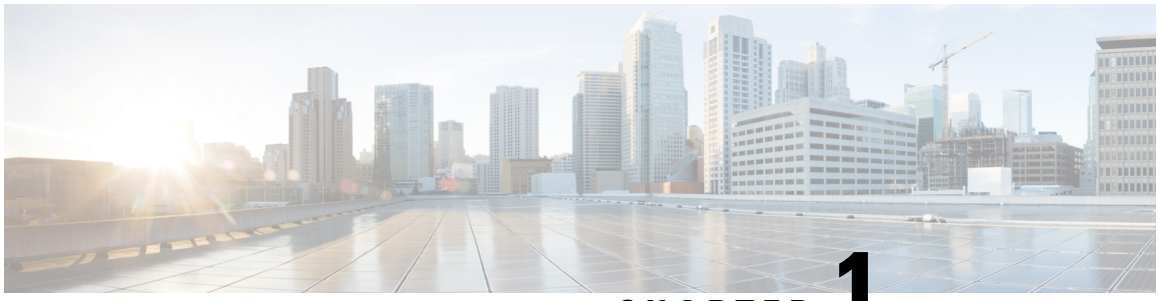
Cisco Managed Services Accelerator (MSX) 4.2 Platform User Guide

First Published: 2022-01-31

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Overview

This chapter provides information about the intended audience of the Cisco MSX platform, what's new in the current release, and related documentation.

Cisco MSX Platform Overview

Cisco MSX is an open software platform that enables service providers to create and manage services across physical and virtual network elements. The Cisco MSX solution utilizes network function virtualization and enables service providers to provide their customers a flexible selection of services that are easily customized through a self-service portal. It reduces the costs for service creation, customer acquisition, service fulfillment, time to repair, and maintenance. With Cisco MSX solution, you can automate end-to-end provisioning for different use cases and service topologies. Each release of the Cisco MSX provides out-of-box capabilities to orchestrate particular use cases, also called service packs (such as, Cisco MSX SD-WAN, Cisco MSX SD-Branch, and Cisco MSX Managed Devices). The Cisco MSX service packs are a suite of prepackaged software capabilities that fully automate the end-to-end service creation including ordering, service chaining, orchestration, service assurance, user self care, real time performance reporting, and user-defined policy changes. With these fully validated service level packages, end customers can quickly turn on, control, and ensure cloud-based managed services offered by the service provider. For more information about Cisco MSX solution, see Cisco Managed Services Accelerator (MSX) 4.2 Solution Overview Documentation.

What's New in Cisco MSX Platform

Feature	Description
Change Management and Approvals for Device Configuration	The Cisco MSX device configuration workflow includes a change request and approval capability. Modifications to an onboarded device require Change Management approval. For more information, see Configuring Change Management Approvals.
Cisco MSX IDP-initiated Flow Support	The Cisco MSX IDP now includes IDP initiated flow and validation against the Meraki implementation. For more information, see Configuring IDP-initiated SSO for Meraki.
Tracing End-to-End HTTP Request in Cisco MSX	Cisco MSX supports tracing end-to-end HTTP requests. Cisco MSX injects an X-B3-TraceID header into the requests to make it easier to trace an HTTP request. You can see the Trace ID by expanding the Notification where support is implemented.

Audience

This guide is designed for administrators who use Cisco MSX platform to configure basic operations after installing Cisco MSX.

The platform addendum should be used in conjunction with this guide.

Logging In and Logging Out of the Cisco MSX Portal

To log into the Cisco MSX portal, 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>/vms or https://<your_portal_fqdn>

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.

Your user account privileges determine what you can see and do in the user interface. For information on Cisco MSX users and the actions they can perform, see Managing User Roles.

If you are using any third-party applications with Cisco MSX, you can configure single-sign on (SSO) to access these applications from Cisco MSX. For more information about configuring single-sign on, see Configuring Single Sign-On.

To log out, in the left pane of the Cisco MSX portal, click **Logout**.

Accessing Cisco MSX APIs

In Cisco MSX, OAuth 2.0 access tokens are used to make API requests to the application on behalf of a user. After the user is authenticated using the Cisco MSX credentials, they can obtain the access token which is shown in the procedure below. The same token can be used on each API request to indicate the request is executed on behalf of the user.

Using this procedure, you can use the Cisco MSX APIs for platform or service-pack operations.

Before you begin

Configure authorization server (Auth Server) properties. For more information, see Configuring Authorization Server Properties.

Procedure

Step 1 Obtain the Cisco MSX client credentials.

Use the credential for logging in to the Cisco MSX portal. If you do not have these credentials, contact your Service Provider Administrator.

Step 2 Obtain an access token from the Cisco MSX authorization Server.

Use the following curl command to get the token.

```
curl -k -d 'grant_type=password&username=*********&password=*****' -H "Content-Type:
application/x-www-form-urlencoded" -H "Authorization: Basic *******" -X POST
https://<Product_URL>/idm/v2/token
```

Step 3 Send the access token to an API.

After obtaining the access token, send the token to an Cisco MSX API in an HTTP authorization header. The below example shows a sample curl command for updating the current password policies. Use the access_token that was obtained in Step 2 to run this curl command.

```
curl -k -X PUT --header "Content-type: application/json" --header "accept:
application/json" --header "authorization: Bearer <ACCESS_TOKEN>" -d '{ "accountLocking":
{
"enabled": true, "lockoutDurationMin": 30, "lockoutFailCount": 3,
"lockoutFailIntervalSec": 60 }, "agingRule": { "enabled": true, "expireWarningSec":
1209600, "graceAuthNLimit": 3, "maxAgeSec": 0, "minAgeSec": 0 }, "characterRule": {
"enabled": true, "minDigit": 1, "minLowercasechars": 1, "minSpecialchars": 0,
"minUppercasechars": 1 }, "description": "string", "historyRule": { "enabled": true,
"passwdhistorycount": 10, "passwdhistorydurationMonth": 60 }, "lengthRule": { "enabled":
true, "maxLength": 16, "minLength": 8 }, "name": "ppolicy_default" }'
https://<Product_URL>/idm/api/v1/pwdpolicy/ppolicy_default
```

Your client application requests an access token from the Cisco MSX authorization server, extracts a token from the response, and sends the token to the Cisco MSX API that you want to access.

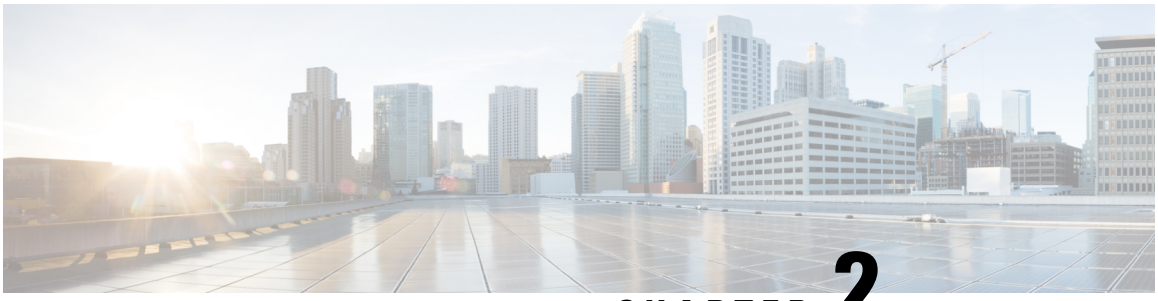
Related Documentation

You can access Cisco MSX 4.3.0 content at https://www.cisco.com/c/en/us/td/docs/net_mgmt/msx/end_user_doc/4_2/Cisco_MSX_End_User_Documentation.html.

The documents listed here are available for additional reference. To access API documentation on the Swagger GUI, log in to the Cisco MSX GUI and navigate to **My Profile > Swagger API**.

Cisco MSX SDK documentation is available at https://developer.cisco.com/site/msx/.

Document	Description
Cisco Managed Services Accelerator (MSX) 4.2 Release Notes Documentation	This documentation provides information about the new features in Cisco MSX 4.2.
Cisco Managed Services Accelerator (MSX) 4.2 Administration Documentation	This documentation covers the post-install configuration information that is required to set up Cisco MSX.
Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum	This addendum covers all the permissions that are required to operate Cisco MSX and the service packs.
Cisco Managed Services Accelerator (MSX) 4.2 SD-WAN Service Pack Documentation	This documentation includes details that are related to deploying, managing, configuring the Cisco MSX SD-WAN service pack, and troubleshooting service errors.
Cisco Managed Services Accelerator (MSX) 4.2 SD-WAN and Meraki Out-of-the-Box Applications Addendum	This document is an addendum to the *Cisco MSX SD-WAN Service Pack* content. It has details about the out-of-the-box applications of Cisco MSX 4.2 and the comparison of applications in older releases with applications in Cisco MSX 4.2 based on possible application mapping.
Cisco Managed Services Accelerator (MSX) 4.2 Enterprise Access Service Pack Documentation	This documentation includes details that are related to deploying, managing, configuring the Cisco MSX Enterprise Access service pack, and troubleshooting service errors.
Cisco Managed Services Accelerator (MSX) 4.2 Solution Overview Documentation	This documentation provides a comprehensive explanation of the design of the Cisco MSX solution that enables service providers to offer flexible and extensible services to their business customers.
Open Source Used in Cisco MSX and Service Packs Documentation	This documentation contains licenses and notices for Open Source software that is used in this product.



CHAPTER 2

User and Role-Based Access 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 user roles. Based on the permissions assigned to a user by an administrator, a user can define and customize how their services are exposed to customers. The permissions allow the user to customize 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 the following categories:

- **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 all the available permissions in Cisco MSX and to also see the minimum required permissions to perform various operations in Cisco MSX, see the latest version of Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum.

Note You will need Cisco Customer or Cisco Employee privileges to access the Cisco MSX documentation.

Cisco MSX provides out-of-the-box roles that have permissions applied by default. You can either modify the permissions associated with these out-of-the-box roles or add a new role. For the description of these permissions, see the latest version of Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum.

Cisco MSX Out-of-the-box Roles

The following are the out-of-the-box roles available with Cisco MSX:

- **Service Provider Operators** support multiple customers by maintaining service information and settings, viewing, monitoring the SP-DNA platform, remediating basic customer issues, and escalating severe issues.

- **Service Provider Administrators** have Operator permissions and can also perform more advanced tasks like managing price plans, importing, and exporting service definitions, and configuring the service platform.
- **Service Provider API Administrators** update tenant data using API calls instead of the standard methods available through applications and platform web interface. This is a powerful role, as it bypasses Tenant RBAC checks.
- **Tenant Administrators** have Tenant Operator permissions and can also perform more advanced tasks like managing service policies and configurations.
- **Super User** supports all actions from user management to service management or operator.

For more information on how to add a new role or modify an existing role and to associate this role to a user, see Managing User Roles and Managing Users.

Role-Based Access 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 user roles. Based on the permissions assigned to a user by an administrator, a user can define and customize how their services are exposed to customers. The permissions allow the user to customize 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 the following categories:

- **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 all the available permissions in Cisco MSX and to also see the minimum required permissions to perform various operations in Cisco MSX, see the latest version of Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum.

Note You will need Cisco Customer or Cisco Employee privileges to access the Cisco MSX documentation.

Cisco MSX provides out-of-the-box roles that have permissions applied by default. You can either modify the permissions associated with these out-of-the-box roles or add a new role. For the description of these permissions, see the latest version of Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum.

Cisco MSX Out-of-the-box Roles

The following are the out-of-the-box roles available with Cisco MSX:

- **Service Provider Operators** support multiple customers by maintaining service information and settings, viewing, monitoring the SP-DNA platform, remediating basic customer issues, and escalating severe issues.
- **Service Provider Administrators** have Operator permissions and can also perform more advanced tasks like managing price plans, importing, and exporting service definitions, and configuring the service platform.
- **Service Provider API Administrators** update tenant data using API calls instead of the standard methods available through applications and platform web interface. This is a powerful role, as it bypasses Tenant RBAC checks.
- **Tenant Administrators** have Tenant Operator permissions and can also perform more advanced tasks like managing service policies and configurations.
- **Super User** supports all actions from user management to service management or operator.
- **Enterprise Administrator** is a superset of Tenant Admin-level permissions, but with additional capabilities of accessing billing and licensing insights.
- **Workflow Administrator** can view and manage workflows and instances.
- **Workflow User** can view and manage workflow instances.

For more information on how to add a new role or modify an existing role and to associate this role to a user, see Managing User Roles and Managing Users.

Managing Cisco MSX Platform-Specific User Roles

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

To create a new role and assign it to users:

Procedure

Step 1 Log in to the Cisco MSX portal (as an Admin or Super User).

Step 2 Create the tenants. For more information, see Managing Tenants and Tenant Groups.

Step 3 Create a new role (such as Tenant Operator) and assign the permissions required to operate the Cisco MSX application and the service packs.

- For more information on basic permissions required to perform the documented tasks for the Cisco MSX platform and the service packs, see the latest version of Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum.
- For more information on creating a new user role, see Managing User Roles.

Step 4 Create a user (such as Tenant Operator User), assign the role defined in Step 3 to this 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

What you can see and do in the user interface is controlled by your user account privileges. In Cisco MSX, the permissions are managed using Role-Based Access Control (RBAC). RBAC restricts or authorizes system access for users based on 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 Designer role 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, see Managing Users.

Adding a User Role

Using this procedure, you can add a user role:

Procedure

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

Step 2 From the left pane, click **Roles**.

The **Roles** window is displayed.

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 box for the permission that you want to grant to the role.

For more information on permissions required to perform a specific task on the Cisco MSX platform and for the complete list of Cisco MSX permissions, see the latest version of *Cisco MSX Platform and Service Pack Permissions Addendum*.

The types of permission you can grant are:

Permission	Description
View	Provides only 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

Using this procedure, you can modify an existing role.

Procedure

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

Step 2 From the left pane of the **Service Interface**, click **Roles** to view the list of roles.

The **Manage Roles** windows are displayed.

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:

Permission	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 Users

Using this procedure, you can add new user details, assign an appropriate role to the user, and associate the new user to the tenant.

Note You can disable the creation and modification of users, if you choose **Single Sign-On** and use your Identity Provider. The following procedure, describes the use of local user accounts.

Procedure

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

Step 2 From the left pane, click **Users** to view the list of users with their details in the **Manage Users** window.

The **Users** window is displayed.

Step 3 Click **Add User** and enter details such as first name, last name and user ID, email address, and contact number.

Step 4 To assign a role, you can choose from the available options in the drop-down by selecting them from the **Assigned Roles** drop-down list. You can associate one or more roles to a user.

Step 5 Choose a tenant from the **Associate Tenants** drop-down list. You can associate one or more tenants to a user.

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

Adding a User

In Cisco MSX, after you have added the password policy in the settings through the web portal, you can add a user and assign the password policy for the user.

Using this procedure, you can add a user.

Procedure

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

Step 2 From the left pane, click **Users**.

The **Users** window is displayed.

Step 3 Click **Add Users**.

The **User** window is displayed.

Step 4 In the User window, enter:

- First Name
- Last Name
- User ID
- Email Address
- Language
- Assign Role—Choose a role from the **Assign Role** drop-down list.
- Associate Tenants—Choose a tenant from the **Associate Tenants** drop-down list.
- Password Policy—Choose a password policy from the **Password Policy** drop-down list that the user uses for his password.

Step 5 Click **Save**.

Step 6 Select a user, click the **Edit** icon from the existing Users table if you want to edit the Password Policy of the user.

Step 7 Choose a password policy from the **Password Policy** drop-down list that the user uses for his password.

Step 8 Click **Update**.

Note
- You can delete a user from the list by clicking the **Delete** icon.
- When you delete a user, the password policy also gets deleted.

Searching for a User

In Cisco MSX, the User Management window uses a pagination API form to address the scaling issue in the page.

Using this procedure, you can search for a user.

Procedure

Step 1 Log in to the Cisco MSX portal window is displayed.

Step 2 From the left pane click **Users**.

The **Users** window is displayed.

Step 3 Search for any user by using the search bar.

Note
- The search is executed using the first five characters provided. This limitation is due to the strong encryption policies for personally identifiable information used by Cisco MSX.
- It takes only a minute for the user to get indexed to be able to be searched. Once the user gets indexed, the user will show up in your searches.

Managing Tenants and Tenant Groups

The multi-tenant architecture of Cisco MSX provides the ability to segment the data stored by tenant. When tenants are defined, data is partitioned by tenant. This 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 following are the key points you must know while configuring tenants:

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

This topic contains the following sections:

Managing Tenants

You can add a new tenant and sub-tenant details using this procedure. When you add a customer user, you need to associate the user with a tenant.

The following are the key points you should know while managing tenants:

- Tenant administrators are linked to their data by a tenant object.
- Tenant objects should be unique across all clusters.
- A tenant administrator cannot view or modify the data of any tenant not under their direct control.
- A tenant administrator can manage more than one tenant.

Using this procedure, you can manage tenants.

Procedure

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

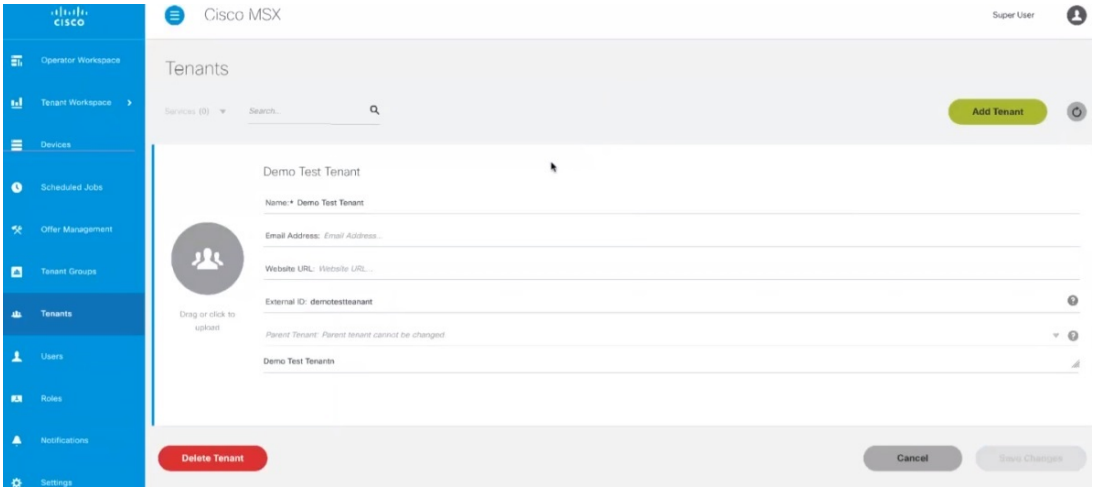
Step 2 From the left pane, click **Tenants** to view the list of existing tenants with their details on the **Tenants** window.

The **Tenants** window is displayed

Step 3 Click **Add Tenant** and enter the customer name, email address, website URL, external ID, and select the parent tenant/sub-tenant.

Note Enter the email address to receive email notification of the device vulnerabilities. The discovered vulnerability information is sent to the tenants as an alert. For more information, see Managing the Device Compliance Vulnerability Using API.

Figure 1: Tenants Window



Step 4 Click **Save**.

The new customer details are listed on the **Tenants** window as parent tenant.

You can create a sub-tenant/child tenant similarly.

You can also update the customer details (under **Action**), if required.

Step 5 Click **View Sub-Tenants** to list the sub-tenants under the parent tenant.

Note Sub-tenancy allows you to manage tenants in a parent-child relationship.

In addition, you can also disable the ability to create, modify or delete Tenants. For more details, see Configuring Integrations for Outbound APIs.

Note You can delete a tenant only if the tenant is not associated with any user.

Managing Tenant Groups

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

Using this procedure, you can manage the tenant groups.

Procedure

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

Step 2 From the left pane, click **Tenant Groups**.

The **Tenant Groups** window is displayed with the list of all the Tenant Groups.

Step 3 Create a new Tenant Group.

a) Click + on the far right of the window to add a new Tenant Group.
b) Enter the Name, Display Name, Description, Associate Tenants, and Extension Parameter(s).
c) From the **Associate Tenants** drop-down list, choose the tenants you want to add into the tenant groups.

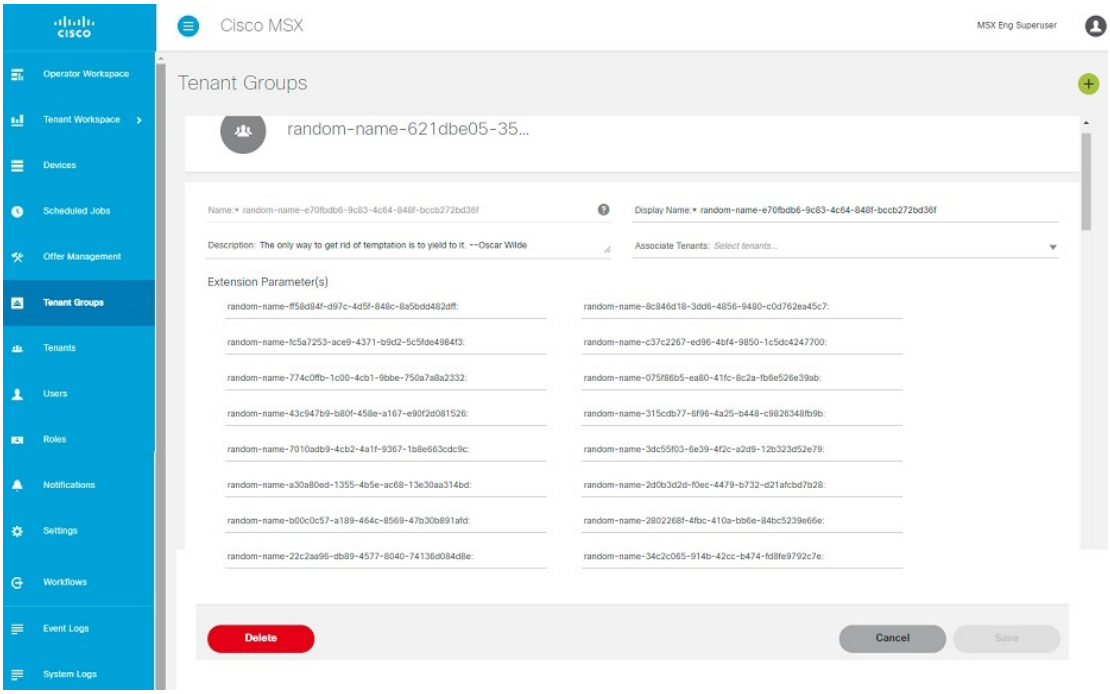
Note A tenant can be associated with only one tenant group. The **Associate Tenants** drop-down list display tenants who are not associated with any other tenant groups.

d) Click **Save**.

