit, or delete Cisco MSX SD-Branch sites.

Along with the preceding permissions, SD-WAN services also need permissions from the MSX platform side. For more information on minimum permissions (platform) that are required to perform a task in SD-WAN and on the complete list of MSX permissions, see Cisco Managed Services Accelerator (MSX) Platform and Service Pack Permissions Addendum.

Adding a User Role

To add a user role:

Step 1   Log in to the Cisco MSX Portal.

Step 2   In the main menu, click **Roles**. The Manage Roles screen appears.

Step 3   Click the **Add Role** button.

Step 4   Enter the role name, display name, and description.

Step 5   To assign the permission for the roles, click **Category** and select the corresponding check boxes for the permissions that you want to grant to the role. For permissions related to SD-WAN, see SD-WAN-Specific Permissions.

The types of permission you can grant are::

Table 3: Assigning User Roles

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

Step 6   Click **Save**.

Modifying an Existing Role

To modify an existing role:

Step 1   Log in to the Cisco MSX Portal.

Step 2   In the main menu, click **Roles** to view the list of roles.The Manage Roles screen 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 select or clear the corresponding check box for the permissions.The types of permission you can grant are:

Table 4: Permission Types

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

Step 5   Click **Save**.

Managing Tenants, Tenant Groups, and Users

The multitenant architecture of MSX provides the ability to segment the data stored by a tenant. When tenants are defined, data is partitioned by a tenant, thus providing data security and privacy for each tenant. This multitenant approach allows cloud or managed service providers to consolidate many smaller customer configurations on a set of infrastructure servers.

Consider the following points while configuring tenants:

- Tenant administrators are linked to their data by a tenant object.

- Tenant objects should be consistent and unique across all clusters.

- A tenant administrator cannot view or modify the data of another tenant.

Managing Tenants

To manage tenants:

Step 1   Log in to the Cisco MSX Portal.

Step 2   In the main menu, click **Tenants** to view the list of existing tenants (customers) with their details on the Manage Tenants page.

- To add a new tenant, click **Add Tenant** and enter the customer name and description, email address, website URL, and contact number.

- Click **Save**. The new customer details are listed on the Manage Tenants page.

- To update the tenant details, select the tenant on the list and click the **Edit** icon.

- To delete a tenant, select the tenant from the list and click the **Delete** icon.

Managing Tenant Groups

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

To manage tenant groups:

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 tenant group name and description.

Step 5   Select the tenants that you want to add to the tenant group.

Note   A tenant can be associated with only one tenant group. The Tenant drop-down lists only those tenants which are not associated with any tenant group.

Step 6   Click **Save**.

Managing Users

You can add new user details, assign appropriate role to the user, and associate the new user to the tenant.

To manage users:

Step 1   Log in to the Cisco MSX Portal.

Step 2   In the main menu, click **Users** to view the list of users with their details in the Manage Users window.

Step 3   Click **Add User** and enter the username and ID, email address, and contact number.

Step 4   To assign a role, you can choose from the available options.

Note   For more information on categories and permissions for the Cisco MSX SD-WAN service pack, see Cisco Managed Services Accelerator (MSX) Platform and Service Pack Permissions Addendum.

Step 5   Select a tenant from the **Associate Tenants** drop-down list.

Step 6   Click **Save**. The new user details are displayed in the Manage User window username.