Getting Started

Revised: May 18, 2022

↶ Back

Logging In to the Cisco MSX Portal

You can access the SD-WAN service pack on the Cisco MSX Portal, only after installing the Cisco MSX platform along with the required service pack.

To log into the Cisco MSX portal, enter the following URL in your web browser address field:

https://<*server-ip*> or https://<*your_portal_fqdn*>

In this URL:

< *server-ip*> is the IP address or fully qualified domain name (FQDN) name of the Cisco MSX server:

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 Managing Roles in Cisco MSX.

Log in to the Cisco MSX portal and ensure all Microservices and Service UI information in the **Settings** main menu > **Component Versions** displays the latest Cisco MSX version.

Configuring Single Sign-On Between Cisco MSX and Cisco SD-WAN

Use the procedure below to configure the SSO between Cisco MSX and Cisco SD-WAN. Only a user with an appropriate role (operator or supervisor role) can configure the SSO.

Procedure

Step 1 Upload the Cisco MSX metadata to the SD-WAN control plane.

- **a.** Download the Cisco MSX metadata from the following link: https://msx-fqdn/idm/metadata.
- **b.** Upload the metadata file to the SD-WAN control plane by choosing **Settings** > **Identity Provider Settings**. For information on logging in to the Control Plane, see Logging in to the Cisco SD-WAN Control Plane.
- **c.** Click **Edit** and then select **Enable Identity Provider** option.
- **d.** Copy the contents of the metadata file to the **Upload Identity Provider Metadata** field.
- **e.** Click **Save**.

Step 2 Download the Cisco SD-WAN SAML metadata file:

- **a.** From the Cisco SD-WAN control plane, choose **Administration> Settings >Identify Provider Settings** .

b. Navigate to **Click here to download the SAML metadata** and save the contents in a file, for example, vmanage_metadata.xml.

Step 3 Configure the SSO client (Cisco SD-WAN control plane) details in the Cisco MSX portal.

a. Log in to the Cisco MSX portal.

b. In the main menu, choose **Settings > SSO Configuration**.

c. Expand the **Add SSO Client** window and click **Add** . In the **Add SSO Client** window, specify the following details:

- **Associate Tenants**: Specify the tenant for whom the SSO client is configured. If no tenants are specified, Cisco MSX assumes that the SSO client configuration is for all the tenants, if no tenants are specified.

  Note Superuser, Tenant Administrator, and Service Provider operator can access the control plane without configuring SSO.

- **Grant Types**: From the drop-down, choose the option 'urn:ietf:params:oauth:grant-type:saml2-bearer'.
- **Metadata Source** : Copy the Cisco SD-WAN metadata downloaded from step (2) above into the Metadata Source field. The metadata source field takes url or a file path.

  Note The metadata field is displayed only if you have specified a SAML service provider client ID in the **Client ID** field.

- **Authorities** : From the drop-down, choose the **ROLE_USER** option.
- **Use Session Timeout**: Select the **No** option.
- **Access Token Validity Seconds**: Enter the time in seconds for when the token is valid. Enter this value as '1'.
- **Max Tokens Per User**: From the drop-down, choose the number of tokens allowed per user.
- **Refresh Token Validity Seconds** : Enter the time in seconds.
- **Client ID**: Specify the SAML service provider's client ID (Cisco SD-WAN control plane IP address in this case). The SAML service provider's client ID is the same as the "entityId" which can be found in the downloaded from the SAML metadata of the Cisco SD-WAN control plane.
- **Client Secret**: Enter the password to authenticate the client with the client ID.
- **Scopes**: From the drop-down, choose 'read'.
- **Auto Approve Scopes**: From the drop-down, choose 'read'.

d. Click **Save**.

A new SSO client configuration is added and displayed in the **SSO Clients** table.

A green success banner indicates that the above settings are correct. If a red banner is displayed, verify the Metadata Source is correct.

Step 4 Create user roles in the Cisco MSX portal. These roles should map to one of the SD-WAN control plane user roles (Basic, Netadmin, or Operator).

Step 5 (Optional) Disable the SAML security settings.