Step 4 Edit an existing Tenant Group.

a) Click the Tenant Group that you need to edit.
b) To edit the previous entries, enter the required data in the appropriate fields such as Name, Display Name, Description, Associate Tenants, and Extension Parameter(s).
c) Click **Save** to retain the latest changes.

Figure 2: Tenant Groups



Deleting Tenant Groups

Using this procedure, you can delete the tenant groups.

Procedure

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

Step 2 From the left pane, click **Tenant Groups**.

The **Tenant Groups** window is displayed with the list of all the Tenant Groups.

Step 3 Click the Tenant Group that you need to delete.

Step 4 Click **Delete** to remove the tenant group.

Generating Tenant Dynamically from Cisco.com Account

The Cisco MSX platform integrates with the Okta to enable the expansion of existing Cisco MSX identity capabilities and onboard users into Cisco MSX. The Cisco MSX assigns the first user from the company as the tenant administrator user. The tenant administrator can browse through the Cisco MSX as-a-service catalog and subscribe to an offer. Other users logging in to the Cisco MSX portal from the same company are grouped

under this tenant. You can enable the option to dynamically generate tenants and associate enterprise users to a tenant from the Cisco MSX portal.

The Cisco MSX platform can generate a new tenant for a user logging into the Cisco MSX portal for the first time using cisco.com credentials. The Cisco MSX portal checks the user based on the SAML attributes in the assertion and extracts the Company_Name attribute value. Once an offer subscription has been selected, Cisco MSX must create the tenant for this customer by pulling the Company_Name field from the user's cisco.com profile. If the Company_Name field is not specified, the user should be prompted to supply this information in the Cisco MSX portal. Once the tenant is created, the subscription should be associated with this tenant (federated user), and any subsequent operations for this user and subscription are done within the context of the newly created Tenant.

To enable this functionality for an enterprise, do the following:

1. Create or edit your existing SAML Identity Provider setting from the Cisco MSX portal to enable the **Create user** option.

   When **Create user** option is enabled, Cisco MSX works as follows:

   - The Cisco MSX checks the user who attempts to login based on the assertion.
   - If the user does not exist already, Cisco MSX checks tenant using the value of the Company_Name attribute and finds that tenants are missing. New tenant (federated user) is automatically created using the attributes in the SAML assertion.
   - If the user already exist, Cisco MSX compares the Company_Name attribute with the existing user's tenant. If it does not match, SSO process will stop and an error message is shown on the portal. Otherwise the user's name and email will be updated according to the value in the assertion.

2. Apply elevated user roles for an administrator user or regular user roles for other users.

For more information on new tenant creation and assigning roles, see Step 8 through Step 12 in the Configuring SAML-Based IDPs on MSX.

Viewing Permissions Mapping

The API permissions viewer allows you to view API endpoints for all Cisco MSX microservices and permissions required to execute these API endpoints.

Using this procedure, you can view the permissions mapping.

Procedure

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

Step 2 From the left pane, choose **Settings** > **API Permissions**.

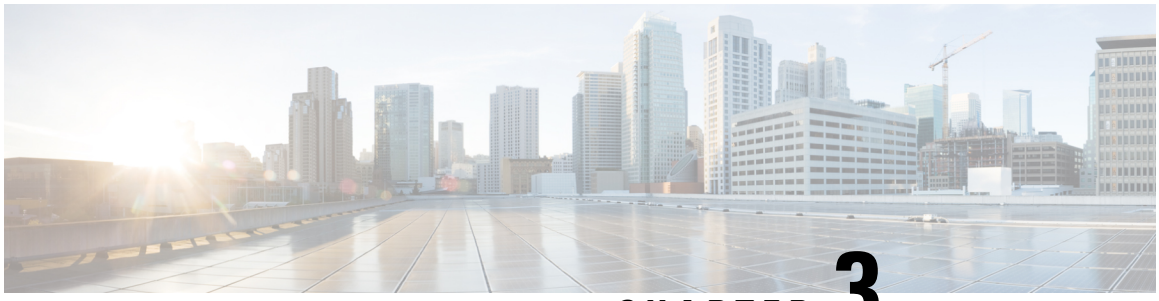
The **API Permissions Viewer** window is displayed.

You can view the permissions by:

- Microservice—Click **By Microservice** to list all the Cisco MSX services. Select a microservice to display microservice to API endpoint mapping. Click on the API endpoint to further display the permissions required for the selected API endpoint.

- Permission—Click **By Permission** to list all the Cisco MSX permissions. Select permission to display microservice. Click on the microservice to further display the API endpoint.
- Path—Click **By Path** to list all the Cisco MSX APIs. Select an API to display the type of microservice. Click on the microservice to further display the permissions.

Note
- You can also search for any permission by using the search bar.
- Some APIs may not have permissions.



CHAPTER 3

Authentication and SSO Configurations

This chapter describes Cisco MSX authentication process, managing user sessions, and information on accessing Cisco MSX APIs.

This chapter contains the following sections:

Managing Cisco MSX Authentication

Managing Cisco MSX Authentication contains the following sections:

Configuring Password Policies

The password policies allow you to enforce secure password checks on newly created passwords for additional management users of the controller and access points.

Cisco MSX allows you to configure and update password policies using an API or the Cisco MSX admin portal.

This topic contains the following sections:

Configuring Password Policies Through an API

In Cisco MSX, as a user with an administrator role, you can define various settings for the password policies, such as password strength, password length, account locking, password history, and password aging.

By default, there are three built-in policies available on Cisco MSX. As a user with an administrator role, you can modify these existing policies or create new policies. These built-in policies can be used when you add users. The default policies could be edited, but can not be deleted. The default policies created are:

- *ppolicy_default*: Applies to the consumer user.
- *ppolicy_strong*: Applies to the administrator accounts.
- *ppolicy_system*: Applies to both consumer user and administrator accounts.

To define the password policies, use the PwdPolicy POST API in the IDM User Controller section of the **User Management Service API**. For more information on the **User Management Service API**, refer to the Swagger documentation accessible from the **Cisco MSX portal > Account Settings > Swagger > User Management Service API**.

The following are the password policy settings available in Cisco MSX:

- **Password strength (characterRule)**: Determines series of guidelines that are important for a strong password.
- **Password length (lengthRule)**: Determines minimum and maximum password length.
- **Account Locking (accountLocking)**: Determines the lockout of a user account. Using this setting you can control how may invalid password attempts (**lockoutFailCount**) are allowed within a time period (**lockoutFailIntervalSec**). If the number of attempts is exceeded, then account gets locked for a specified time (**lockoutDurationMin**).
- **Password History (historyRule):** Determines whether the users can reuse previous password within a predefined time period.
- **Password Aging Rules (agingRule):** Determines how long an existing password is valid. The following password aging settings are available in Cisco MSX.
  - **Password Expire Warning Period (expireWarningSec)**: With this setting, you can set the number of seconds before a password expires. In this policy, you can also set when an email notification is sent to the user before their password expires. Use the **pwdExpireWarning** parameter to define when the user starts to receive password expiration notifications. If this time interval is set to 0, no warning messages are sent out. The user can change their password at any time before the expiry. After expiry, they must change their password to continue using Cisco MSX.
  - **Password Grace Period (graceAuthNLimit)**: Use this setting to define the number of grace login attempts after the Password lifetime limit has exceeded. In this policy, you can set the number of times an expired password can be used to authenticate after the password lifetime limit has exceeded. Users attempting to log in to the account during this grace period receives a warning message to change the password. If grace authentication is not defined for the user or the user has used all allowed attempts, user login to the account fails, and the system displays the following error message, "Your password expired. Please Reset your password".
  - **Maximum Password Age (maxAgesec)**: Using this setting, specify the number of seconds after which a password expires. Set the value to 0 if you want the password never to expire.
  - **Minimum Password Age (minAgesec)**: Using this setting, you can set the minimum number of seconds between modifications to the password. Set the value to 0 if you want to reset/change the password at any time.
  - **Password Characters (dictionaryRule)**: Using this setting, you can enable the dictionary rule to reject passwords that are vulnerable. The user’s password is checked against the words in the dictionary and is rejected if the password matches any of these dictionary words. If the parameter 'testReversedPassword' is true, the user’s password is checked against the reversed word as well.

The following is a sample implementation of the *ppolicy_default* .

```
{
  "policies": [
    {
      "name": "ppolicy_default",
```

```
"description": "PHI ppolicy_default",
"characterRule": {
  "enabled": true,
  "minDigit": 1,
  "minLowercasechars": 1,
  "minUppercasechars": 1,
  "minSpecialchars": 1
},
"lengthRule": {
  "enabled": true,
  "minLength": 8,
  "maxLength": 16
},
"accountLocking": {
  "enabled": true,
  "lockoutDurationMin": 30,
  "lockoutFailCount": 3,
  "lockoutFailIntervalSec": 60
},
"historyRule": {
  "enabled": true,
  "passwdhistorycount": 10,
  "passwdhistorydurationMonth": 60
},
"agingRule": {
  "enabled": true,
  "graceAuthNLimit": 3,
  "maxAgeSec": 10368000,
  "minAgeSec": 86400,
  "expireWarningSec": 1209600
},
 "dictionaryRule": {
    "enabled": true,
    "testReversedPassword": true
  }
}]
```


Managing Device Password Using API

Cisco MSX allows you to retrieve the deleted secrets. It also allows you to store and view the historical data of the secrets.

To define the secrets, use the below APIs in the IDM Microservice of the User Management Service API:

- Secret Controller
- Tenant Secrets Controller

For more information on the **User Management Service API**, refer to the Swagger documentation accessible from the **Cisco MSX portal > Account Settings > Swagger > User Management Service API**.

The current secret API supports:

- Soft delete
- Secret version
- Store by any combination of the identifiers like serial and device id and tenant id

You can set the force flag as an optional parameter. For example:

- For soft delete —You need to set the flag force=false

- For hard delete —You need to set the flag force=true

Note With hard delete, you cannot get the secret back, which means it is an irreversible action. By default, in Cisco MSX, the secret delete option is a soft delete, which is a reversible action, unless you mention the parameter as force=true.

Configuring Password Policies Through the Cisco MSX Portal

In Cisco MSX, as a user with an administrator role, you can configure and update password policies using the Cisco MSX admin web portal, in addition to using the API.

The password policies supported are:

1. Password History—The number of previous passwords that cannot be reused.
2. Maximum Password Age—The number of days a password is valid.
3. Minimum Password Length policy—Minimum number of characters needed to create a password.
4. Complexity Requirements—Passwords must:
   - Contain a number
   - Contain a special character
   - Contain an upper case character
   - Contain a lower case character

Using this procedure, you can configure password policies using the Cisco MSX portal.

Procedure

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

Step 2 From the left pane, choose **Settings** > **Authentication**.

The **Authentication** window is displayed.

Step 3 Click **Add Policy** to add a new policy.

The **Create Password Policy** window is displayed.

Step 4 In the Password Policy section, enter:

- Policy name
- Password History
- Password Age
- Password Length

Step 5 In the Complexity Requirements section, check:

- Must contain a number
- Must contain a special character
- Must contain an upper case character
- Must contain a lower case character

Step 6 Click **OK**.

A new policy is added and displayed in the Password Policies table.

Step 7 Select a policy from the Password Policies table, click the **Edit** icon if you want to change the password policy features.

The **Edit Password Policy** window is displayed.

Step 8 Change the features as required and click **OK**.

Step 9 Select a policy from the Password Policies table, click the **Delete** icon if you want to delete a policy feature.

The **Delete Password Policy** window is displayed.

Step 10 Click **Delete**.

Enabling Two-Factor User Authentication

Two-Factor Authentication (TFA) is an additional layer of security along with a strong password to ensure the identity of a user and reduce the risk of unauthorized access to Cisco MSX application and data. This additional factor can be something that only a user has access to, such as a One-time authentication code (OTP).

You can enable the Two-Factor Authentication from the Cisco MSX portal or by using the Global Settings API. To enable it from the Cisco MSX portal, select the **Use Two Factor Authentication** check box available in **Settings > Authentication**. For more information on the Global Setting API, refer to the Swagger documentation accessible from **Cisco MSX Portal > Account Settings > Swagger > Administration Service API**.

When enabled, it is applicable for all users. After the Two-Factor Authentication is enabled, users accessing the Cisco MSX portal must provide the following authentication factors:

- Username and password
- One-time authentication code (OTP). This code is sent to registered email address of the user. Each OTP is intended for use by only one user. This code is valid for a specific period of time and becomes invalid after the user successfully logs in.

By default, the user login attempts and validity duration of OTP are as follows:

- Number of user login attempts–The number of times a user can try logging in to the Cisco MSX portal. By default, this is five.
- Validity duration of OTP–The default validity duration of an OTP is 5 minutes. If the OTP expires, the user is forced to sign in again with the first authentication factor, that is, username and password.

Note

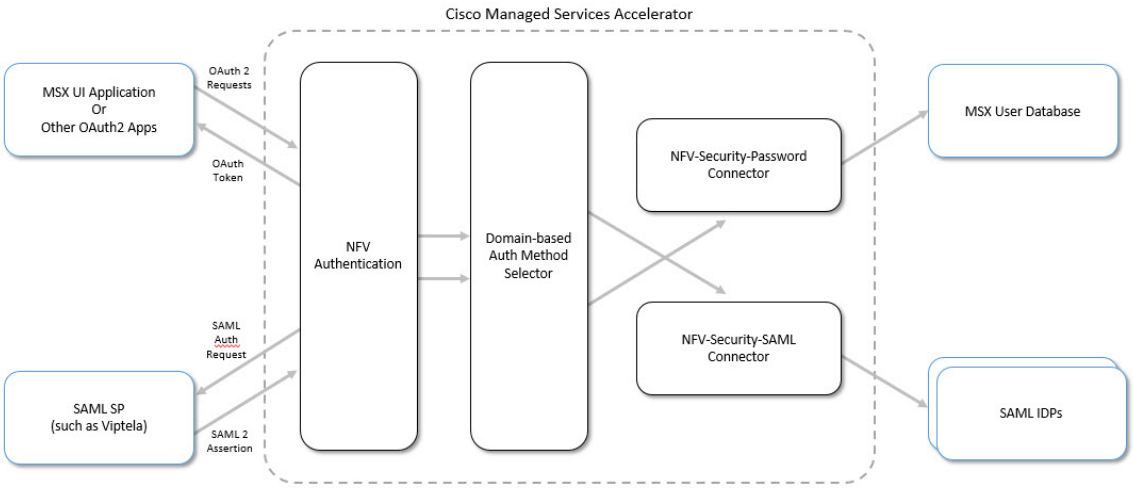
- Two-Factor Authentication is applicable only for web interface logins and not for REST API authentications.
- Two-Factor Authentication in web interface is not supported when Cisco MSX is configured with SAML Service.

Configuring Authorization Server Properties

The Cisco MSX authorization server provides standard authorization APIs - OAuth2 and SAML. Using these APIs, clients (i.e., Cisco MSX UI app, SD-WAN vManage, and so on) can authenticate their users. Access tokens granted to the authenticated user can be used to access Cisco MSX APIs.

The Cisco MSX authorization server also provides the ability to connect to different identity providers. The identity provider is resolved based on the domain. In a deployment, a domain can be configured to a specific identity provider (i.e., internal user, SAML IDP, and so on), and a client can authenticate using this identity provider via Cisco MSX authorization server using either OAuth2 or SAML.

Figure 3: Handling Login Requests



You can configure auth server properties, such as the timeout period, an authentication method, access token validity, and so on.

Using this procedure, you can specify session timeout and other auth server properties.

Procedure

Step 1 Specify the SAML protocol:

```
curl -X PUT
http://consul.service.consul:8500/v1/kv/userviceconfiguration/defaultapplication/security.auth.saml.protocol
 -d <https or http>
```

Step 2 Specify the Host:

```
curl -X PUT
http://consul.service.consul:8500/v1/kv/userviceconfiguration/defaultapplication/security.auth.saml.host
 -d <domain_name>
```

Specify the domain for which the session cookie must be set. Usually, this is the base domain when multiple IDP is configured. For example, msx.com when there are saml.msx.com and internal.msx.com, and so on. Setting it to the base domain abstract the IdP detail from third-party SSO app.

Step 3 Specify the server session timeout property. The property, server.session.timeout defines the max idle time of the server session after which the platform logs out the user out automatically. After the session timeout period, the session expires. To specify the timeout period, use the following curl command:

```
curl -X PUT
http://consul.service.consul:8500/v1/kv/userviceconfiguration/defaultapplication/
server.session.timeout -d <timeout_seconds>
```

Step 4 Set the following parameters as required:

Table 1: Parameters

Parameters	Description
Security authentication related parameters	
auth-method-supported-at-cookie-domain	Specify the supported authentication method for the session cookie. The valid values are OAuth and SAML, which means the cookie is only valid for OAuth and SAML authorization endpoints. By default, the value is set to SAML.
allowed-listed-redirect-url	Specify the redirect URL where the user will be directed to after the logout process. For example, http://localhost:9003/
login.accessTokenValiditySeconds login.refreshTokenValiditySeconds	The access token is used for API access. A refresh token can be used to get a new access token when the current one is about to expire. **Note** The refresh token's expiration time must be the same as the server session time for the Cisco MSX UI application to have consistent session timeout experience. This is because when the refresh token is expired, the server session should expire as well. This way when the client sends the auth request again, the login form is presented.
saml.clock-skew	Number of seconds before a lower time limit, or after an upper time limit, to consider the authRequest as still acceptable.
saml.expires	Number of seconds after which the message is considered expired.

Parameters	Description
saml. compare-endpoints	Indicates whether to compare the auth request message's stated intended endpoint to the actual receiver endpoint.
Key Store Properties	
Security.auth. saml.key-store.file.classpath:< file_name or file:file_path>	This property accepts classpath:file_name or file:file_path (file_path should be abolsute path) or file_path (file_path relative to the JVM working directory).
saml.key-store.file.type: keypair	
saml.key-store.key-store-password: <password>	
saml.key-store. alias: <alias_name>	
saml.key-store. password: <password>	
Identity Providers Properties	
Security.idp.internal.domain –d <internal user database >	To be used when Cisco MSX is setup as an IDP. The full domain under which the internal user database is used for authentication.
security.idp.saml.enabled -d true	Enable to connect to the external IDP.
security.idp.saml.identity-providers [0] .domain: <domain_name>	Each entry in the list represents an IDP we want to connect to. Each entry should be represented by a different domain.
security.idp.saml.identity-providers[0].metadata-file-path: < file_name or file:file_path >	The IDP's metadata location. Can be a file path (file: if the path is absolute, otherwise relative to the working JVM directory) or a url (starts with http(s)://).
security.idp.saml.identity-providers[0].entity-id: <IDP_entity_ID>	Specify the IDP's entity ID. The entity ID is available in the IDP's metadata.
security.idp.saml.identity-providers[0].external-idp-name: <external_IDP_name>	Specify the external IDP name. This is the name given for the IDP to identify Cisco MSX.
security.idp.saml.identity-providers[0].external-id-name: <email ID>	Specify the Identity Provider's email ID.

Step 5 Verify the auth server properties using the following curl command:

```
curl
http://consul.service.consul:8500/v1/kv/uservicеconfiguration/defaultapplication/security?recurse|
 python -m json.tool
```

Configuring Session Timeout Values

The Cisco MSX portal allows you to configure the inactivity timeout of a server session, as well as the absolute timeout.

Note

- Only an administrator user can modify the settings in the Settings area. These are system-wide timeouts that apply to all the users.
- Inactivity timeout defines how long the user session can last if the computer is idle or inactive for the configured amount of time. Whereas, absolute session timeout requires the user to log in again even if the user has been active the whole time.

When the session expires, Cisco MSX displays a message stating that the session has expired. You have the option to log in again or reauthenticate with the login credentials.

Using this procedure, you can configure session timeout values.

Procedure

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

Step 2 From the left pane, choose **Settings** > **Authentication**.

The **Authentication** window is displayed.

Step 3 In the session timeout, enter the inactivity timeout value and the absolute session timeout value in seconds.

Note

- Make sure that the inactivity timeout value is less than the absolute session timeout value.
- If you want to disable either one of these features, set the value to **-1**. Note that disabling these features is not recommended.

Step 4 Click **Save**.

Configuring Single Sign-On (SSO)

Cisco MSX allows you to configure and update SSO either through the API or the Cisco MSX admin portal.

Cisco MSX supports the following types of SSO configuration:

- **Configuring SAML-Based IDPs on Cisco MSX**: An Identity Provider (IDP) is responsible for issue authentication assertions. Cisco MSX can be configured with multiple SAML IDPs. If Service Providers already have one or more IDPs, they can configure Cisco MSX to work with these IDPs to set up SSO. Cisco MSX supports SAML 2.0 for SSO.

  When one or more IDPs are configured, Cisco MSX uses a subdomain to determine which IDP to route the login request to. The default IDP is the local database IDP—user credentials will be validated against the local user database. This means that by default, SSO using SAML is not enabled on Cisco MSX. Additional SAML IDP can be configured either through an API or through the Cisco MSX admin portal.

Adding an IDP allows the login request to be routed to that IDP. Users will be logged in to Cisco MSX once the IDP authenticates the user.

Note For **Configuring Identity Provider used by Cisco MSX** to work, the property `security.idp.saml.enabled` should be set to true. For more information, see the Parameters table in the Configuring Authorization Server Properties section.

- **Configuring the SSO Clients (Using Cisco MSX as an IDP)**: This means Cisco MSX can be configured as an IDP. Cisco MSX itself can also act as an IDP to other systems that want to use Cisco MSX for SSO. A third-party system can connect to Cisco MSX using OAuth2, OpendID Connect (OIDC), or SAML. SAML is an XML-based, open-standard data format that enables users to have access to multiple applications seamlessly after they sign in to Cisco MSX.

  When a user visits the third-party system, they will be redirected to Cisco MSX to login. Once Cisco MSX authenticates the user, the user will be redirected back to the third-party system and is logged in there. These third-party systems are considered SSO clients to Cisco MSX. This can work in conjunction with the multiple IDPs configured in Cisco MSX.

This topic contains the following sections:

Configuring Single Sign-On (SSO) Through API

Cisco MSX enables you to configure and update SSO through API at run time. This will allow you to add and remove IDP, OAuth2 client, and SAML client without having to interact with consul directly. It will also not require a microservice restart.

Cisco MSX supports the following types of SSO authentication through API:

- **Configuring SAML-Based IDPs on Cisco MSX**: To configure Cisco MSX with multiple SAML IDPs, use the Identity Provider Management Controller section of the **User Management Service API**. For more information on the **User Management Service API**, refer to the Swagger documentation accessible from the **Cisco MSX portal > Account Settings > Swagger > User Management Service API**.
- **Configuring the SSO Clients (Using Cisco MSX as an IDP)**: To configure Cisco MSX as an IDP, use the Security Client Controller section of the **User Management Service API** if the SSO client is an Oauth2 or OpenID Connect (OIDC) client.

  If the SSO client is a SAML Service Provider, you need to additionally add the SAML specific details by using the SAML Service Provider Management Controller section of the **User Management Service API**. For more information on the **User Management Service API**, refer to the Swagger documentation accessible from the **Cisco MSX portal > Account Settings > Swagger > User Management Service API**.

Configuring Single Sign-On (SSO) Through the Cisco MSX Portal

In Cisco MSX, as a user with an administrator role, you can configure SSO using the Cisco MSX admin portal, in addition to using the API.

You need to either add the IDP or SSO clients based on your SSO requirements.

The SSO clients are of two types—SAML and Non-SAML. It depends on the selection of the value in the **Grant Types** field selection.

Cisco MSX supports the following types of SSO authentication through Cisco MSX Portal:

Configuring SAML-Based IDPs on Cisco MSX

Using this procedure, you configure the SAML based IDP using the Cisco MSX portal (Setting up Cisco MSX as an IDP).

Procedure

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

Step 2 From the left pane, choose **Settings > SSO Configuration**.

The **SSO Configuration** window is displayed.

Step 3 Click the expand button for **Add IDP**.

A table appears with a list of all the IDPs that you can add, edit, or delete.

Step 4 Click **Add** to configure Cisco MSX with one SAML IDP.

The **Add IDP** window is displayed.

Step 5 Enter the following in the **Domain** section.

- Enter the **Domain Name**
- Select the **Type** from the drop-down list

Step 6 Enter the following in the **Identification** section.

- Entity ID
- External ID Name
- External IDP Name

Step 7 Enter the following in the **Security** section.

- Enter the **Metadata**
- Enter the **Failure URL**
- Check the **Require Signature** check box
- Check the **Require Trust Check** check box
- Enter the **Trusted Keys**

Note Click + if you want to enter multiple trusted keys.

Step 8 Create a tenant dynamically by enabling **Create User** option.

To create a tenant:

a) Check the **Create User** checkbox to create a tenant (federated user) based on the SAML assertion, if the user does not exist already.

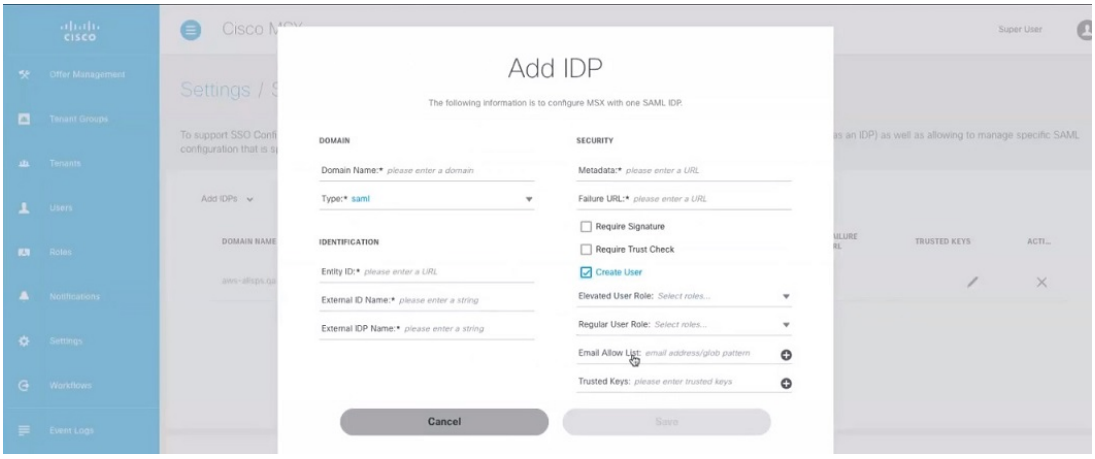
Note For more information on the dynamic tenant creation, see Generating Tenant Dynamically from Cisco.com Account.

b) Click any one of the following field to further define the create user functionality or roles.

- **Elevated User Roles**: Roles assigned to the first user, who is dynamically created as tenant.
- **Regular User Roles**: Roles assigned to the other users created under the tenant (federated user).
- **Email Allow List**: Allowed list restricts the user who can be auto created or updated from this IDP. If the allowed list is defined, only user that matches the allowed list can be auto created or updated in Cisco MSX. Each item in the allowed list will be used to match the email attribute in the assertion. The allowed list can contain exact match that is either the exact email address or just the email domain (@Cisco.com) to match all the email address from Cisco.com.

Note If the allowed list is not defined, any user from the IDP will be auto created or updated in Cisco MSX.

Figure 4: Create User



Step 9 Click **Save**.

A new IDP is added and displayed in the IDPs table.

Step 10 Select an IDP from the IDPs table, click the **Edit** icon if you want to change the IDP features.

The **Edit IDP** window is displayed.

Step 11 Change the features as required and click **Save**.

Step 12 Select an IDP from the IDPs table, click the **Delete** icon if you want to delete an IDP.

The **Delete IDP** window is displayed.

Step 13 Click **Delete**.

Configuring IDP-initiated SSO for Meraki

Using this procedure, you can configure IDP-initiated SSO for Meraki. IDP-initiated SSO allows you to access Meraki dashboard from Cisco MSX.

Procedure

Step 1 Configure the following on Meraki side:

a) Download the Cisco MSX metadata from the following link: https://msx-fqdn/idm/metadata.

b) Configure the SAML Single Sign-on for Dashboard. Perform the tasks mentioned in Meraki Documentation here.

Note Instead of uploading a metadata file, Meraki requires you to provide an **X.509 cert SHA1 fingerprint**. The x509 certificate is included in the metadata file downloaded in step a. You can use any suitable tool to generate the fingerprint. Meraki documentation shows how to do it using a Windows machine. If you are using a Mac machine, you can use the **openssl** command to generate the fingerprint. For more information, see Generating X509 Fingerprint from Metadata File on Mac, on page 29.

Step 2 After you complete the above steps, configure the following on Cisco MSX side:

a) You must create a metadata file to use in Cisco MSX because Meraki does not provide a metadata file. Follow the instructions in the section *IdP Attribute Information* to create a metadata file. Use the following as a template and replace the **validUntil** attribute as appropriate. For the **entityID** and the **AssertionConsumerService.Location** field, refer the section *IdP Attribute Information* in the Meraki Documentation.

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
validUntil="2021-11-12T16:48:56.423Z" entityID="https://dashboard.meraki.com">
  <SPSSODescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
validUntil="2021-11-12T16:48:56.422944Z"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
AuthnRequestsSigned="false" WantAssertionsSigned="true">
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://n127.meraki.com/saml/login/adMGuc_b/aVSjpa9HtWDc" index="0"
isDefault="true"></AssertionConsumerService>
  </SPSSODescriptor>
</EntityDescriptor>
```

b) After you complete the above steps, use the metadata file in Cisco MSX. For configuration, see Configuring SAML-Based IDPs on Cisco MSX, on page 27.

Step 3 Finally, add a link similar to the following in Cisco MSX to trigger the IDP initiated SSO.

```
http://localhost:8765/idm/v2/authorize?entity_id=https%3A%2F%2Fdashboard.meraki.com&
grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Asaml2-bearer&idp_init=true
```

In the above link, **entity_id** points to the Meraki SAML **entityID** you used in step 2.a, on page 29. The **idp_init** parameter tells Cisco MSX to initiate the SSO process from Cisco MSX side.

Generating X509 Fingerprint from Metadata File on Mac

Using the procedure, you can generate X509 fingerprint from a metadata file on Mac.

Procedure

Step 1 Copy the <X509Certificate> used for signing from the metadata file and save it in a temp file. For instance, tmp.txt.

Step 2 Use the following command to format the temp file to 64 characters per line:

```
sed -e "s/.\{64\}/&\r/g" < tmp.txt > idp.crt
```

Step 3 Open the idp.crt file and add **-----BEGIN CERTIFICATE-----** as the first line of the file and **-----END CERTIFICATE-----** as the last line:

```
-----BEGIN CERTIFICATE-----
<CERTIFICATE-CONTENT-HERE>
-----END CERTIFICATE-----
```

Step 4 Use the **openssl** command to generate the finger print:

```
openssl x509 -noout -fingerprint -in idp.crt
```

Configuring the Non-SAML SSO Client

Using this procedure, you can configure SSO using the Cisco MSX portal for non-SAML SSO client authentication.

Procedure

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

Step 2 From the left pane, choose **Settings > SSO Configuration**.

The **SSO Configuration** window is displayed.

Step 3 Click the expand button for **Add SSO Clients**.

A table is displayed with a list of all the SSO Clients that you can add, edit, or delete.

Step 4 Click **Add** to configure Cisco MSX with non-SAML SSO Client.

The **Add SSO Client** window is displayed.

Step 5 In the **Attributes** section:

- Select the **Grant Types** from the drop-down list.

  Note
  - Based on the **Grant Types** value you select, you can either select the SAML Authentication or non-SAML Authentication.
  - Select anything from the **Grant Types** drop-down list except for SAML2 bearer for non-SAML authentication.

    For example, if you select anything from the Grant Types drop-down list apart from *urn:ietf:params:oauth:grant-type:saml2-bearer*, it is a non-SAML authentication.

- Enter the **Additional information**

- Click **Yes/No** radio button next to the **Use Session Timeout**
- Enter the **Registered Redirect URLs**
- Enter nfv-api to the **Resource IDs**

Note *nfv-api* is the only valid resource ID value accepted right now.

Step 6 In the **Token** section, enter:

- Access Token Validity Seconds
- Max Tokens Per User
- Refresh Token Validity Seconds

Step 7 In the **Client ID** section, enter:

- Client ID
- Client Secret

Note In the case of Cisco SD-WAN, specify the IP Address of the SD-WAN Control Plane.

Step 8 In the **Scope** section, enter:

- Scopes
- Auto Approve Scopes

Step 9 Click **Save**.

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

Step 10 Select a SSO Client from the SSO Clients table, click the **Edit** icon if you want to change the SSO Client features.

Note The Client Security is displayed with **********. Do not change its value to save the SSO Client, which means that the existing value will be used.

The **Edit SSO Client** window is displayed.

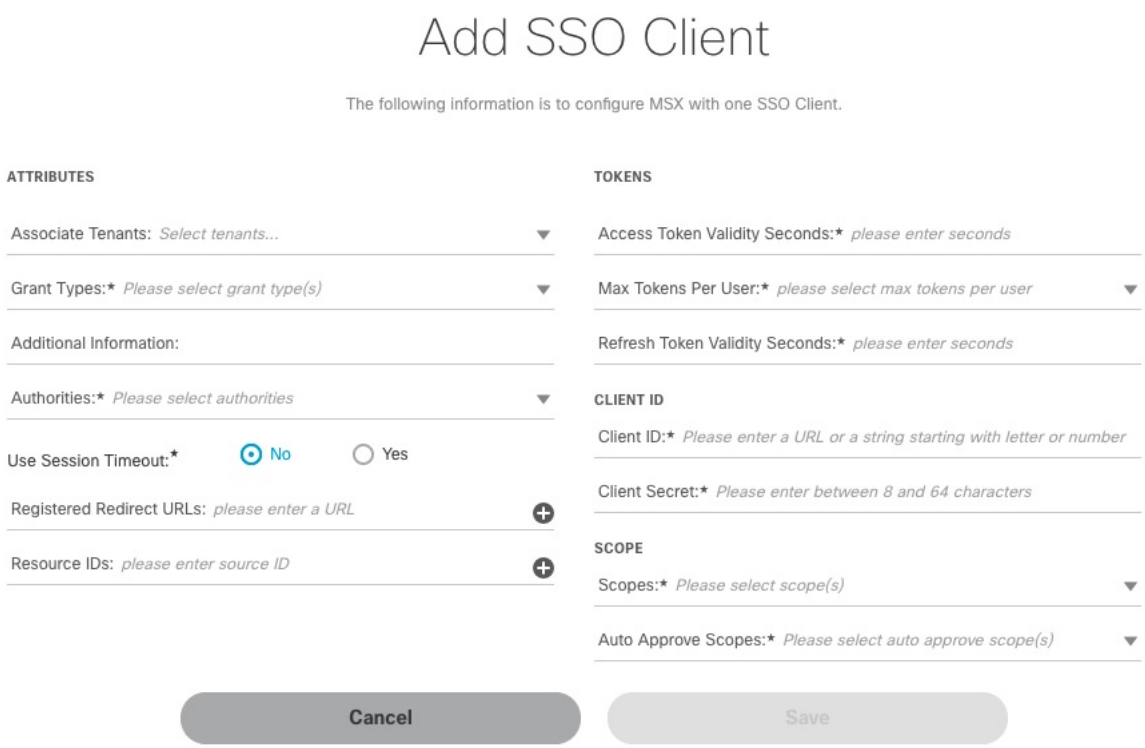
Step 11 Change the features as required and click **Save**.

Step 12 Select a SSO Client from the SSO Clients table, click the **Delete** icon if you want to delete a SSO Client.

The **Delete SSO Client** window is displayed.

Step 13 Click **Delete**.

Figure 5: Add SSO Client Window



What to do next

Applicable only for Cisco SD-WAN users (For Cisco SD-WAN-specific SSO Configuration).

For SSO to seamlessly work between Cisco MSX to SD-WAN Control Plane, do the following additional steps:

1. Upload the Cisco MSX Metadata to 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 SD-WAN Control Plane manually using the SD-WAN Control Plane web interface under Settings > Identity Provider Settings.
2. Create user roles in Cisco MSX that map to SD-WAN Control Plane user roles (Basic, Netadmin, and Operator).

Configuring the SAML SSO Client

Using this procedure, you can configure SSO using the Cisco MSX portal for SAML SSO client authentication.

Procedure

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

Step 2 From the left pane, choose **Settings > SSO Configuration**.

The **SSO Configuration** window is displayed.

Step 3 Click the expand button for **Add SSO Clients**.

A table is displayed with a list of all the SSO Clients that you can add, edit, or delete.

Step 4 Click **Add** to configure Cisco MSX with SAML SSO Client.

The **Add SSO Client** window is displayed.

Step 5 In the **Attributes** section:

- Select the **Grant Types** from the drop-down list.

  Note
  - Based on the **Grant Types** value you select, you can either select the SAML Authentication or non-SAML Authentication.
  - Select **SAML2 bearer** for SAML authentication from the **Grant Types** drop-down list.

    For example, if you select *urn:ietf:params:oauth:grant-type:saml2-bearer* from the Grant Types drop-down list, it is a SAML authentication.

- Enter the **Metadata Source**.

  Note You need to enter the Metadata Source details if you select SAML authentication, which is not required for non-SAML authentication.

  - Check the **Require Metadata Signature** box
  - Check the **Require Metadata Trust** box

- Enter the **Security Profile**
- Enter the **Metadata Trusted Keys**

  Note Click + if you want to enter multiple trusted keys.

- Enter the **Additional information**
- Click **Yes/No** radio button next to the **Use Session Timeout**
- Enter the **Registered Redirect URLs**
- Enter the **Resource IDs**

Step 6 In the **Token** section, enter:

- Access Token Validity Seconds
- Max Tokens Per User
- Refresh Token Validity Seconds

Step 7 In the **Client ID** section, enter:

- Client ID
- Client Secret

Note In the case of Cisco SD-WAN, specify the IP Address of the SD-WAN Control Plane.

Step 8 In the **Scope** section, enter:

- Scopes
- Auto Approve Scopes

Step 9 Click **Save**.

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

Step 10 Select a SSO Client from the SSO Clients table, click the **Edit** icon if you want to change the SSO Client features.

Note The Client Security is displayed with **********. Do not change its value to save the SSO Client, which means that the existing value will be used.

The **Edit SSO Client** window is displayed.

Step 11 Change the features as required and click **Save**.

Step 12 Select a SSO Client from the SSO Clients table, click the **Delete** icon if you want to delete a SSO Client.

The **Delete SSO Client** window is displayed.

Step 13 Click **Delete**.

What to do next

Applicable only for Cisco SD-WAN users (For Cisco SD-WAN-specific SSO Configuration).

For SSO to seamlessly work between Cisco MSX to SD-WAN Control Plane, do the following additional steps:

1. Upload the Cisco MSX Metadata to 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 SD-WAN Control Plane manually using the SD-WAN Control Plane web interface under Settings > Identity Provider Settings.
2. Create user roles in Cisco MSX that map to SD-WAN Control Plane user roles (Basic, Netadmin, and Operator).

Managing User Sessions

When a user is authenticated (regardless of the authentication mechanism), an authenticated session is created for the user. For an authenticated session, administrators can configure:

- A session timeout. For more information on configuring session-related properties, see Configuring Authorization Server Properties.
- Limit the number of authenticated sessions for a user. By default, the number of sessions is unlimited. For more information, see Enabling Concurrent Sessions.

Enabling Concurrent Sessions

Concurrent interactive sessions refer to the simultaneous active sessions a user can have per Cisco MSX instance. Cisco MSX session is considered active with every new login. By default, there are no limitations on the number of active sessions a user can have.

As an administrator user, you can activate and configure the concurrent sessions from the Cisco MSX Portal or by using the PUT API /administration/api/v1/globalsettings. For more information on the API, refer to the Swagger documentation accessible from the **Cisco MSX portal > Account Settings > Swagger > Administration Service API.**

Using this procedure, you can enable the concurrent session from the Cisco MSX portal.

Procedure

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

Step 2 From the main menu, choose **Settings > Integrations**.

The **Integrations** window is displayed.

Step 3 In the **Global** settings tab, select one of the following options for the Concurrent Sessions:

- Allow one session per user- Allows users to have only one active session per instance. Once the maximum number of concurrent sessions is set to 1, on the next login of a user, all the existing sessions of that user will be terminated and a new one will be initiated. This is applicable only for web portal UI sessions.
- Allow unlimited sessions per user- Allows the user to open unlimited concurrent sessions. This is enabled by default.

Retrieving the Device Password

The Cisco MSX platform allows you to retrieve the deleted or existing device password using the serial number. When the devices are deleted from the Cisco MSX, you can enter the device serial number in the **Devices** window and retrieve the deleted device password using the **IDM Microservice** API.

You can manage the configurations of the **IDM Microservice** API as follows:

Manage the secrets configuration and supports scope such as servicetype, devicetype, devicesubtype, and serialkey. Use the **Secrets Controller** API of the **IDM Microservice** API.

For more information on this API, refer to the Swagger documentation that can be accessed for **Cisco MSX portal > Account Settings > Swagger > IDM Microservice API**.

Using this procedure, you can retrieve the deleted password using the device serial number.

Procedure

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

Step 2 From the left pane, click **Devices**.

The **Devices** window is displayed.

Step 3 Click the **ellipsis (...)** that is located on the far right of the column heading and choose **Retrieve Deleted Device**.

The **Retrieve Deleted Device** dialog box is displayed.

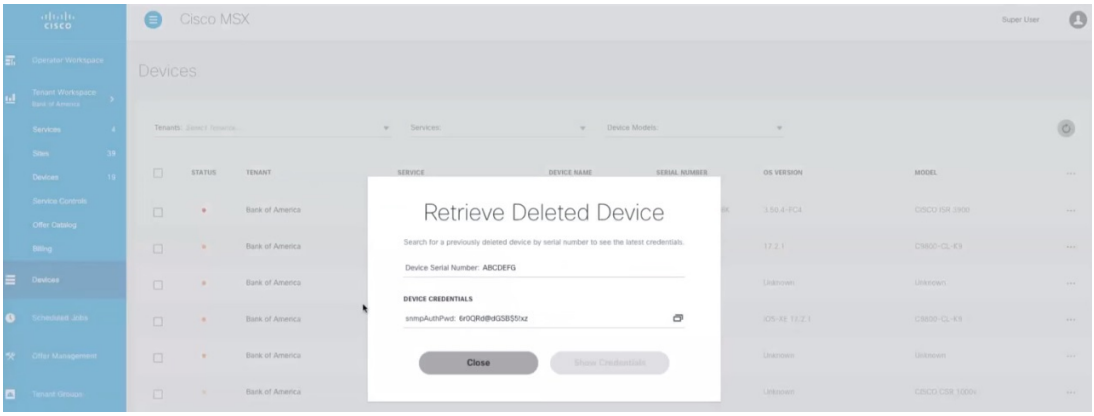
You can also select mutliple device and click the **ellipsis (...)** on the column heading to retrieve multiple deleted devices credential.

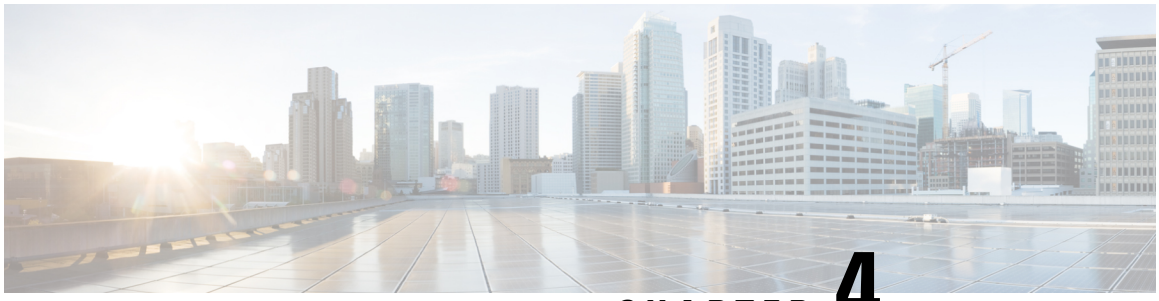
Step 4 Enter the device serial number.

Step 5 Click **Show Credentials**.

The device credential is displayed. You can also copy this device password by clicking the **Copy** icon.

Figure 6: Retrieve Deleted Device





CHAPTER 4

Other Global/Common Configurations

This chapter provides the Global/Common configuration for Cisco MSX.

This chapter contains the following sections:

Configuring Integrations for Outbound APIs

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

Procedure

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

Step 2 From the left pane, choose **Settings > BSS Integration**.

The **BSS Integration** window is displayed.

Step 3 In the **Global** tab, enable or disable the following attributes:

- Read only User View—This sets a flag that basic users are only allowed read only views.
- Show Profile—This enables the user to see all their profile data. A link will appear in the upper right-hand user menu that lets them go to their profile.
- Read only Tenant View—This enables a flag denoting a basic tenant only has read-only view of their services.

Step 4 Click the **REST Configuration** tab to set the authentication mode details for the Integrations system. Here you provide the BSS credentials to receive the API.

Step 5 Select **Basic** or **OAuth 2** based on your requirement.

- If you have selected **Basic**, enter the user ID and password of the Integrations system.
- If you have selected **OAuth 2**, enter the client ID, password, Token request URL, HTTP Method, Token Validation header, Token header format, and other necessary details.

Step 6 Click **Save** to save the authentication details.

Step 7 In the **Outbound API** tab, under **API Context**, enter the base context URL for the outbound API calls in the **Base Context** attribute. It allows you to define the file path for APIs to BSS.

a) Under **APIs** area, you can modify the **Allowed Values**, **Pricing Options**, **Accessible Services**, **Service Cancellation**, **Notification URL** of APIs. Click **Update** to save changes.

Step 8 The **Service Pack API** tab allows API payload validation by platform from service packs.

Configuring SMTP Parameters

Using this procedure, you can configure various SMTP parameters using SMTP settings. The Cisco MSX portal allows you to edit the SMTP settings after the installation.

Procedure

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

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

The **Settings** window is displayed.

Step 3 Click **SMTP**.

Step 4 Enter the following SMTP Basic information:

- Host name
- Port
- Support email address
- Write timeout (in milliseconds)
- Connection timeout (in milliseconds)
- Retry delay (in milliseconds)
- Retries

Step 5 Enter the Security setting details that allows Cisco MSX to communicate to the SMTP server. The security setting has the following fields:

- Require TLS—Check the check box in case you need to enable an SSL connection between Cisco MSX and the SMTP server.

- Require Auth—Check the check box in case you need to configure a username and password to be used while connecting to the SMTP server. When you enable it, the following fields get enabled:
  - Username
  - Password
  - Confirm Password

Step 6 Click **Save**.

Enabling Notification for Events

You can either enable notifications for various events through email or REST API. Cisco MSX provides support to trigger notifications when certain events occur:

Note

- Ensure you have configured Integrations, REST configuration details, and Outbound API details for sending REST notifications, if you want to use REST API rather than email notifications. For more information, see the section Configuring Integrations for Outbound APIs.
- Both REST and Email communication modes are supported for all of the following list of events. However, only Email notification is supported (and not REST) for the event **End User Password Reset Link**.
- Email notifications are sent only when you have configured email client.

Table 2: List of Events

Recipients	Events
Consumer, operator, or administrator	Password is reset.
Remote user	• Remote user created or deleted. • User ID is activated or deactivated/suspended. • Password reset.

Recipients	Events
Service Provider End User	• Update Site • Delete Site • Add Site • Tenant Added. • Tenant Updated. • Tenant Deleted. • Approval Pending for Requester. • Approval Pending for Approver. • Service Approved or Rejected. • Device Added. • Device Deleted. • Device Only Purchase. • Device Updated. • Device Registered. • End User Added. • End User Deleted. • End User Password Reset Link (supports only Email notification).

Recipients	Events
Service Provider End User	• End User Password Success Confirmation. • End User Updated. • Confirmation for Service Order. • Service Order Failure. • Service Activation Success Confirmation. • Service Activation Failure. • Service Deprovisioned. • Service Deprovisioning Failure. • Service Unsubscribed. • Service Updated • Service Update Failure. • Configuration of Tenant VCE Required (indicating that the Cisco VCE is added to the Cloud VPN service). • SSL VPN User Added. • SSL VPN User Add Failure. • SSL VPN User Deleted. • SSL VPN User Password Reset Link (supports only Email notification). • SSL VPN Password Reset Success. • SSL VPN Password Reset Failure. • SSL VPN User Status Changed. • Enable Bandwidth Prioritization.

Using this procedure, you can enable notification for events.

Procedure

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

Step 2 From the left pane, click **Notifications**.

The **Notifications** window is displayed.

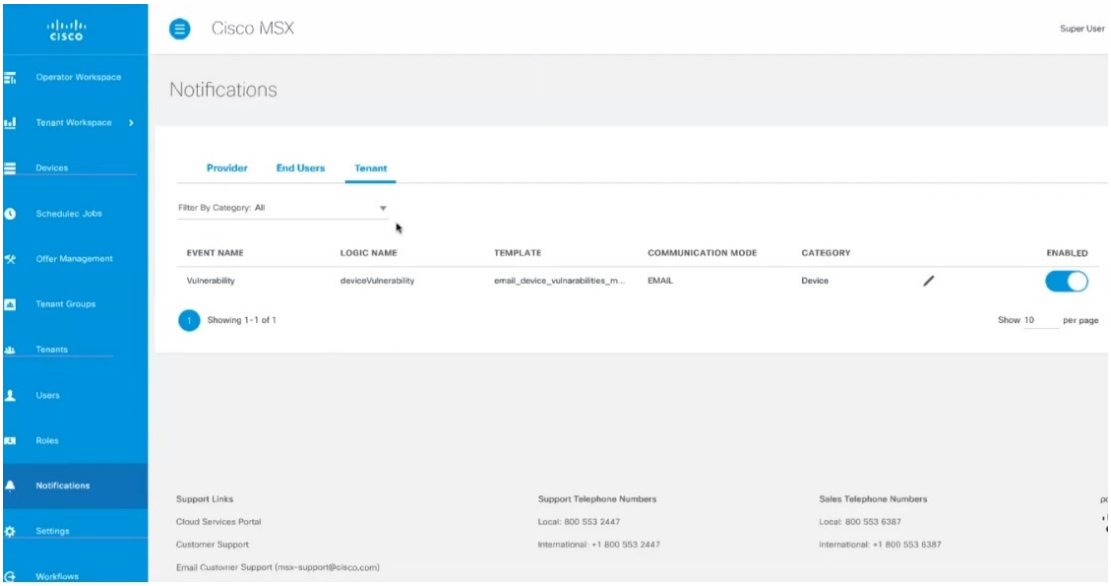
Events related to Provider, End Users, and Tenants are displayed when you click the **Provider**, **End Users**, or **Tenant** tab respectively.

- Using the **Category** drop-down list, you can further categorize events.

- For an event, you can edit the **Template** name, **Communication Mode** by clicking the **Edit** icon (located next to the Communication Mode value).
- You can also enable or disable the notification for a specific event.

The **Tenant** tab contains the vulnerability events details of the registered devices. The new template is created for the notification service to support vulnerability alerts. The vulnerability information is communicated to the tenants by sending an email, which contains the list of discovered device vulnerabilities and the severity level of the devices. The email address of the Cisco MSX tenants should be updated periodically and stored for sending the email communication. The tenant emails are included in the **Tenants** window. For more information, see Managing Tenants.

Figure 7: Notifications Window



Auditing an Event Log

Cisco MSX provides an auditing framework that allows you to capture Platform and Service Pack events.

Cisco MSX auditing framework is a microservice that monitors, collects, and publishes auditing events data. This framework also provides integration endpoints for third party systems to monitor real-time auditing events via technologies such as HTTP streams.

Cisco MSX auditing framework relies on Kafka to collect auditing events. Also, this framework is protected by Cisco MSX SSO.

Cisco MSX auditing framework has two components - the library and the collecting service that would expose a set of APIs and streaming of the components to expose the data collected. Streaming APIs is used for general purpose.

Currently, Cisco MSX supports three types of events:

- General-purpose audit events—Publish general-purpose events via an Auditing API

- Device logging events—Publish device logging events via an Auditing API
- Auditing events—Publish auditing events via an Auditing API

For more information on the Auditing API, refer the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Auditing Microservice API**.

Configuring an Announcement

Using this procedure, you can create an announcement text to display the alert messages such as planned maintenance alert and technical issues. These announcements are displayed for users upon login.

Procedure

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

Step 2 From the left pane, choose **Settings > Announcements**.

The **Announcements** window is displayed.

Step 3 Enter the title and the message to be communicated.

Step 4 Choose an announcement style - **Danger**, **Warning**, **Info**, or **Success** from the **Visual Style** drop-down list, depending on the criticality or type of announcement to make.

Step 5 Optionally select the **Start Time** and **End Time** for the announcement.

If **Start Time** is not specified, the announcement is displayed immediately after it is saved. If an **End Time** is not specified, the announcement is displayed indefinitely after start time - You need to resolve the message for it to stop displaying.

Step 6 Choose either **Page Header Announcement** or **Ticker Announcement** to select the Announcement Type.

Step 7 Click **Save**.

The newly added announcements are listed.

Once the issue is resolved, you can select the announcement that you want to delete from the list.

Viewing Permissions Mapping

The API permissions viewer allows you to view API endpoints for all Cisco MSX microservices and permissions required to execute these API endpoints.

Using this procedure, you can view the permissions mapping.

Procedure

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

Step 2 From the left pane, choose **Settings > API Permissions**.

The **API Permissions Viewer** window is displayed.

You can view the permissions by:

- Microservice—Click **By Microservice** to list all the Cisco MSX services. Select a microservice to display microservice to API endpoint mapping. Click on the API endpoint to further display the permissions required for the selected API endpoint.
- Permission—Click **By Permission** to list all the Cisco MSX permissions. Select permission to display microservice. Click on the microservice to further display the API endpoint.
- Path—Click **By Path** to list all the Cisco MSX APIs. Select an API to display the type of microservice. Click on the microservice to further display the permissions.

Note
- You can also search for any permission by using the search bar.
- Some APIs may not have permissions.

Managing Service Chains in Cisco MSX

Using the Cisco MSX CRUD APIs, you can manage configurations for the following entities for the service chains in Cisco MSX:

- SD-Branch Catalog
- Service virtual network function descriptor (VNFD)—VNFDs describe the requirements of a particular VNF on its execution environment. For example, a given VNF might need a fixed set of virtual CPUs and a certain amount of memory and disk space.
- Service network service descriptor (NSD)—NSDs describe the relationship between a set of VNFDs such that they become a network service. Typically, this entails a service chain of connected VNFDs with parameters for how they function together. For example, the NSD could specify the options for scaling up the service if utilization passes a certain threshold.

  Descriptors are templates to instantiate VNFs and services. After being instantiated, these are represented as *records*: NSR and VNFR.
- Service network service information (NS Info)—In the latest ETSI specifications, NSR and VNFR are renamed as NS Info and VNF info elements.

For more information on these APIs, refer to the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Orchestration API**.

Important Notes:

- Any configuration changes to the service chains must be executed only using these service chain APIs.
- Only users with **NSO Configuration/Data (Manage)** permission can execute these service chain APIs. This permission can be found under the **Services, Configurations, and Devices** category.
- Cisco MSX provides two sets of service chain APIs for SD-Branch Catalog, VNFD, and NSD. One set of APIs needs ‘ShardID’ as input, whereas the other set of APIs requires ‘servicetype’ as an input.

Use only the API that requires ‘servicetype’ as an input to make these configuration changes because the “ShardID” are deprecated.

Standardizing Device Listing and Status

Cisco MSX allows you to create a centralized place for device listing and the visualizing associated site status through a defined API across all the service packs that are deployed within Cisco MSX.

The capabilities of Device API (/v4/devices) are to:

- Create a device
  - Create a device with and without having a prior subscription ID and a service instance ID.
  - Create a device with and without having a prior serial key (This is optional).
  - Set initial status to a new device created.
  - Create non-NSO devices, such as Meraki.
- Delete one device by ID
- Get one device by ID
- Get paginated devices by filters (multiple filters, that is, AND combination is supported at a time to get the desired result)
- Get count of the total number of devices by filters (Multiple filters, that is, AND combination is supported at a time to get the desired result)
- Update the device status

Cisco MSX supports three types of v4 devices for creating and deleting devices:

- Unmanaged Devices—When you create/delete a device, the device gets created/deleted in the platform and does not need further processing by any system, like NSO or Meraki.
- Managed Devices (NSO-specific devices)—When you create/delete a device in the platform, it expects to be processed by other devices. This is used by Cisco MSX SD-Branch and Managed Device service pack.
- Managed Devices (Viptela and Meraki-specific devices)—When you create/delete a device in the platform, it expects to be processed by other devices.

Only users with **Device Settings (Manage)** permission can execute these Device APIs. This permission can be found under the **Services, Configurations, and Devices** category.

To enable this feature, use the **Devices (/v4/devices) API** in the **Device Controller** section of the **Manage Service API**. For more information on these APIs, refer to the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Manage Service API**.

Managing Region Using API

The Cisco MSX platform provides **Administration Microservice** API to create, update, delete, and get configurations of the region. This API manages the PnP and VPN configurations of the region.

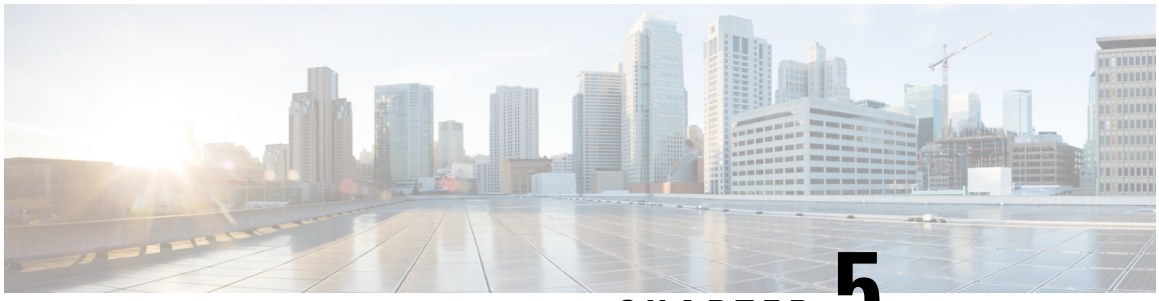
Use the **Administration Microservice** API for the following:

- To manage the region configuration, use the **Region Controller** section of the **Administration Microservice** API.
- To manage the PnP configuration, use the **PnP Controller** section of the **Administration Microservice** API.
- To manage the VPN configuration, use the **VPN Controller** section of the **Administration Microservice** API.

From the **Integrations, Settings, and Logs** category, assign these permissions to a user to run this API.

- Region (View and Manage)
- PnP (View and Manage)
- VPN (View and Manage)

For more information on this API, see the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Administration Microservice API**.



CHAPTER 5

Service-Specific Configurations

This chapter provides the Service-Specific configuration for Cisco MSX.

This chapter contains the following sections:

Enabling Multiple Subscriptions for a Tenant

Multiple orderings of a service allow service providers to customize the same service to meet different needs of a subscriber. For example, multiple WAN networks can be instantiated separately for security reasons to provide an air gap in the network by configuring a red network and a green network using WAN network.

As a user with an administrator role, you can enable this feature at the service definition time. Upon installing service packs, you need to do the necessary configuration at the service pack level to enable this feature on Cisco MSX Portal. To configure this feature, enable the multipleInstance metadata using the POST request in the Catalog Service API. For more information on this API, refer the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Cisco MSX Platform Catalog Service API**. By default, only a single instance of a service can be ordered. After this feature is enabled, tenants can order more than one instance of a service.