Perform this step if the SSO configuration is not successful and is not working as expected.

By default, the following SAML security parameters in Cisco MSX are set.

- `security.auth.saml.want-authn-request-signed`

- `security.auth.saml.encrypt-assertion`

For SAML service provider integration with Cisco MSX, if the above security parameters are set to True, the auth request from the service provider must be signed, and the assertion sent back by Cisco MSX is encrypted.

To turn off this default setting, update an existing SAML Service Provider's values by using the PUT /idm /api /v1 /samlsp /update API in the IDM microservice, as shown in the example below:

```
{
  "entityId": "Entity ID can be found in the Cisco SD-WAN metadata file that was downloaded from step
 (2)”,
  "metadataRequireSignature": false,
  "metadataSource": “Content of Cisco SD-WAN metadata downloaded from step (2),
  "metadataTrustCheck": false,
  "metadataTrustedKeys": [],
  "securityProfile": "MetaIOP",
  "skipAssertionEncryption": true,
  "skipAuthRequestSignatureVerification": true
}
```

Configuring Integrations

Using this procedure, you can enter the configuration details for the Business Support Set (BSS), Representational State Transfer (REST), and outbound API calls.

To configure BSS integrations, do the following:

Procedure

Step 1 Log in to the Cisco MSX portal.

Step 2 From the left hand pane, click **Settings**.

Step 3 Click the **BSS Integrations** tile. The **BSS Integration** page is displayed.

Step 4 Click the **Global** tab and configure the following fields:

- **Read only User View**: Check this option to allow your users to only view the details.

- **Show Profile**: Check this option to enable the show profile option for your tenants.

- **Read only Tenant View**: Check this option to allow your tenants to only view the details.

Step 5 Click the **REST Configuration** tab to set the authentication mode details for the integrations system.

a) Select the **Basic** or **OAuth2** radio button, based on your requirement.

   - If you select the **Basic** radio button, enter the **User ID** and **Password** of the integrations system.

   - If you select the **OAuth2** radio button, enter the details such as the **Token Request URL**, **Client ID**, **Client Secret**, **HTTP Method**, **Token Validation Header**, **Token Header Format**, and so on.

b) Click **Save** to save the authentication details.

Step 6 Click the **Outbound API** tab and specify the APIs used for business integrations. Click on the edit button to modify the **Allowed Values**, **Pricing Options**, **Accessible Services**, **Service Cancellation**, and **Notification URL** for the APIs.

Step 7 Click **Update** to save the changes.

Managing SD-WAN Notifications

Before You Begin

You can configure integrations for enabling support for BSS, REST, and outbound API calls. For more information, see Configuring Integrations.

Perform this procedure to enable notifications:

Procedure

Step 1 Log in to the Cisco MSX portal.

Step 2 From the left hand pane, choose **Settings** > **Service Configurations** > **SD-WAN** > **Notifications**.

The **Provider** and **End Users** tab displays the events that are related to service provider and end users. Using the **Category** drop-down list, you can further categorize events as End Users, Services, and Devices.

Step 3 To edit the notification settings, click the **Edit** icon adjacent to the Category column.

For an event, you can edit the template name, the communication mode, and enable or disable notifications for a specific event.

Step 4 Click **Save**.

The following table lists the Cisco MSX notifications and the corresponding recipients for events:

Table 1: Notifications and Recipients

Notifications	Recipients
SD-WAN control plane status changed	REST clients
SD-WAN control plane operation notifies user	End users
SD-WAN control plane operation notifies tenant	Tenants
SD-WAN control plane operation notifies provider	Provider
SD-WAN site deletion notifies user	End users
SD-WAN site deletion notifies tenant	Tenants
SD-WAN site deletion notifies provider	Provider
SD-WAN site creation notifies user	End users
SD-WAN site creation notifies tenant	Tenants

Notifications	Recipients
SD-WAN site creation notifies provider	Provider
SD-WAN site status changed	REST clients

The following are examples of control plane and data plane notifications:

- Control Plane Message
    - Dear customer, the requested changes on your SD-WAN service have been applied.
    - *<Control plane URL>*
    - *<Control plane Org>*
    - *<User ID>*
    - *<User name>*
    - Best regards, Cisco MSX powered by Cisco
- Data Plane Message
    - Dear customer, the requested changes on your service have been applied.
    - *<Site ID>*
    - *<Site Name>*
    - *<Chassis Number>*
    - *<User id>*
    - *<User name>*
    - *<Tenant id>*
    - *<Tenant name>*
    - *<Tenant email>*
    - Best regards, Cisco MSX powered by Cisco

Defining Terms and Conditions

Cisco MSX allows you to define and maintain the terms of a service for acceptance by a consumer while purchasing a service.

Procedure

Step 1 Log in to the Cisco MSX portal using your credentials.

Step 2 From the left hand pane, choose **Settings** > **Service Configurations** > **SD-WAN** > **Terms & Conditions.**

Step 3 Enter the details. This information will be displayed while a consumer is placing an order for a service. The terms and conditions are specifically defined specific to an offer in a service.

The **Offers** drop-down list displays the service pack offer selected in step 2.

Step 4 Click **Save**.

Configuring Password Policies

In Cisco MSX, as an administrator user, you can define various settings for the password policies, such as password strength, password minimum/maximum length, password history, and password aging.

By default, there are two default policies available on Cisco MSX. An Administrator user can modify these existing policies or create new policies. The default policies that are created at the deployment time are:

- ppolicy_default - Applicable for a consumer user
- ppolicy_strong - Applicable for administrator accounts

For more information on the password policies and to modify the default password policies, see Cisco Managed Services Accelerator (MSX) 4.3 Administration Documentation.

Managing Roles in Cisco MSX

In Cisco 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 Cisco 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. Cisco MSX provides five out-of-box roles. For more information on Cisco MSX out-of-box roles, see Cisco Managed Services Accelerator (MSX) 4.3 Administration Documentation.

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

Table 2: 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.

	Procedure	References
3	Create a new role if you want to perform specific tasks on SD-WAN. **Note** By default, Cisco 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 Cisco 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 Cisco MSX platform and the service packs, see Cisco Managed Services Accelerator (MSX) 4.3 Platform and Service Pack Permissions Addendum. For more information on creating a new user role, see Managing User Roles.
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 Cisco MSX user interface. In Cisco 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 3: 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 Configuring Cisco SD-WAN Orchestrator Settings.
	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 Traffic Policies. This permission along with **Service Configuration Application** manage permission is also required to configure application relevance for various applications across Cisco MSX managed sites.
	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 Cisco 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 Cisco MSX permissions, see Cisco Managed Services Accelerator (MSX) 4.3 Platform and Service Pack Permissions Addendum.

Adding a 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 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 4: 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:

Procedure

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 5: 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 Cisco 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:

Procedure

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:

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 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:

Procedure

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) 4.3 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.

Deployment Workflow for Cisco SD-WAN

Using the workflow in the table below, you can deploy Cisco SD-WAN vEdge Cloud, or vEdge SP Cloud, or the Physical site.

Table 6: Workflow for Cisco SD-WAN vEdge Cloud, or vEdge SP Cloud, or Physcial Sites

Task	See
1. Attach an existing control plane or create a new control plane.	Setting Up Control Plane for Cisco SD-WAN
2. Complete Control Plane post deployment tasks.	Postdeployment Tasks for SD-WAN Control Plane
3. Add a vEdge Cloud or vEdge SP Cloud or a Physical Site/Device.	• For vEdge Cloud, see Adding a vEdge Cloud Device. • For vEdge SP Cloud, see Adding a vEdge SP Cloud Device. • For Physical site, see Adding a Physical Device.
4. (Optional) If you have details of multiple sites available, you can import these details into Cisco MSX.	Importing Multiple Site Data from Cisco SD-WAN into MSX
5. Push the site details to the Control Plane such that the device is set up for day one configurations.	Provisioning a Device
6. Verify all the components of SD-WAN service are deployed.	Monitoring SD-WAN Control Plane Status
7. Configure Traffic Policies	Configuring Traffic Policies

↶ 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.