```
{
"id": "f3e326cc-6545-11e7-6547-be2e65b06b65",
"name": "vbranch",
"label": "cisco.consume.service.vbranch.name",
"activeFlag": true,
"version": 1,
"displayOrder": 1,
"description": "cisco.consume.service.vbranch.description",
"image": "/services/vbranch/images/icons/image_vbranch_service.svg",
"multipleInstanceAllowed": true,
"configuration": {
"device": "false",
"parts": "2",
"showOffers": "true"
  },
```

Note Multiple Service instance is supported for both Create and Update Subscription.

Assigning Offers to Tenants

Using the Cisco MSX platform, you can hide or show service offerings to a tenant or a group of tenants. You can enable this feature from the Cisco MSX portal or by using the **Cisco MSX Platform Catalog Services** API. Only tenants with required permissions can subscribe to the service offerings visible to them. The **Cisco MSX Platform Catalog Service** API provides an extended capability to set labels or tags such as Preview on the service offer that is available on the **Tenant Workspace > Offer Catalog** window.

Use **Cisco MSX Platform Catalog Services** API to create, update, cancel, close, and delete service offerings.

You can manage the configurations of services and offers using **Cisco MSX Platform Catalog Services** API:

- Manage the services configuration, use the **Service Controller** section of the **Cisco MSX Platform Catalog Services** API.
- Manage the offers configuration and provide labels on the service offer, use the **Service Offer Controller** section of the **Cisco MSX Platform Catalog Services** API.

From the **Services, Configurations, and Devices** category, assign the following permissions for the user to run this API.

- Subscribed Services (View)
- Import Service and Offer Definitions (Manage)

For more information on this API, refer to the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Cisco MSX Platform Catalog Services API**.

The service providers can assign the service offers to a specific or all tenants from the Cisco MSX portal.

Using this procedure, you can assign service offer to the tenant.

Procedure

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

Step 2 From the left pane, click **Offer Management**.

The **Offer Management** window is displayed.

Step 3 Select an offer.

The service offer details window displays both the **Variant Details** pane and **Tenant Assignments** pane.

The **Variant Details** pane allows you to view the details of the service offers.

The **Tenant Assignments** pane allows you to restrict the service offers to the specific tenants.

Step 4 Edit the service offer or variants in the **Variant Details** pane.

a) To edit the title, description, image of a service offer, and pricing details of the variants, click the **Edit** icon that is located on the top right of the window.
b) Click **Save** to update the latest changes of the service offers or variants.

Step 5 Assign service offer to tenant from the **Tenant Assignments** pane.

Note The service offers are available to all tenants. To restrict, assign the offer only to the specific tenants.

a) From the **Tenant Assignement** pane, click the **Assign** icon that is located on the top right of the window and do one of the following:

Note The tenants, who are already subscribed to a service offer cannot subscribe to this same service offer again. Assigned tenants are displayed in the **Tenant Assignments** pane. Add only new tenants to this offer.

- Click the **Specific Tenants** radio button and select the tenants.
- Click the **All Tenants** radio button to select all the tenants.

b) Click >.

The **Confirm Assignment** dialog box is displayed. Confirm the assignation of the offer to the specific tenants or all the tenants.

c) Click >.

The **Tenants Assignment** dialog box is displayed with the information that tenants are added.

Note If the tenant assignment fails, the failure message and number of tenants failed to be assigned are displayed.

d) Click **Close** to exit.
e) (Optional) Click **View Tenants** to see the list of tenants to whom the offer is assigned on the **Tenant Assignments** pane.

What to do next

Tenants can view the assigned offers by clicking **Tenant Workspace > Offer Catalog**. The list of all the assigned application offers are displayed on the **Offer Catalog** window for the tenants to subscribe to the available offers. For more information, see Subscribing an Application from Tenant Workspace.

Unassigning offers From Tenant

Using this procedure, you can unassign service offer from tenant.

Procedure

Step 1 Log in to the Cisco MSX portal using your credentials.
Step 2 From the left pane, click **Offer Management**.

The **Offer Management** window is displayed with all the available service pack offers.

Step 3 Select a service pack offer.

The **Offer Details** window is displayed. The **Variant Details** pane lists the available variants and the **Tenants Assignments** pane that lists the tenant to whom the service pack offer was assigned.

Step 4 Select the tenant to unassign the service pack offer.

Step 5 Click the **X** icon in the **Unassign** column of the **Tenants Assignment** pane.

Note If a tenant had already subscribed this service pack offer, the **Unassign** icon appears to be disabled.

The **Unassign Tenant** dialog box is displayed.

Step 6 Click **Unassign**.

The **Tenant Unassigned** dialog box is displayed.

Step 7 Click **Close** to exit.

Step 8 (Optional) Click **View Tenants** to view the tenants list in the **Tenants Assignment** pane.

Subscribing to a Service Offer from Tenant Workspace

Using this procedure, tenants can subscribe to a service offer.

Procedure

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

Step 2 Select the tenant.

The tenant dashboard is displayed.

Step 3 Click **View Offer Catalog**.

The **Offer Catalog** window is displayed with all the available service offers assigned by the service provider for the tenants.

Step 4 Select an application.

Step 5 Click **Subscribe**.

The **Confirm Subscription** dialog box is displayed to confirm the subscription.

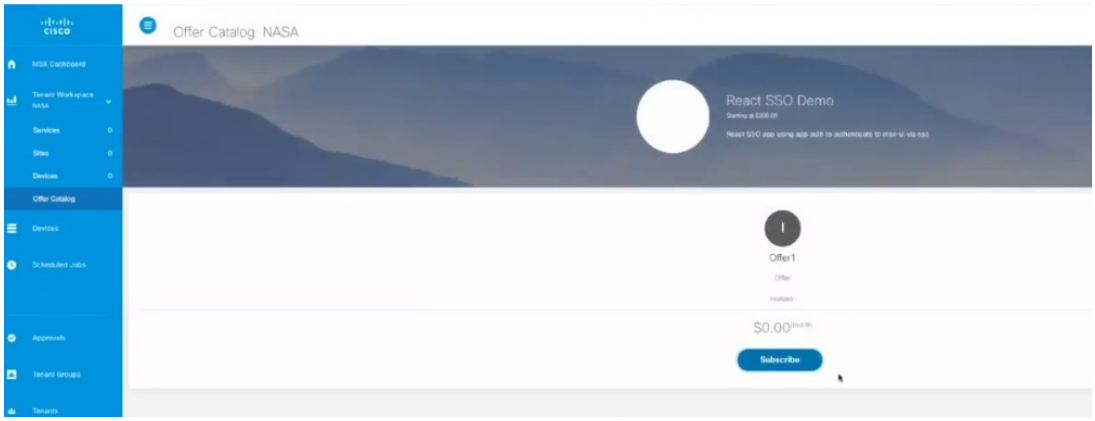
Step 6 Click **Subscribe**.

The confirmation dialog box is displayed.

Step 7 Click **Continue**.

The application is subscripbed to the tenant. This application is displayed on the tenant dashboard.

Figure 8: Offer Catalog



Unsubscribing Tenants from an Application

Using this procedure, tenants can unsubscribe an application from Tenant Workspace.

Procedure

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

Step 2 From the left pane, choose **Tenant Workspace**.

Step 3 Select the tenant.

The tenant dashboard is displayed.

Step 4 To unsubscribe from an application, click **X** that appears on the far right of the application pane.

The **Unsubscribe** dialog box is displayed.

Step 5 Click **Unsubscribe**.

Defining Terms and Conditions for a Service

Using this procedure, you can define and maintain the terms for a service.

Procedure

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

Step 2 From the left pane, choose **Settings > Service Configuration**.

The **Service Configuration** window is displayed.

Select the service pack.

Step 3 Click **Terms & Conditions**.

Step 4 Select one of the service packs offers from the **Offers** drop-down list.

Step 5 Select the desired format for the font.

Step 6 Enter details required for acceptance by a consumer while purchasing a service. This information is displayed while the consumer places an order for the service. The terms and conditions are defined specific to an offer in a service.

Step 7 Click **Save**.

Building New Services Using Cisco MSX Platform SDK

Cisco MSX Platform SDK allows you to build new services for Cisco MSX. These new services can be:

- Platform extensions that add functionality to the platform.
- Service packs that implement new products apart from the service packs provided by Cisco MSX. Cisco MSX provides SD-Branch, SD-WAN, Cloud UTD, Managed Devices, and Enterprise Access service packs. For more information on the service packs available with Cisco MSX, see Cisco Managed Services Accelerator (MSX) 4.2 Solution Overview Documentation.

The Cisco MSX supports the following APIs integrated as part of the platform SDK:

- User Management Service
- Catalog Service
- Manage Service
- Monitor Service
- Workflow Service

The Cisco MSX SDK documentation is available here: *https://developer.cisco.com/site/msx*.

Onboarding and Deploying Component into Cisco MSX

The Cisco MSX allow service providers to develop the third-party services or components using the Software Development Kit (SDK). These new services can be onboarded, deployed, and published into Cisco MSX. You can enable this functionality from the Cisco MSX portal or by using the **Service Lifecycle Management (SLM)** API. The new service can be any service, including platform extension, which can run within the Cisco MSX infrastructure after the platform is deployed.

Each component can provide one or more APIs and applications.The component is a configuration file that contains all the information required to onboard and deploy a service. Applications must be published to the Cisco MSX Offer Catalog before users can subscribe to the applications.

The capabilities of the SLM API include:

- Uploading a third-party component (in parts, if required)
- Getting component details

- Getting the deployment status of component Kubernetes
- Getting a list of components
- Deleting a component

To deploy a new service using API, use the **Service Lifecycle Management Controller** section of the **SLM** API.

From the **Services, Configurations, and Devices** category, assign the Service Lifecycle Management (View and Manage) permission to a user to run this API.

For more information on this API, see the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Service Lifecycle Management API**.

Process involved in onboarding a new service into the Cisco MSX:

1. Deploying the Component
2. Publishing the Application
3. Creating an Offer

Deploying the Component

Using this procedure, the service providers can deploy the service or components in Cisco MSX from the Cisco MSX portal.

Procedure

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

Step 2 From the left pane, click **Settings > Component Management**.

Step 3 Click the **Upload Component** icon that is located on the far right on the **Component Management** window.

The **Upoad Component** dialog box is displayed.

Note Click **Sample Manifest** to know more about the configuration details that needs to be included in the new service tar files.

Step 4 Choose the component tar file from your local storage.

Step 5 Click **Upload** to upload and install the component into Cisco MSX.

The confirmation dialog box is displayed to confirm the new component upload.

Step 6 Click **Upload**.

Note Uploading a component might take few minutes depending upon the size of the application.

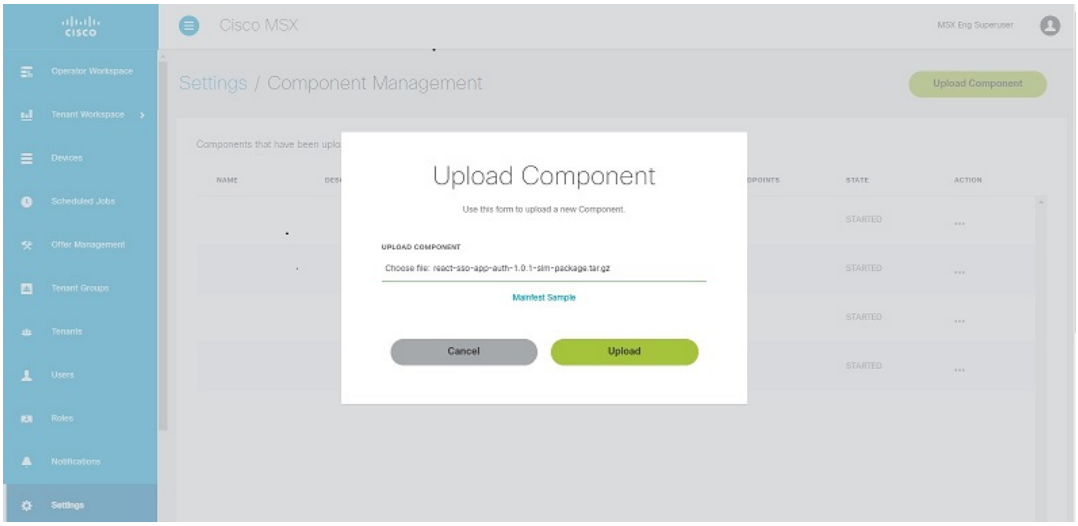
Step 7 After the successful completion of the new component upload, the confirmation dialog box appears, click **Close**.

The **Component Management** window displays the newly uploaded component. The component details such as Name, Description, Product, Version, Endpoint, State, and Action are displayed on this window. Specify the endpoint value to display both the **Delete** and **Publish Application** options on clicking the **ellipses (...)**

icon that is located on the same row of every component. If the endpoint values are not included only Delete option is displayed.

The newly uploaded service component is now readily available as a part of the Cisco MSX Microservices API list. You can use this new API to manage the new component.

Figure 9: Uploading Component



Publishing an Application

After deploying a component, it should be published to make it available on the Cisco MSX. On publishing this new application, a tile is created on the **Offer Management** window. A tenant cannot subscribe to the application until it has been published, and an offer is created.

Using this procedure, you can publish an application into the Cisco MSX.

Procedure

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

Step 2 From the left pane, click **Settings > Component Management**.

Step 3 Click the **ellipses (...)** icon that is located on the same row of the component and click **Publish Application**.

The **Add Application** dialog box is displayed.

In the **Add Application** dialog box, specify the following details:

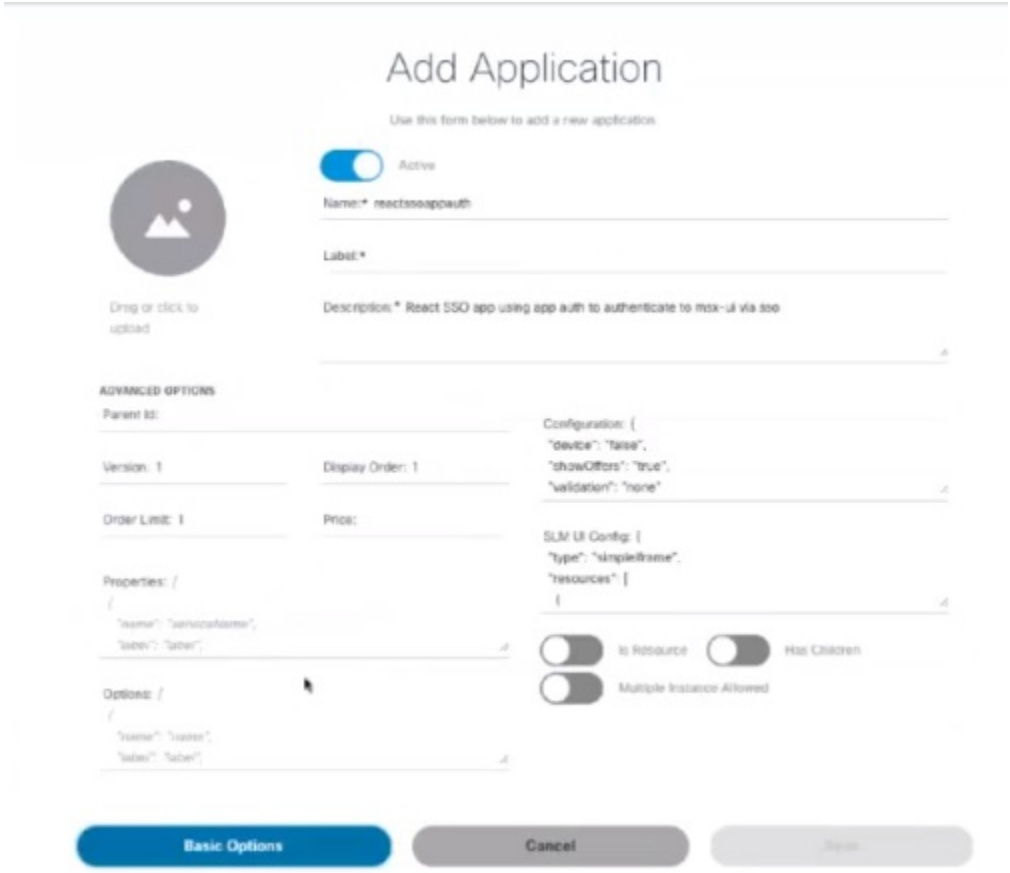
- Enter the Label of the application. The Name and Descriptions are automatically populated.
- Click **Advanced Options**, if you need to enter some additional details to further define the application.

Note Click **Basic Options** to enter only basic information, without any additional data.

Step 4 Click **Save**.

The newly-added application is displayed on the **Application** window.

Figure 10: Adding Application



Creating an Offer

Using this procedure, you can create an offer that has pricing and terms and conditions details.

Procedure

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

Step 2 From the left pane, click **Settings > Component Management**.

Step 3 Click the **ellipsis (...)** on the far right in the same row of the application and then click **Offer**.

The **Add Offer** dialog box is displayed.

Step 4 Enter the Name, Label, Description, Terms and Conditions, and Price Plan of the offer.

Step 5 Click **Save**.

The newly-added offer is displayed on the **Offer** window. You can create as many offers as you want.

The offers can be edited, duplicated, or deleted. To know more about managing offers, see Managing an Offer.

Figure 11: Offers Window

What to do next

- From the left pane, choose **Offer Management**.

  The **Offer Management** window displays the deployed service component tile. Click the new component tile to see the offers.

- The Cisco MSX service providers can assign service offer to the tenant from the **Offer Management** window. For more information, see Assigning Offers to Tenants.

- The tenants can subscribe to the assigned offers. For more information, see Subscribing an Application from Tenant Workspace.

Managing an Offer

Using this procedure, the service providers can manage the service offers from the Cisco MSX portal.

Procedure

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

Step 2 From the left pane, choose **Settings > Component Management**.

Step 3 Click the **ellipsis (...)** on the far right in the same row of the application that needs to be edited or duplicated.

Step 4 Choose **Offer**.

The **Offer** window is displayed.

Step 5 **Edit an offer.**

a) Click the **ellipsis (...)** on the far right in the same row of the existing list of offers and choose **Edit**.

The **Edit Offer** dialog box is displayed.

b) Enter the Name, Label, Description, Terms and Condition, and Price Plan of the offer.

c) Click **Save**.

Step 6 **Duplicate an offer.**

a) Click the **ellipsis (...)** on the far right in the same row of the existing list of offers and then choose **Duplicate**.

The **Add Offer** dialog box is displayed.

b) Enter the Name, Label, Description, Terms and Condition, and Price Plan of the offer.

c) Click **Save**.

Deleting the Component from Cisco MSX

Using this procedure, service providers can delete the service or component from Cisco MSX.

Procedure

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

Step 2 From the left pane, choose **Settings** > **Component Management**.

The **Component Management** window is displayed.

Note If the tenants are subscribed to the application that is to be deleted, the service providers should ensure that the tenants unsubscribe from that particular application. For the tenants to unsubscribe from the application, choose **Tenant Workspace** > **Services**. Click the **Unsubscribe** icon that is located on the far right of the application pane that is to be deleted.

Step 3 Click the **ellipsis (...)** on the far right in the same row of the component that you need to delete and then choose **Delete**.

The **Delete Component confirmation** dialog box is displayed. Confirm the deletion of the component from Cisco MSX.

Step 4 Click **Delete**.

The component is deleted.

Uploading a New Network Element Driver Package

The NED is uploaded to Cisco Network Services Orchestrator (NSO) to enable network connectivity of different device types and services. Cisco MSX allows you to add, replace, and delete NED for device management.

You can add a new NED at any time after the Cisco MSX is installed and deployed into production.

To support this feature for all the service packs, you must have the ability to upload a NED package to NSO, and NSO must appropriately get restarted to take on that new NED.

Using this procedure, you can upload a new NED package using the Cisco MSX portal.

Before you begin

- Download the Network Element Driver (NED) from the URL. Use your Cisco credentials to log in.
- The downloaded NED package contains the following files:

```
README.signature
cisco_x509_verify_release.py
ncs-4.7.6-juniper-junos-4.5.13.signed.bin
```

```
ncs-4.7.6-juniper-junos-4.5.13.tar.gz
ncs-4.7.6-juniper-junos-4.5.13.tar.gz.signature
tailf.cer
```

Table 3: NED Package Files

Downloaded NED Package Files	Name of Each NED files
ncs-4.7.6-juniper-junos-4.5.13.tar.gz	Main NED file
ncs-4.7.6-juniper-junos-4.5.13.tar.gz.signature	Signature File
tailf.cer	Certificate File

Procedure

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

Step 2 From the left pane, choose **Settings > NED Management**.

The **NED Management** window is displayed with a table.

All the NEDs installed in different service packs are displayed in this table.

Step 3 Click **Add NED**.

The **Upload NED File** dialog box is displayed.

Step 4 Upload the downloaded NED package files in their respective fields:

- Upload NED Package
  - Choose file—Select the main NED file from the downloaded NED package and upload it.

    Note The same NED file cannot be uploaded more than once unless we delete the existing file.

- Verify NED Package—After the NED package is uploaded, a back-end process verifies the correctness of the file.
  - Choose file—Select the Signature file from the downloaded NED package and upload it.
  - Choose file—Select the Certificate file from the downloaded NED package and upload it.

  Note You will get a popup message stating whether the validation was successful or had any error.

- Install NED Package—After the NED package is verified, it gets installed to the NSO.
  - Service Pack—Select the Service Pack from the Service Pack drop-down list.

    Note NSO pods are restarted, and the new NED package becomes active.

Step 5 Click **Upload**.

The **Upload NED** confirmation dialog box is displayed for you to confirm the upload.

Step 6 Click **Upload** again.

Note Now the NSO POD restarts; during this time, the device operations are unavailable. So, do not navigate away from the window.

The **Validating and Installing NED file** popup is displayed. The installation process takes a few minutes to complete.

After a while, the popup message **Success** appears if the validation is successful, else the popup message **An Error Occurred** is dispayed if the validation is not successful.

Step 7 Click **Close**.

Now you can see the NED in the **NED Management** window.

Deleting a NED Package

You can delete an uploaded NED package at any time after the Cisco MSX is installed and deployed into production.

Using this procedure, you can delete a NED package using the Cisco MSX portal.

Before you begin

- Ensure to delete all the sites that are using the NED.
- On deleting NED, the device models that use NED namespace cannot be used in the service pack anymore.

Procedure

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

Step 2 From the left pane, choose **Settings > NED Management**.

The **NED Management** window is displayed with a table.

This table displays all the NEDs installed in different service packs.

Step 3 Select the NED, and click **ellipsis (…) > Delete**.

The **Delete NED** confirmation dialog box is displayed for you to confirm the delete.

Step 4 Click **Delete**.

Note Now the NSO POD restarts; during this time, the device operations are unavailable. So, do not navigate away from the page.

The **Deleting and Uninstalling NED file** dialog box is displayed. The deletion process takes a few minutes to complete. Then the popup message **Success** is displayed.

Step 5 Click **Close**.

Replacing a NED Package

Cisco MSX allows you to replace NED for device management. The replace option is used to upgrade or change an existing version of the NED package.

Using this procedure, you can replace a NED package using the Cisco MSX portal.

Procedure

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

Step 2 From the left pane, choose **Settings > NED Management**.

The **NED Management** window is displayed with a table.

This table displays all the NEDs that are currently installed in different service packs.

Step 3 Select the NED, and click **ellipsis (…) > Replace**.

The **Replace NED File** dialog box is displayed.

Step 4 Upload the downloaded NED package files in their respective fields:

- Upload New NED Package
  - Choose file—Select the main NED file from the downloaded NED package and upload it.
- Verify NED Package—After the NED package is uploaded, a back-end process verifies the correctness of the file.
  - Choose file—Select the Signature file from the downloaded NED package and upload it.
  - Choose file—Select the Certificate file from the downloaded NED package and upload it.

  Note You will get a pop-up message stating whether the validation was successful or had any error.
- Install NED Package—After the NED package is verified, it replaces the already installed NED.

  Note
  - The Service Pack is selected by default.
  - NSO pods are restarted, and the new NED package is replaced.

Step 5 Click **Replace**.

The **Replace NED** confirmation dialog box is displayed for you to confirm the replace.

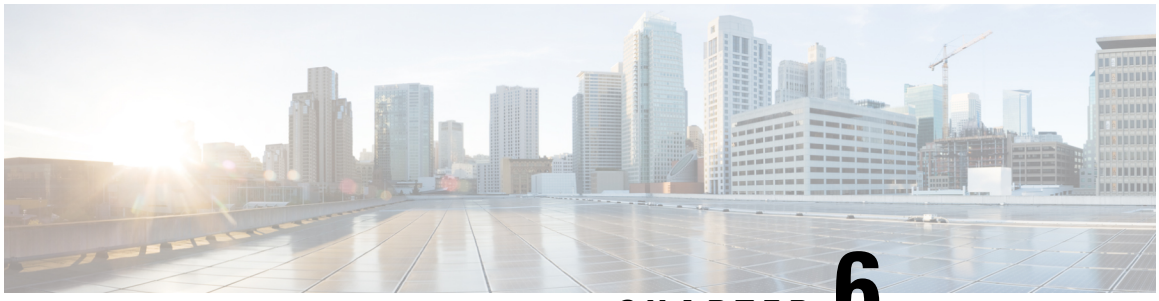
Step 6 Click **Replace** again.

Note Now the NSO POD restarts; during this time, the device operations are unavailable. So, do not navigate away from the page.

The **Validating and Replacing NED file** pop-up is displayed. The replacement process takes a few minutes to complete.

After a while, the pop-up message **Success** is displayed, if the validation is successful, else the pop-up message **An Error Occurred** is dispayed, if the validation is not successful.

Step 7 Click **Close**.



CHAPTER 6

Other Platform Capabilities

This chapter provides the Platform Capabilities for Cisco MSX.

This chapter contains the following sections:

Other Platform Capabilities

This section covers details on configuring change management approval workflow between Cisco MSX and ServiceNow. This section also includes information on integrating the ServiceNow ticketing system, managing device compliance vulnerability, and so on.

Integrating Incident Tracking System (ServiceNow) with Cisco MSX

The Cisco MSX platform provides **Incident Microservice** API that enables you to integrate an incident tracking system (ServiceNow) with Cisco MSX platform and extends to all the Cisco MSX tenants. Using this API, you can create, update, cancel, close, and delete an incident using the access token. While deploying Cisco MSX, incident system is also onboarded during the installation. The service providers should have a ServiceNow account to create and manage incident tickets.

The prerequisites to create tickets and change request is to configure an incident service after deploying the Cisco MSX. Using V8 configurations, multiple ServiceNow login accounts are mapped to tenants.

Sample API configurations

Create new incident

```
v1/incident
{
  "attributes": {
    "additionalProp1": {}
  },
  "category": "inquiry",
  "description": "string",
  "impact": "Low",
  "priority": "Planning",
  "severity": "Low",
  "state": "New",
  "subcategory": "string",
  "tenant": "3fa85f64-5717-4562-b3fc-2c963f66afa6",
  "urgency": "Low"
}
```

V8 Configuration

```
{
  "clientId": "b5c011a8db00301040ecb0b86b63b7b3",
  "clientSecret": "Cisco@123",
  "domain": "dev64108.service-now.com",
  "password": "Cisco@123",
  "userName": "admin",
  "criticalEvent": true,
  "tenantId": "70ef3a35-d23e-482e-a31d-0f568cc02ab3",
  "proxy":"http://proxy.esl.cisco.com:80"
}
```

Note The tenantId is optional. By default, tenantId global ServiceNow instance is mapped to a internal global tenantId.

The use cases of integrating ServiceNow with Cisco MSX are:

- Vulnerability: To monitor or detect device vulnerability in Cisco MSX.
- Software device compliance: To track the device software compliance in Cisco MSX.
- Cisco MSX creates tickets automatically when any critical event log occurs.

Incident services are capable of managing tickets that are created on service now. Users can directly create an incident on the ServiceNow and later use the incident ID to track services in the Cisco MSX. It is referred to as bidirectional flow for managing incident services, change requests, and approvals.

Use the **Incident Microservice** API for the following:

- Provide the authentication settings that helps to establish handshake with an incident tracking system, use the **Configuration Controller** section of the **Incident Microservice** API.
- Manage the incident, use the **Incident Controller** section of the **Incident Microservice** API.
- Manage the change request, use the **Change Requests Controller** section of the **Incident Microservice** API.
- Manage the approvals of the change request, use the **Change Requests Approvals Controller** section of the **Incident Microservice** API.
- Manage several tasks involved in the change request, use the **Change Requests Tasks Controller** section of the **Incident Microservice** API.

From the **Integrations, Settings, and Logs** category, assign the Incidents (View and Manage) permission to a user to run this API.

For more information on this API, refer to the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Incident Microservice API**.

Configuring Change Management Approvals

The Cisco MSX platform provides an approval process for the device configuration change requests made by a user. When the approval feature is enabled on Cisco MSX, change request for device configuration changes on Cisco MSX will be subjected to approval. If there is a change request on Cisco MSX, the request

is forwarded to ServiceNow through the Change Request service. The changes will take effect once the user approves the request through the ServiceNow portal.

Note Only tenants with a ServiceNow account can use this functionality. For more information on integrating ServiceNow, see Integrating ServiceNow with Cisco MSX.

Note In 4.2, the change management approval functionality is only implemented for the following device configuration operations.

- Applying Device Template for a device (by deviceId) - Implemented through UI and API
- Updating Device Template for a device (by deviceId)- Implemented through UI and API
- Remove Device Template for a device (by deviceId)- Implemented through UI and API
- Batch Attach Templates for multiple devices (for list of deviceIds)- Implemented only through API

  Using the Batch Attach Template operation, a user can submit change requests for a group of devices and process many devices in a single instance.

Enabling the ServiceNow Change Management Approval Functionality

When the approval feature is enabled, any change request for any action will go through the ServiceNow change management approval flow. When the user modifies configurations on Cisco MSX, it generates a change request with a "Pending Approval" status. The changes will take effect on Cisco MSX once the tenant approves the request through the ServiceNow portal. Use the steps below to enable the approval workflow between Cisco MSX and ServiceNow.

Cisco MSX Portal-Specific Configurations

ServiceNow administrator need to configure custom role and associate that role to a user using Cisco MSX Portal.

Procedure

Step 1 Create a custom role for approving the change requests from Cisco MSX. Only user role with **Change Request Approval** (Manage) permission under **Service Configuration and Devices** category section can approve a change request from Cisco MSX. For more information on creating a new role, see Adding a User Role.

Note If there is only one ServiceNow instance for all tenant, enable **All Tenant** (Manage) permission under **User, Role, and Tenants** category along with the Change Management Approval permission for the Approval functionality to be enabled on this instance for all tenants.

Step 2 Create a user and associate the approver role to this new user. For more information, see Adding a User.

Note If the Role has access to All Tenants, the Associate Tenant field will be disabled.

Step 3 Reset the password for created user.

Step 4 Create a custom API client for the ServiceNow application to access Cisco MSX APIs. To create a custom Cisco MSX API client, use the POST API (`/idm/api/v2/clientsecurity`) under the Security Client section for the usermanagement service.

For more information on this API, see the **Swagger** documentation, which is accessible from the **Cisco MSX portal > Account Settings > Swagger > IDM Microservice**.

```
"accessTokenValiditySeconds": 9000,

"authorities": [
  "ROLE_USER"
],
"autoApproveScopes": [
  "address", "email", "openid", "phone", "profile", "read", "write"
],
"clientId": " ServiceNow-api-client",
"clientSecret": "secret-value",
"grantTypes": [
  "password", "authorization_code"
],
"maxTokensPerUser": -1,
"refreshTokenValiditySeconds": 18000,
"registeredRedirectUris": [
          "https://dev73810.service-now.com/oauth_redirect.do"
],
"resourceIds": [

],
"scopes": [
  "address", "email", "openid", "phone", "profile", "read", "write"
],
"tenantRestrictions": [

],
"useSessionTimeout": false
```

In the above content for the custom Cisco MSX API client, make sure to specify the following details:

a. ClientID: This is the name of the new API client.

b. ClientSecret value: Provide an encrypted value for this attribute.

c. For the registeredRedirectUris, replace the URi with ServiceNowinstance DNS.

Step 5 Enter ServiceNow account Details.

a) Log in to the Cisco MSX portal.

b) From the left pane, choose **Tenant Workspace > Settings > ServiceNow Settings.**

The ServiceNow Settings page is displayed.

c) Enter the ServiceNow account details to be able to use ServiceNow for raising and tracking incident tickets.

Step 6 Enable Change Management functionality on Cisco MSX. To enable, do the following steps:

a) From the left pane, choose **Tenant Workspace > Settings > Compliane and Change Management.**

b) Under the **Change Management** section:

- Provide the Cisco MSX user group for the change approval. This is the same user group that was created on the ServiceNow portal for approving the requests coming in from Cisco MSX.

- To enable the change management approval workflow on Cisco MSX, check the **Enable Change Management** check box.

ServiceNow Portal-Specific Configurations

Register Cisco MSX as an OAuth Provider on ServiceNow and create a business rule for approval and rejection notification flow.

Note Only a user with an administrator role must perform these steps.

Procedure

Step 1 Create an application registry entry in ServiceNow. For more information, see the *ServiceNow documentation*.

Step 2 While adding a new entry, select **Configure to a third-party OAuth Provider** from the provided options.

Step 3 Provide the following details while creating the API Client Security:

a) **Name:** OAuth Provider Name. In this case, Cisco MSX will be the OAuth provider.
b) **Client ID and Client Secret:** This value must be the value that was provided while creating a custom API client on Cisco MSX. For more information, refer to that section.
c) **Authentication URL:** msxdns/idm/v2/authorize
d) **Token URL:** msxdns/idm/v2/token
e) **Token Revocation URL:** msxdns/idm/v2/logout
f) **Redirect URL:** servicenowdns/oauth_redirect.co
g) **Send Credentials:** As Basic Authorization Header
h) Set Encoded value of <*api-client:super-secret-value*> for Authorization: field in Cisco MSX API Token Rest Message on ServiceNow.
i) Create an OAuth Entity Profile by giving information such as a name, an OAuth Provider Grant type with read and write permissions.

Step 4 Add two system properties to store the username and the password of the CR Approver. For more information on adding a system property, see the *ServiceNow documentation*.

Note The Password should be of the type Password.

Step 5 Create a business rule for the Cisco MSX approval and rejection process. For more information, see Creating Business Rule for Approval and Rejection Notification from ServiceNow to MSX

Creating Business Rule for Approval and Rejection Notification from ServiceNow to Cisco MSX

Procedure

Step 1 Create two business rules for the approval and the rejection notifications. For detailed procedure on creating business rules, see the ServiceNow documentation.

Step 2 For the approval and rejection notifications to work on Cisco MSX, ensure that you update the following details when you create the business rules for approval and rejection.

- Check the **Active** and **Advanced** check boxes.
- Click the **When to run** tab and select the required options and Filter Conditions.
- Click the **Advanced** tab and add the approval or reject business rule script as given below:

Approval Business Rule Script

```
var msxAPIAccessToken;

function GetOAuthToken() {

 var oAuthClient = new sn_auth.GlideOAuthClient(),
    username = gs.getProperty('msx-cr-approver-user'),
    password = gs.getProperty('msx-cr-approver-password'),
    params = {
      grant_type: "password",
      username: username,
      password: password
    };

   var text = JSON.stringify(params),
     tokenResponse = oAuthClient.requestToken('MSX Provider', text),
     body = JSON.parse(tokenResponse.getBody()),
     token = tokenResponse.getToken();

 msxAPIAccessToken = token.getAccessToken();
}

function SendApproval() {

 GetOAuthToken();


 request = new sn_ws.RESTMessageV2();
 request.setHttpMethod("post");
 var msxUrl = gs.getProperty('msx.baseurl');



request.setEndpoint('https://aws-allsps.qa.ciscovms.com/changemanagement/api/v1/changerequests/'+current.number+'/approve');

 //TO Be replaced with MSX Change Request Approve
 request.setRequestHeader("Authorization", "Bearer "+ msxAPIAccessToken);

 // TODO:: form dynamic date and retry request
 var glideTime=new GlideDateTime();

 var formattedDate = glideTime.getDate().getDisplayValue() + "T" +
glideTime.getTime().getDisplayValue() + ".999999999Z";


  request.setRequestBody('{"details": "approved",  "modifiedBy": "serviceNowAdmin",
"modifiedOn": "'+ formattedDate +'"}');


 gs.addInfoMessage("Approving change request number " + current.number);

  gs.addInfoMessage("Approving request " + request.getRequestBody());
```

```
 var response = request.execute();
 var httpResponseStatus = response.getStatusCode();

 gs.info("Response status code is " + httpResponseStatus);
 if (httpResponseStatus == 201) {
  responseObj = response.getBody();
  var res = JSON.parse(responseObj);
 } else {
  //error

  var gr = new GlideRecord("problem");
  gr.initialize();
  gr.short_description=current.number + "::" + httpResponseStatus ;

  gr.insert();
 }


}

(function executeRule(current, previous /*null when async*/) {

 SendApproval();


})(current, previous);
```

Reject Business Rule Script

```
var msxAPIAccessToken;

function GetOAuthToken() {

 var oAuthClient = new sn_auth.GlideOAuthClient(),
    username = gs.getProperty('msx-cr-approver-user'),
    password = gs.getProperty('msx-cr-approver-password'),
    params = {
      grant_type: "password",
      username: username,
      password: password
    };

   var text = JSON.stringify(params),
     tokenResponse = oAuthClient.requestToken('MSX Provider', text),
     body = JSON.parse(tokenResponse.getBody()),
     token = tokenResponse.getToken();

 msxAPIAccessToken = token.getAccessToken();
}

function SendRejection() {

 GetOAuthToken();

 request = new sn_ws.RESTMessageV2();
 request.setHttpMethod("post");
 var msxUrl = gs.getProperty('msx.baseurl');

 request.setEndpoint(msxUrl +
'/changemanagement/api/v1/changerequests/'+current.number+'/reject');

 request.setRequestHeader("Authorization", "Bearer "+ msxAPIAccessToken);

 var glideTime=new GlideDateTime();
 var formattedDate = glideTime.getDate().getDisplayValue() + "T" +
```

```
glideTime.getTime().getDisplayValue() + glideTime.getTZOffset() + "Z";

 request.setRequestBody('{"details": "rejecting",  "modifiedBy": "serviceNowAdmin",
"modifiedOn": '+ formattedDate +'}');

 var response = request.execute();
 var httpResponseStatus = response.getStatusCode();

 gs.info("Response status code is " + httpResponseStatus);
 if (httpResponseStatus == 201) {
  responseObj = response.getBody();
  var res = JSON.parse(responseObj);

 } else {
  //error
  gs.log(response.getErrorCode() + "---" + response.getErrorMessage());
 }


}

(function executeRule(current, previous /*null when async*/) {

 SendRejection();


})(current, previous);
```

Managing Change Request

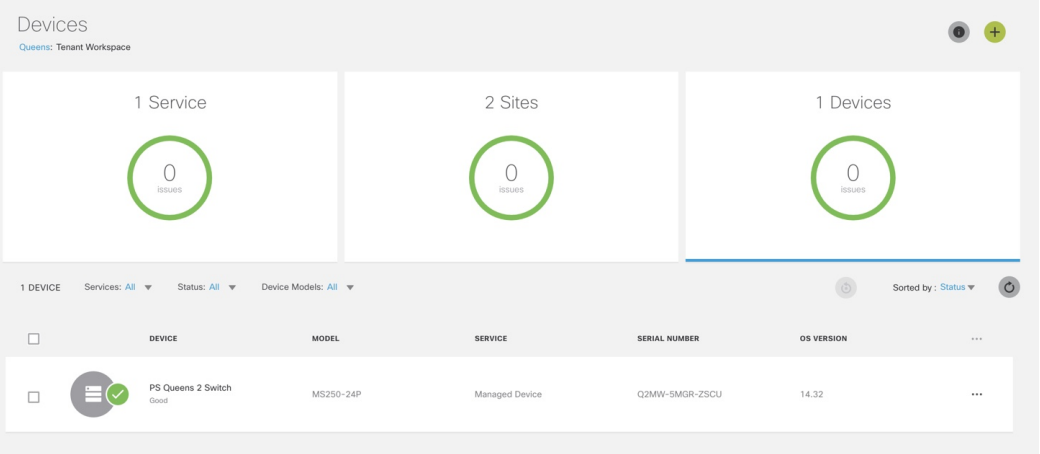
The following steps describe the approval flow between Cisco MSX and ServiceNow for a device configuration change request:

Procedure

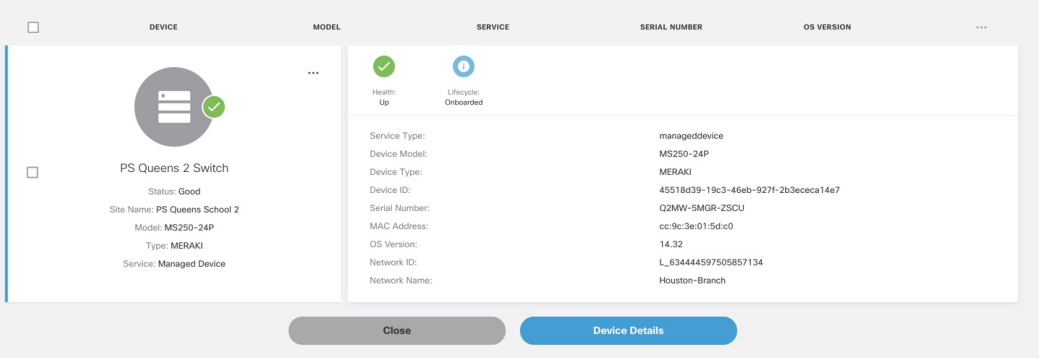
Step 1 Log in to the Cisco MSX portal.

Step 2 From the left pane, choose **Tenant Workspace > Select a Tenant > Devices**.

The **Devices** tile is displayed with the list of devices.



Step 3 Click **Device Details** to display the **Devices** page.



Step 4 On the Devices page, scroll down to the **Device Template Details** section and perform one of the device configuration action such as **Apply, Update, or Remove Device Template** to initiate a change request approval flow.

Note The change request will be processed in the order in which it was created.

Step 5 Click on the blue *Pending Approval* link from the device template list to display the **Change Request Details** dialog box. For pending request, all the fields are disabled until the request is approved, and the user will not be able to make any further changes.

Alternatively, you can hover over the hourglass icon on device template to view the details in the **Change Request Details** dialogue box.

Note Cisco MSX uses out-of-the-box templates to generate these device configuration change requests details. You can use custom templates to change the format of the content displayed on the details page.

Step 6 Click the **Change Request ID** in the **Change Request Details** dialogue box to view the the pending change requests in the **Tenant Workspace > Service Control > Change Requests**.

Step 7 Approve/Reject the change request from the ServiceNow application.

a. Ensure the change request is available on the ServiceNow web interface.

The change request from Cisco MSX is automatically created on ServiceNow when a configuration change is received from Cisco MSX. You can view the open change request on the ServiceNow service management web interface. For more information on how to view open change request, refer to the *ServiceNow documentation*.

b. Request for Approval on the ServiceNow. For more information on how to request for an approval, refer to the ServiceNow documentation.

Note Only a user from Cisco MSX approval group can approve or reject a change request. After the user from the Cisco MSX group approves the request, the request is sent to another group, the Change Advisory Board (CAB) approval group, for the final approval.

Note The state of the approved request changes to Scheduled state in the ServiceNow.

Step 8 To view the status of the change request on Cisco MSX, choose **Tenant Workspace > Service Controls > Change Requests**. You can use filter the change request by status and click on **Details** for detailed information about the change request. The following table lists the color codes used for tracking the change request status:

Status	Colour Code
Pending Approval / Queued for Processing	Purple
Approved / Applied	Green
Rejected / Detached / Apply Failed / Detach Failed	Red
Applying / Detaching	Blue

Managing Billing

The Cisco MSX platform has the ability to identify, track, and report the various subscription billing activities that happen across the Cisco MSX system using **Billing Services** API. Using **Billing Services** API, inventory reports can also be generated. You can manage the billing for several items such as devices, sites, control plane, general purpose events and services.

Note By default, the only Service Pack that has currently implemented a price/cost model using the Billing Service is SD WAN. Other Service Packs may implement this functionality in the future.

The **Billing Service** API also provides event-based billing capabilities for the tenants. The events that are registered from the service pack are determined as billable and monetary values are assigned by operators for different service pack-based events in the Cisco MSX. The event generation and billing calculation are scheduled as per the pre-configured interval (either monthly or yearly).

You can manage the billing cycle and price definition for services using the **Billing Services** API. For more information on these API, refer to the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Billing Services API**

- To filter the billing events by services and to define a prorated price, use **Billing Events** (Billing Event Controller) section of the **Billing Services** API.

- To manage the pricing definition for the service pack, use **Billing Prices** (Billing Price Controller) section of the **Billing Services** API. For example, to define a price definition for a service, use POST /api/v8/prices API.

```
{
"name": "Device Price"
"description": "Pricing Details for Device Types",
"type": "Device"
"subtype": "Cisco CSR 1000V"
"source": "customer_name"
"service": "sdbranch"
"billing period": "-1/daily/monthly/yearly/minute" millis
"price": 250.0
"tenantID": "tenant id value"
}
```

  Where:

  1. Set the billing period attribute to:
     a. -1, to set a non-recurring/single billing instance.
     b. Monthly/yearly/minute values in milliseconds. For example, for monthly the value is 2629800000 milliseconds.
  2. Set the service value as the name of the Service Pack for which the price definition must be applied.

- To manage a billing cycle, use the **Billing Cycle** (Billing Cycle Controller) section of the **Billing Services** API.

From the **Billing/Metering** category, assign the following permissions to a user to run this API.

- Event (View)
- Price (View and Manage)

Using this procedure, you can view the various billing activities across Cisco MSX system. To manage these billing activities, use the APIs described above.

Procedure

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

Step 2 From the left pane, choose **Tenant Workspace > Billing**.

The **Billing** window is displayed.

Step 3 Select a tenant.

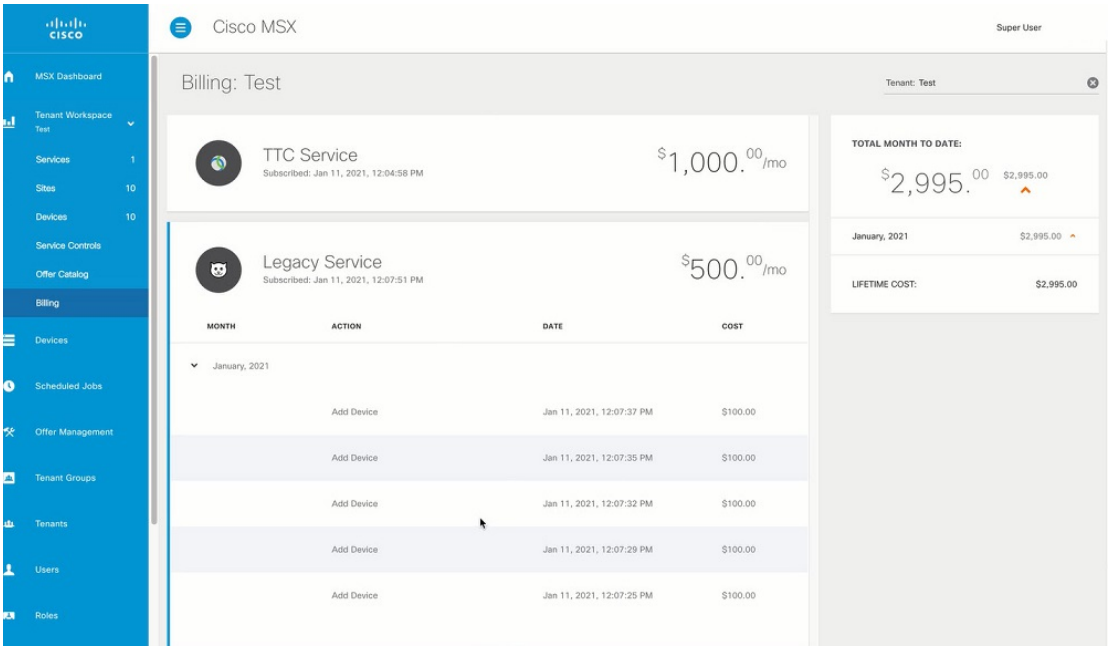
Note Assign a service pack offer, if the tenant had not subscribed to any of the offers. For more information, see Subscribing the Service Pack Offer from Tenant Workspace.

Step 4 View the billing summary of the assigned service pack offers.

a) Select a service pack offer to get the expanded view of the offer price and other billing events (such as create site and add device) summary for each month.

The total billing amount of all the subscribed service offers for each month are displayed on the right pane.

Figure 12: Billing Window



Managing Device Compliance Vulnerability Using API

The Cisco MSX platform now detects and reports the software compliance vulnerabilities for both the Cisco devices and third-party software devices using the **Vulnerability Service** API.

Note The Cisco Product Security Incident Response Team (PSIRT) manages the investigation and public reporting of security vulnerability information of the Cisco products and networks.

To register a product for vulnerability inspection, use the POST API in the **Registration** section of the **Vulnerability Service** API.

For more information on this API, see the Swagger documentation that can be accessed from **Cisco MSX portal > Account Settings > Swagger > Vulnerability Service API**.

Note Only users with the following permissions from the **Integrations, Settings, and Logs** category will be able to run this API:

- Vulnerability (View permission)
- Vulnerability (Manage permission)

The Cisco Vulnerability Service ingests vulnerability data feed (available in the JSON format) from National Vulnerability Database (NVD) or Common Vulnerabilities and Exposures (CVE) to the Cisco MSX. The Vulnerability Service monitors the existing Cisco MSX device inventory table on a scheduled basis.

When a device is monitored for vulnerabilities, a registration is created in vulnerability service automatically, and the service will watch for vulnerabilities for those devices, publishing messages with vulnerability details that the platform uses to update the vulnerability state of devices.

You can add a device and enable compliance monitoring capability to ensures that the device that is configured to a set of standards remains in that state until it is changed. For more information about adding a device and configuring the compliance for devices, see the "Device Compliance" section in the Cisco Managed Services Accelerator (MSX) 4.2 Managed Device Service Pack Documentation.

To monitor the device vulnerablity status, click **Tenant Workspace > Devices**. The Vulnerablity section displays the list of all the vulnerability information of the selected device. For more information, see the "Viewing Device Vulnerabilities" section in the Cisco Managed Services Accelerator (MSX) 4.2 Managed Device Service Pack Documentation.

The Cisco MSX platform sends an email notification to all the tenants regarding the captured vulnerability information of the registered devices. The tenant's email addresses are stored and vulnerabilities are tracked as events in the **Notification** window. Update the notification services to handle the tenant-based emails. For more information, see Enabling Notifications for Events.

The Cisco MSX fetches the email address of the tenant that is available as a part of the payload and builds an email. This email will contain the list of discovered vulnerabilities of the devices with URL and severity level of the devices is also mentioned for the users to know the status of the devices.

To enable the Vulnerability Service to monitor the device vulnerability, onboard and publish the Vulnerability Service component on the Cisco MSX platform to detect and report the existing software compliance vulnerability. For more information about onboarding new services, see Onboarding and Deploying Component into Cisco MSX.

Validating the Smart Account License Using API

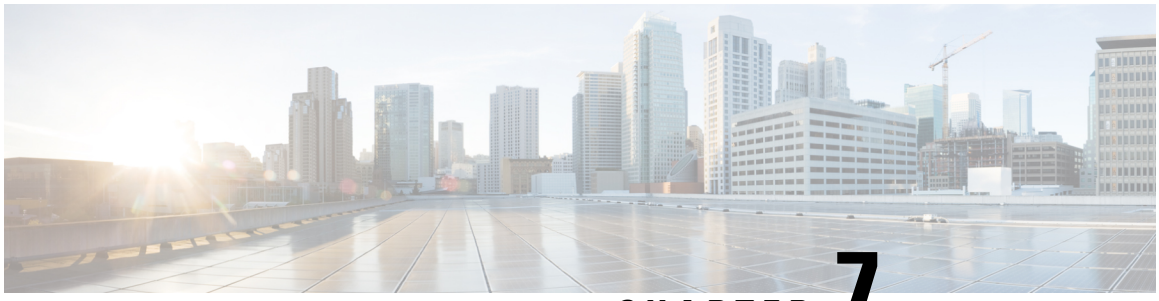
The tenants can log into Cisco MSX using the Cisco.com SSO credentials and select a service offer for a subscription. The Cisco MSX platform provides **Licensing Service** API to validate the list of smart accounts, virtual accounts, and licenses associated with the Cisco.com user's account. Only based on the authentication the users are allowed to proceed with the offer subscription process.

You can manage the configurations of the **Licensing Service** API as follows:

- To manage the service configuration required for licensing and smart account, use the **Configuration Controller** section of the **Licensing Service** API.
- To fetch the smart account list or virtual account list, use the **Account Controller** section of the **Licensing Service** API.
- To fetch the smart account list, use the **Licenses Controller** section of the **Licensing Service** API.

From the **Service, Configurations, and Devices** category, assign the **Licensing** (View and Manage) permission to a user to run this API.

For more information on these APIs, refer to the Swagger documentation that can be accessed for **Cisco MSX portal > Account Settings > Swagger > Licensing Service API**.



CHAPTER 7

Automate Processes Using Workflows

Cisco MSX interacts with Cisco Action Orchestrator (AO) to import and operate on the workflows from within Cisco MSX. This feature is enabled by default.

A workflow consists of activities, invocations of child workflows, and logic components that can be included to automate processes.

The workflow actions can be performed from both the Cisco MSX Portal or by using APIs (Workflow, Workflow Instance, and Category APIs). For more information on APIs related to Action Orchestrator/Workflow engine, refer to the Swagger documentation that can be accessed from the **Cisco MSX portal > Account Settings > Swagger > Manage Microservice API**.

For more information on AO-specific permissions, see the latest version of *Cisco MSX Platform and Service Pack Permissions Addendum*.

This chapter contains the following topics:

Importing a Workflow

Using this procedure, you can import workflows for associated tenants from Service Design Studio (SDS) and view the workflows.

Procedure

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

Step 2 From the left pane, click **Workflows**.

The **Workflow** window is displayed.

Step 3 Click **Import New Workflow** to import a workflow into Cisco MSX.

It is possible to upload a new version of the same workflow. In this case, you will have the option to cancel or overwrite the existing one.

Step 4 Select the Associate Tenants, click **Import Workflow**, and click **OK**.

After uploading a workflow into Cisco MSX, Cisco MSX lists the imported workflow on the Workflows page. Click on a workflow to view its details.

Running a Workflow

Using this procedure, you can run a workflow, view, and delete a workflow instance details.

Procedure

Step 1 Log in to the Cisco MSX portal.

Step 2 From the left pane, click **Workflows**.

The **Workflows** window is displayed.

Step 3 Select a workflow and click the **Details** icon.

Step 4 Enter workflow execution startup parameters, for example, a service name.

Step 5 Click **Run** to run the workflow.

If the workflow runs without any issues, status changes to green for all three checks. If there are issues, select the workflow running instance from the **Runs window** on the right-hand side, click ellipsis (...) and select **View Result** to view the error.

To delete or cancel a running workflow instance, click ellipsis (...) and select **Delete** or **Cancel**.

Deleting a Workflow

Using this procedure, you can delete a workflow.

Procedure

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

Step 2 From the left pane, click **Workflows**.

The **Workflow** window is displayed.

Step 3 Select a workflow and click **Delete** icon to delete the imported workflow.

Creating Account Keys

Account keys are the credentials for the system to be able to authenticate and access the workflows that you are trying to target.

Using this procedure, you can create account keys.

Procedure

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

Step 2 From the left pane, click **Workflows**.

The **Workflows** window is displayed.

Step 3 Click **Account Keys**, and then click **Create Account Key**.

Create Account Key dialog box is displayed.

- Select the Account Key Type from the drop-down list.
- Enter the Display Name and Credentials.

Step 4 Click **Save**.

The new account key is listed on the Workflows > Account keys window.

- To edit an account key, select the Account key and click the ellipses button (the button with three dots).
- Click the **Edit Account Key** to edit the selected account key.

  Note If there are secure strings, not modifying them and leaving them as asterisks maintain the previous value.

  The **Edit Account Key** dialog box is displayed. Make the required changes and click **Save** to save the updates.

- To delete an account key, select the account key to be deleted and click the **Delete Account Key** button.

  The **Delete Account Key** dialog box is displayed. Click **Delete** to confirm.

Creating Targets

Targets are used by workflows either at the start of the workflow, or, internally during the workflow.

Using this procedure, you can create targets so that the workflow can select any target in runtime.

Note Having account keys is a prerequisite for most targets. If required, you should have the account keys created first before you create the targets.

Procedure

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

Step 2 From the left pane, click **Workflows**.

The **Workflows** window is displayed.

Step 3 Click **Targets**, and then click **Create Target**.

Create Target dialog box is displayed.

- Select the Target Type from the drop-down list.
- Enter the Display Name.
- Select the Account Keys from the drop-down list if an option is provided.
- Select the Protocol, Host/IP Address and Port.

Step 4 Click **Save**.

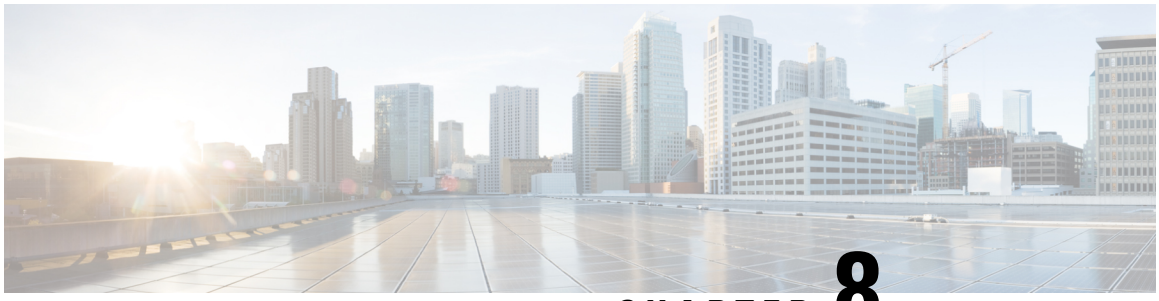
The new target is listed on the **Workflows > Targets** window.

- To edit a target, select the Target and click the **ellipses (...)**.
- Click the **Edit Target** button to edit the selected target.

  The **Edit Target** dialog box is displayed. Make the required changes and click **Save** to save the updates.
- To delete a target, select the target to be deleted and click the **Delete Target** button.

  The **DeleteTarget** dialog box is displayed.

  Click **Delete** to confirm.



CHAPTER 8

Portal Customizations

Cisco MSX provides GUI customizations that allow the Service Provides to alter the portal appearance and the portal experience. Using these GUI customizations, you can customize various aspects of the portal, such as themes, colors, banners, and so on and apply these to the entire portal or on the specific pages of the portal.

This chapter describes the following GUI customizations available with Cisco MSX:

Customizing Portal Themes

Theme Builder enables a customer or a tenant to customize the existing skins and apply new skins on Cisco MSX that matches their brand guidelines as closely as possible.

Before you begin

Only users with the UI_Themes permission can create a theme.

For more information on all the available permissions in Cisco MSX and to also see the minimum required permissions to perform various operations in Cisco MSX, see the latest version of Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum.

Creating a Theme

Using this procedure, you can create a theme.

Procedure

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

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

The **Settings** window is displayed.

Step 3 Select the **UI Theme Builder** tile from the **Settings** window.

The **UI Theme Builder** window is displayed.

Step 4 Click the **Create New Theme** tab and enter the name for your Theme Project.

Step 5 Upload your brand assets under **Upload your Assets** (Brand logo, Login logo, and Brand font).

Note Click the **Show Preview** button to see in the page layout on the right pane.

Step 6 Click **Continue**.

Step 7 Assign your core colors (primary, secondary and tertiary) through the automatic color assignment process. You can set the palette by adding the HEX values.

Step 8 Click auto-assign colors to automatically assign the primary, secondary and tertiary colors to the Cisco MSX skin.

Step 9 After you are done with the theme changes, do one of the following:

a) Click **Save Theme** to save your changes.

b) Click **Publish Theme** to publish the theme.

Editing a Theme

You can use the **Edit a Theme** option to edit a theme.

Using this procedure, you can edit a theme.

Procedure

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

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

The **Settings** window is displayed.

Step 3 Select the **UI Theme Builder** tile from the **Settings** window.

The **UI Theme Builder** window is displayed.

Step 4 Click the **Edit a Theme**.

Step 5 Select the theme that you want to edit from the **Saved Theme** tab.

Note Modify the theme to match it with your brand guidelines.

Step 6 From the **Assign your Colors and Settings** section, select the core colors from the drop-down list you want to modify.

You can use the color and settings inputs to customize the theme further.

Step 7 Click undo icon to undo individual input changes, in other words, to revert a color or other choice to the previous setting.

Step 8 Click **Save Theme** to save the changes. You can also republish a theme after editing the theme.

Managing a Theme

You can use the Manage Theme option to import, export, or delete an existing theme asset. These assets are stored as JSON files created by Theme Builder when assets are exported.

Using this procedure, you can manage created theme assets.

Procedure

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

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

The **Settings** window is displayed.

Step 3 Select the **UI Theme Builder** tile from the **Settings** window.

The **UI Theme Builder** window is displayed.

Step 4 Click **Manage Themes**.

You have two options:

- **Manage Theme Packages**: Theme Packages are JSON files that contain all of the assets associated with a given theme.
- **Manage Individual Theme Assets**: Theme assets are individual data files that are in JSON format.

Step 5 From the Manage Theme Packages, click **Import Theme Package file** under **Import Data** and choose the file to import or publish.

Step 6 Click **Select a Theme** tab to view the published themes.

Step 7 Hover over the newly imported theme, and click the republish icon to republish the theme, or to see when the theme was last republished.

Note If you have permission to edit the theme, you will also have the permission to republish the theme.

You can do the following from the Manage Individual Theme Assets:

- **Import Theme file**: Using this option, you can import the theme file.
- **Import Logo file**: Using this option, you can import the logo file.
- **Import Font Set file**: Using this option, you can import the font set file.
- **Import Published Theme file**: Using this option, you can import the published theme file.

Previewing a Theme

Only users with the ‘UI Themes’ permission set to ‘View’ or ‘Manage’ can **Preview a Theme**. This permission is available under ‘Integrations, Settings, and Logs'.

Using this procedure, you can preview a created theme.

Procedure

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

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

The **Settings** window is displayed.

Step 3 Select the **UI Theme Builder** tile from the **Settings** window.

The **UI Theme Builder** window is displayed.

Step 4 Select the theme you want to set from **Select a Theme** tab.

The tiles for the published themes are displayed.

Step 5 Hover over a tile to preview the theme in the preview pane.

Step 6 Click a tile to preview a theme in Cisco MSX.

Note Users with the Manage option can click **Set Active** to make the chosen theme the default skin for Cisco MSX for all the users.

If the republishing is blocked, an error message appears with the missing theme data.

If you get a warning that there is more than one theme out-of-date, click **Republish Out-of-Date Themes** to republish all the out-of-date themes.

Customizing the Footer

The Cisco MSX portal allows you to edit the Cisco MSX footer in one place so that you do not have to find footer elements in different pages.

You can also update all the contact phone numbers here. The footer tile allows you to update all the contact information in the footer.

The footer elements include:

- Support Links
- Technical Support

Using this procedure, you can edit the Cisco MSX footer.

Procedure

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

Step 2 From the left pane, choose **Settings** > **Footer**.

The **Footer** window is displayed.

Step 3 Edit the **Support Links**, if required.

Step 4 Click **Save**.

Viewing the Cisco MSX Component Versions

The Cisco MSX component versions allows you to view all Cisco MSX microservices information and service UI information.

Using this procedure, you can view the Cisco MSX component version.

Procedure

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

Step 2 From the left pane, choose **Settings > Component Versions**.

The **Component Versions** window is displayed.

You can view the following component versions:

- Microservice Information—This includes:
  - Component Name
  - Version
  - Build Number
  - Build Date
- Service UI Information—This includes:
  - Service UI
  - Version
  - Build Number
  - Build Date
  - Language Support

Updating Languages

The Cisco MSX portal allows you to update or add languages to a running Cisco MSX instance.

An authorized user can download a JSON formatted file of all the current language keys/values used in the UI. This file can be sent to a translation center to update the values for a specific language. When the user gets it back from their translation center, they can then upload the new file after selecting what language the

translations are for in the drop-down list. Any language added into them in this way will become a valid language a user can be configured to use as default.

Using this procedure, you can update or add languages.

Procedure

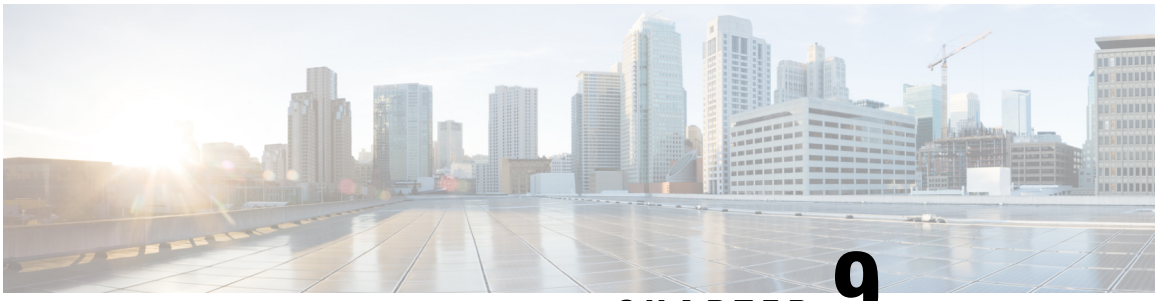
Step 1 Log in to the Cisco MSX portal using your credentials.

Step 2 From the left pane, choose **Settings > Language**.

The **Language** window is displayed.

Step 3 Select your language's **Enabled** check box, and click **Save**.

Note You can also change the Cisco MSX portal's default language from the user profile icon.



CHAPTER 9

Service Monitoring

This chapter contains the following sections:

Monitoring Cisco MSX Service Status in Cisco MSX GUI

The Cisco MSX GUI has:

- The **Operator Workspace** is only visible to operator users. It lists all tenants that the operator is managing and the services they have subscribed to.

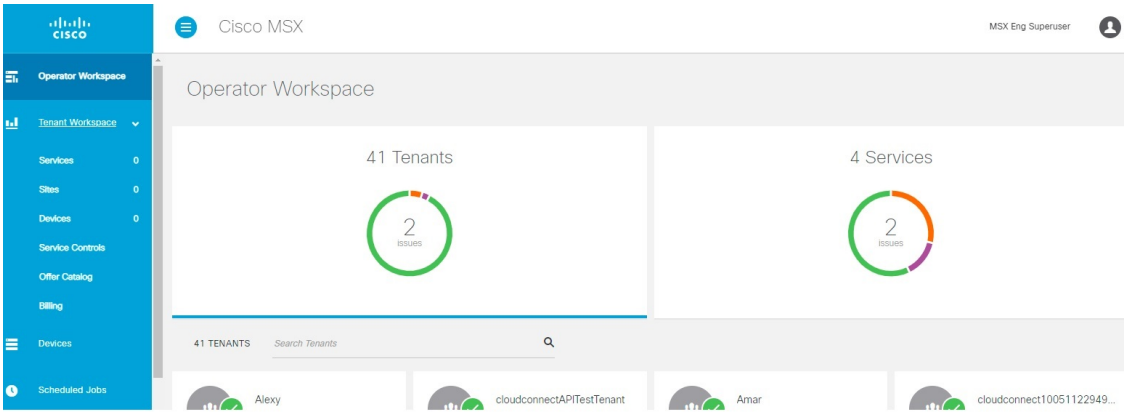
  Click on a tenant's tile to see details specific to a tenant in the Tenant Workspace GUI.

- The **Tenant Workspace**, which allows tenants to access the information related to their subscribed services.

Note Only users with operators permission can view the Operator Workspace.

The figure below shows the Operator Workspace:

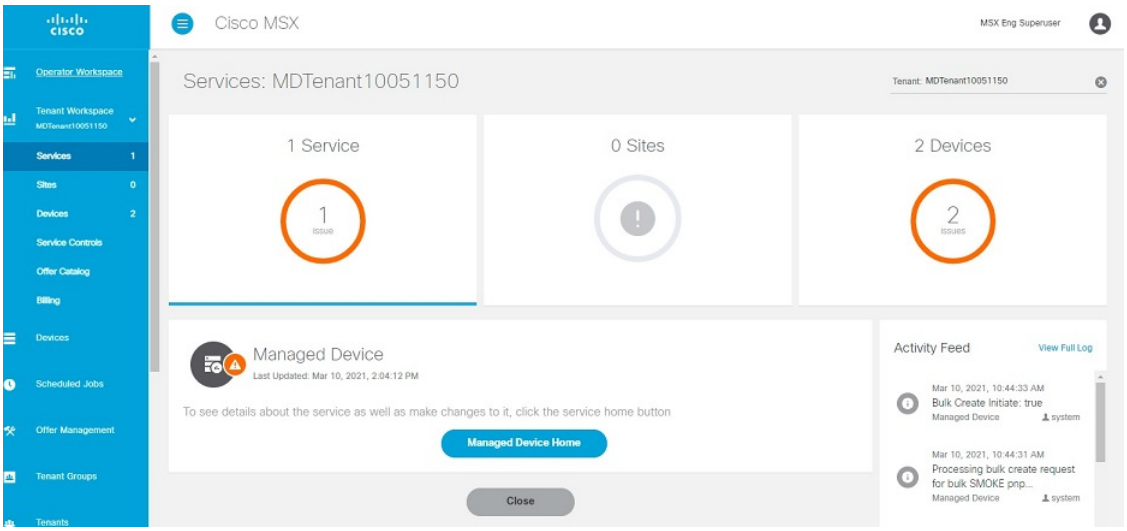
Figure 13: Operator Workspace



Note Only a user with the permissions to manage this Tenant can access the Tenant's Workspace.

The figure below shows the Tenant Workspace:

Figure 14: Tenant Workspace



Viewing Tenant Workspace

A Tenant Workspace allows tenants to access the information related to their subscribed services.

Menu Name	Displays
Services	Display all services subscribed by a tenant, service status, and other service metrics.

Menu Name	Displays
Sites	Display an overview of the tenant's sites, site status, and allows access to site details. **Note** Displays only the sites that have latitude and longitude.
Devices	Display an overview of the tenant's devices, device status, and allows access to device details. **Note** Displays both mapped or unmapped sites or devices.
Service Controls	Display the custom service controls that are used to manage the services.
Offer Catalog	Display existing subscriptions and allows subscribing to new services.
Billing	Display billing information about the tenant's subscriptions.
Settings	Configure service-level settings.

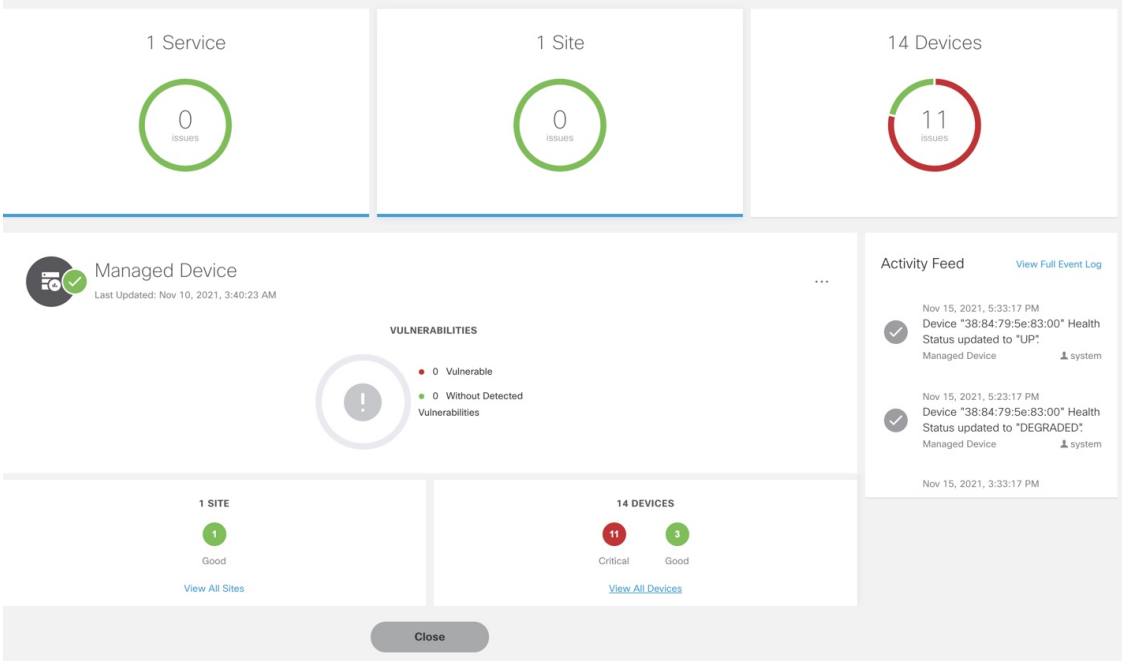
Monitoring Cisco MSX Service Status

The overall service status updates are based on the Lifecycle and Health statuses of the devices and several service-specific characteristics applicable to that service subscribed by a tenant.

The table below describes the Service statuses that are displayed on the Cisco MSX Portal:

Service Overall Status Indication	Service Status	Severity Number
Red	Critical	7
Orange	Poor	6
	Fair	5
Green	Good	1
Grey	Unknown	3

The figure below displays the aggregated service status:



Using this procedure, you can view the service status.

Procedure

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

Step 2 From the left pane, choose **Tenant Workspace > Services**.

Step 3 To view the overall status of a service, click to expand a particular service panel. The service and the overall status of the sites using the services are displayed. Also, the list of devices being used for the selected service is displayed.

Monitoring Cisco MSX Site Status

The Cisco MSX platform provides the overall site status updates based on the health status of the devices attached to the site. The site status are categorized as critical, poor, fair, good, and unknown. The device health status are categorized as Up, Down, and Unknown.

The status of devices in the Cisco MSX system are updated periodically. The health updates are triggered by monitor microservice. The device beat constantly pings the device and the monitor microservice queries the data produced by the beat to update the health status.

The table below describes the site status calculation:

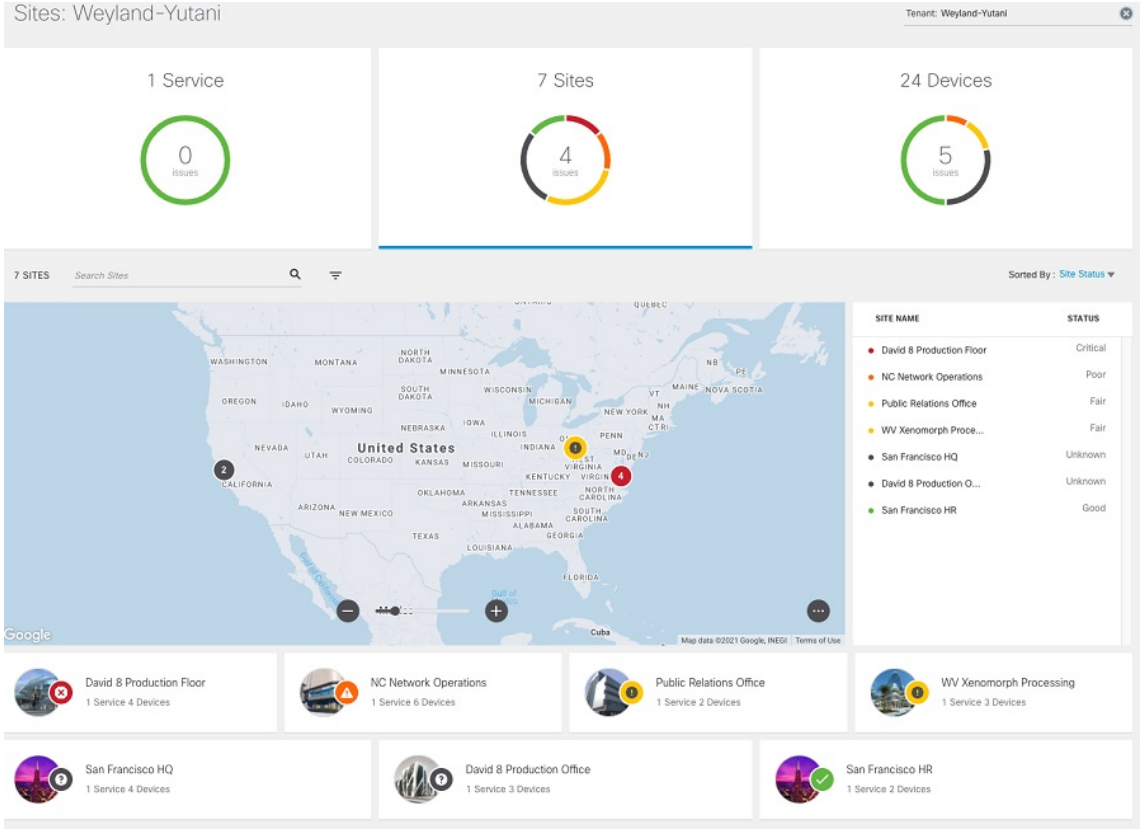
Table 4: Calculating the Site Status

Device Condition	Severity Number	Site Status	Site Overall Status Icon
No device.	1	Good	Green

Device Condition	Severity Number	Site Status	Site Overall Status Icon
All devices are Up.	1	Good	Green
All devices are down.	7	Critical	Red
All devices are unknown.	3	Unknown	Gray
Devices with different health status.	Values correspond to the device with the highest severity number.		

The figure below displays the status of the individual site and aggregated sites:

Figure 15: Site Status



Using this procedure, you can view the site status.

Procedure

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

Step 2 From the left pane, choose **Tenant Workspace** > **Sites**.

The **Sites Overview** window is displayed.

Step 3 To view the status of one site, hover the mouse pointer over the **Site** icon on the map view. The site name and its corresponding status are displayed.

Step 4 Click the **Site** icon to land on the **Site Overview** window. Alternatively, you can use the list view or the tile view to access **Site Overview** window. The list view of the sites appear on the right pane and its corresponding site status are also indicated.

Hover the mouse pointer on the Sites to know the aggregate site status data.

Monitoring Cisco MSX Device Status

The **Devices** menu option in the **Tenant Workspace** provides the devices' overall state. The **Devices** menu displays both mapped (latitude and longitude defined) or unmapped devices.

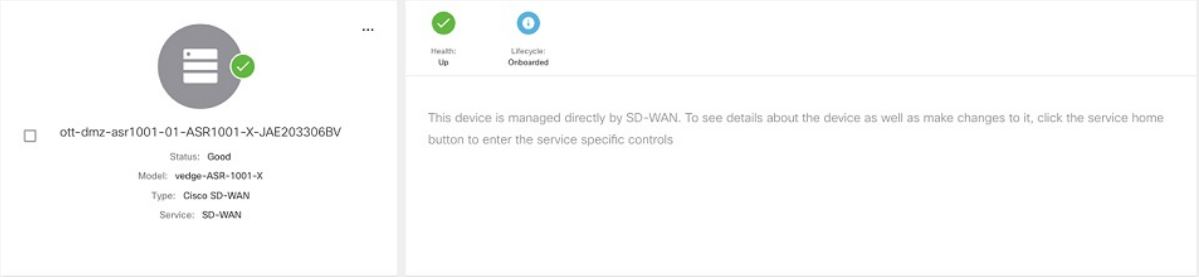
The overall device state is calculated based on various status, such as device lifecycle status, device health status, tunnel status, pnp status, sync status.

Within Cisco MSX, the state of the device is numbered from 1 to 7, with the highest number 7 indicating the state as '**Critical**' and the lowest number 1 indicating the state as 'Good'. An overall state looks into the available statuses (lifecycle or device health or other status) for a device and picks the highest number and maps it to the below overall states.

Overall States vs Severity Number in Cisco MSX

Overall Status	Critical	Poor	Fair	Unknown	Good
Severity Number	7	6	5	3	1

The following figure illustrates overall device state, device health, and lifecycle status for an SD-WAN device.



Using this procedure, you can view the device status.

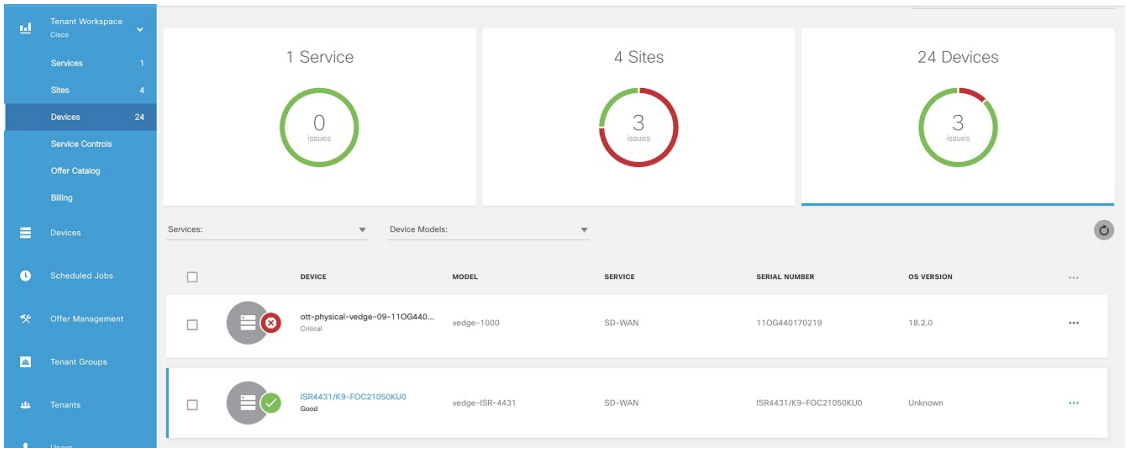
Procedure

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

Step 2 From the left hand pane, choose **Tenant Workspace** > **Devices**.

The **Devices Overview** window is displayed with overall status of the devices.

Figure 16: Device Overview window



Step 3 To view the status of a device, hover the mouse over the device and click to view the device summary.

The device view expands and its overall status is displayed.

Step 4 Click **Device Details** to view additional details of the device.

Viewing an Event Log

Using this procedure, you can view an event log.

Procedure

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

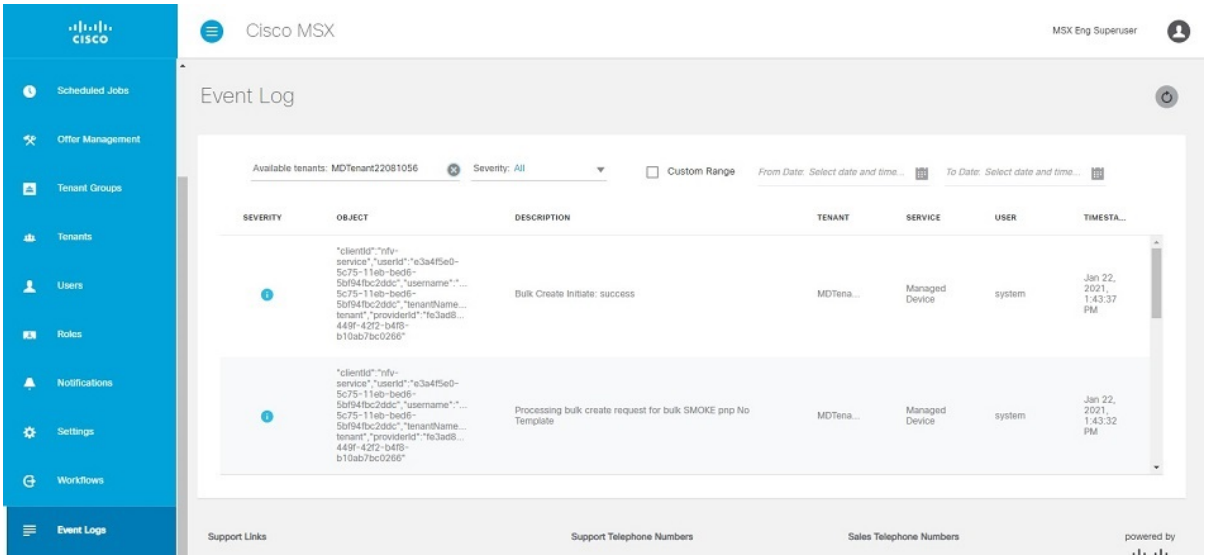
Step 2 From the left pane, click **Event Log**.

The **Event Log** window is displayed.

Step 3 From the Event Log screen, filter the event log records. Select the available tenant from the drop-down. You can filter these events by severity and time frame. To list event logs for a specific duration, select the Custom Range and specify the dates.

The figure below displays the Event Logs window:

Figure 17: Event Logs



Page-Level Actions

The following table lists the page-level actions available for various services in Cisco MSX:

Table 5:

Cisco MSX Services	Page-Level Actions Available with Documentation Links
Managed Device	• Add Device
Enterprise Access	Add New Controller
SD-WAN	Add Site

Monitoring Service Panel

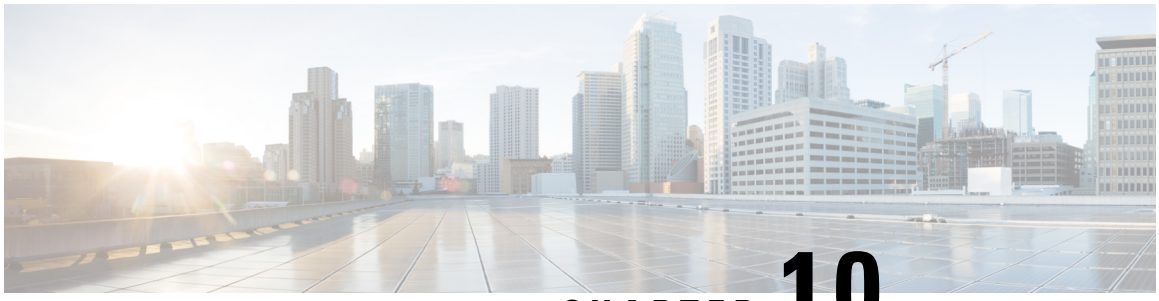
The **Service Panel** in the **Tenant Workspace** allows tenants to see the next steps that they can perform for their subscribed services. After the services are set up and the network has connectivity, the panel also shows the services-related metrics.

Service-Specific Actions

Tenants can perform additional operations for the subscribed services from the service panel using the ellipsis (...) and the (+) options. Use the table below to know more about the service-specific actions:

Table 6: Service-Specific Actions

Cisco MSX Services	Service-Level Actions Available with Documentation Links
Managed Device	• Add Device • Add Site • Import Device Using CSV • Unsubscribe • Manage Compliance
Enterprise Access	• Add New Controller • Setup New Controller • Controller Setup Monitor • Delete Subscription
SD-WAN	• Meraki SD-WAN Home • Control Plane Portal • Edit Control Plane • Control Plane Details • Bulk Import • Traffic Policy • Detach Control Plane • Unsubscribe • Add Device



CHAPTER 10

Troubleshooting Platform Issues

To troubleshoot an issue, define the specific symptoms, identify all potential problems that could be causing the symptoms, and then systematically eliminate each potential problem (from most likely to least likely) until the symptoms disappear.

The following steps provide guidelines to use in the problem-solving process.

1. Analyze the problem and create a clear problem statement. Define symptoms and potential causes.
2. Gather the facts that you need to help isolate possible causes.
3. Consider possible causes based on the facts that you gathered.

This section describes problems, possible causes, recommended actions, and error messages, if applicable to the problem.

Order Fails During Provisioning

Problem

When you place an order and the order goes into provisioning but fails during provisioning. Cisco MSX service interface indicates that the order provisioning has failed.

Solution

1. Review the tenant event logs web interface to confirm the error occurred during provisioning and not initial validation.
2. The tenant user needs to escalate this issue to the service provider operator.

Note The system will not self-recover even if the unplugged devices are plugged back in.

3. The service provider operator has to login to NSO directly and fix the problem.
   - Ensure that the malfunctioning devices are taken offline.
   - Retry the provisioning operation.

When the NSO provisioning operation completes successfully, it sends the correct notification to the northbound interface, and resets the Cisco MSX service interface to the provisioned state.

Order Failed Error Message

Problem

When you place an order and get an order failed message right away (due to first-level call to NSO failing), it means that the order has failed.

Solution

1. Review the tenant Event logs and confirm the error is caused due to first-level call to NSO failing.
2. Deletes the order from the Cisco MSX service interface.
3. Place a new order.

Service Ordering Fails

Problem

When you try to order a service, the service ordering fails.

Solution

- Verify if all microservices are running
- Verify orchestration microservice is sending the appropriate provider name to NSO. Confirm that the "Provider Name" is populated correctly by navigating to **Settings** as an Admin.
- Check NSO netconf-north.log. If not, check connectivity between the Cisco MSX Portal and the NSO.

Device Registration Fails Due to Incorrect Serial Number

Problem

The device does not get registered with the PnP server and does not return any error if the tenant user enters an incorrect serial number during registration.

NSO PnP server zero touch provisioning works as:

- Tenant users register a device serial number against a device, which associates a device with a tenant, a site and a device, so Cisco MSX knows what type of configurations to push to this device.
- The connected devices call home to the PnP server, register themselves, and wait for the PnP server to push the configuration.

These events happen in any order and if the tenant user registers a device with a serial number that has not called home to the PnP server, the server waits for the device to call the PnP server. If this device never calls (because the serial number is invalid), the PnP server continues to wait.

Solution

Tenant user needs to register the device with the correct serial number. For more information, see the service pack guides on cisco.com.

Obtaining a CPE Password

If a CPE is in True/True/True state, then it should be possible to SSH from the NSO to the CPE. Required information (CPE Management IP Address, username, password) can be obtained from NSO by executing the `show pnp-state device` command as shown below.

```
admin@vms-ncs-sm> show pnp-state device XXX194326WW
pnp-state device XXX194326WW
udi PID:C881-K9,VID:V01,SN:XXX194326WW
device-info 15.5(3)M1
ip-address 11.156.141.167
mgmt-ip 10.254.0.29
port 22
name cpe-XXX194326WW
username admin
password cpe_password
sec-password cpe_password
salt ABCD
remote-node vms-ncs-dm
wan-interface FastEthernet4
lan-interface FastEthernet0
configured true
request backoff
added true
synced true
is-netsim false
need-clean false
pending-exec ""
last-contact 2015-12-09 01:53:33
```

```
 last-clean 0
 [ok][2015-12-09 01:54:14]
```

From NSO, establish an SSH session to the CPE.

```
 admin@vms-ncs-sm> ssh 10.254.0.29
 Password:cpe_password
 router line 11
 router#
```

Physical or Virtual CPE Status

If you want to check the CPE status, execute the following command:

```
admin@ncs-sm> show pnp list
SERIAL        IP ADDRESS       CONFIGURED  ADDED  SYNCED  LAST CONTACT
------------------------------------------------------------------------------
FJC2012A29P   11.255.255.35    false       false  false   2016-06-08 16:16:28
FJC2013L1SZ   11.255.255.42    false       false  false   2016-06-08 16:17:13
FJC2020L11L   11.255.255.25    false       false  false   2016-06-06 16:27:12


CONFIGURED: Day-0 config. Pushed onto CPE device
ADDED: CPE device is added into NCS
SYNCED: Service configs pushed into device
```

Display Core Data

If you want to check if the firewall, router and such Cloud VPN components are provisioned, you can execute the `show core-data` command as follows. The following example is for a Cloud VPN Advanced Service with Web Security offer:

```
 admin@ncs-sm% show core-data eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1
offering      CVPN;
service-type  FULL;
provider      vms-ottpod1;
tenant        eb272672-e0e4-4344-9a52-68cc3c1d1be1;
remote-node   ncs-dm;
geo-redundant false;
nfv cpe-FJC2027L1NQ {
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-ASA-dev1-esc-device {
    type          vFirewall;
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
    type          vRouter;
    isProvisioned true;
}
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-WSA-dev1-esc-device {
    type          vWSA;
    isProvisioned true;
}
allocations eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
```

```
    pool-name loopback;
}
```

Core data for VCE

```
 admin@ncs-sm% show core-data eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-2
offering     VCE;
service-type converged;
provider     vms-ottpod1;
tenant       eb272672-e0e4-4344-9a52-68cc3c1d1be1;
nfv eb272672e0e4-03c60e55c66b44bda0ed8da52afafc17-cloudvpn-1-CSR-dev1-esc-device {
    type          vRouter;
    isProvisioned true;
}
```

Device Registration Fails Due to Incorrect CPE Day -1 Configuration

Problem

Problem When you place an order for a service, the service comprises of devices for sites. These devices must be registered with the Cisco MSX service interface.

Problem If the device fails to register with the PnP server, you need to verify that the Day -1 configuration on the CPE allows it to call home to the PnP server.

Solution

1. Log in to the device and verify to which PNP server the device is connected to.
2. Run command show run | s pnp to list the current PnP server that this device is talking to, and examine the output:

   ```
   Router#show run | s pnp pnp
   Router#profile zero-touch transport https ipv4 <IP address> port 443 remotecert ncs
   ```

3. To change the IP address of the PNP server, switch to the configuration mode.

   ```
   Router#config terminal
   Router(config)#
   ```

4. Enter text that you received as output in Step 2, replacing the IP address with the new one.

   ```
   Router(config)#pnp profile zero-touchtransport https ipv4 <IP address> port 443 remotecert
    ncs
   ```

5. Exit out of Router(config-pnp-init) mode and then out of Router(config) mode.
6. Copy the configuration into flash configuration, by running the following command:

   ```
   Router#copy running-config flash:day--1-config
   Destination filename [day--1-config]?
   %Warning:There is a file already existing with this name
   Do you want to over write? [confirm]
   4609 bytes copied in 0.876 secs (5261 bytes/sec)
   ```

PnP Server CLI Command

Solution PnP Server to IP Device

```
show run | s pnp
Router#show run | s pnp pnp profile zero-touch transport https ipv4 203.35.248.89 port 443
remotecert ncs
```

Solution PnP Server configured with HTTPS and SSL

```
admin@ncs-sm-vbranch> show configuration pnp server
port 443;
use-ssl true;
[ok][2016-05-31 19:33:28]
```

Solution List of devices and states in contact with the PnP Server

```
admin@ncs-sm-vbranch> show pnp list
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT
------------------------------------------------------------------------------
FTX1738AJME 173.36.207.85 true true true 2016-05-23 23:44:44
FTX1738AJMG 173.36.207.81 true true true 2016-05-23 23:43:50
FTX1740ALBX 173.36.207.80 true true true 2016-05-23 23:44:21
SSI184904LG 173.36.207.82 true true true 2016-05-23 23:43:56
SSI185104LT 173.36.207.84 true true true 2016-05-23 23:43:57
[ok][2016-05-23 23:44:49]
```

Solution PNP commands to reset the CPE

```
request pnp reset clean serial xxxxxx
request pnp delete serial xxxxxx
```

If the day-1-config file need changing on CPE use the commands to create a new file and overwrite the existing:

```
tclsh
puts [open "flash:day--1-config" w+] {
aaa new-model
aaa authentication login default none
interface GigabitEthernet0
…..
pnp profile zero-touch
transport https ipv4 x.x.x.x port 443 remotecert ncs
}
Tclquit
```

Solution Viewing device-info through PnP-state

```
admin@ncs-sm-vbranch> show pnp-state device FTX1738AJME
pnp-state device FTX1738AJME
udi PID:ISR4451-X/K9,VID:V02,SN:FTX1738AJME
device-info 15.5(3)S2
ip-address 173.36.207.81
mgmt-ip 10.254.0.1
port 22
name FTX1738AJME
username user-site2
password cisco223
sec-password priv-cisco222
snmp-community-ro cisco
salt ABCD
remote-node ""
wan-interface GigabitEthernet0/0/1
lan-interface GigabitEthernet0/0/0
configured true
request config
added false
synced false
```

```
is-netsim false
need-clean false
pending-exec ""
last-contact 2016-05-31 19:29:18
last-clean 0
reload-upon-delete false
[ok][2016-05-31 19:29:23]
```

Troubleshooting Data Platform Issues

Data Platform is used to get the operational status of devices, collect matrix for device and service. They are customizable by service packs.

The following are some of the problems in Data Platform that can be fixed:

- Blocking of data due to low disk space
- Device health status is down
- No device health status is available
- Device metrics are not available

Blocking of data due to low disk space

The table below lists the issues encountered in Read-Only indices.

Table 7: Read-Only Indices Issues

Problem	Solution

Read-Only indices in Elastic Search blocks you pushing any data to it due to the low disk space	Execute the following command in Kibana:
	`PUT .kibana/_settings`
	`{`
	`"index": {`
	`"blocks": {`
	`"read_only_allow_delete": "false"`
	`}`
	`}`
	`}`

Device Health Status is Down

The table below lists the issues due to which the device health status is down.

Table 8: Device Health Status Down Issues

Problem	Solution
Destination (CSRHUB) IP not set properly	Make sure correct CSRHUB IP is set in NSO under “pnp day0-common manageddevice”.
Destination (CSRHUB) is not reachable from the device	Make CSRHUB reachable.

Problem	Solution
The beat network does not have access to the device management network	Grant access to the device management network. • If devices are behind a firewall, add rules to the firewall to let the traffic.
CSRHUB not letting traffic towards the device	Check CSRHUB license and configurations.

No Device Health Status is Available

The table below lists the issues due to which the device health status may not be available.

Table 9: No Device Health Status Available Issues

Problem	Solution
The heartbeat containers are not up	Make sure containers are up and running in Kubernetes.
Deployment issue-check deployment logs for more info	Depends on what you see in the deployment logs.
• Monitor MS failed to push device data to Cassandra • Monitor MS failed to populate "devicemetrics" for the device • Monitor MS failed to populate "deviceofmetrictype" for the device	Trigger the process on Monitor MS to push the device information to the database. • Get device connection info from Manage MS using "*GET /manage /api/v2/devices/connections/{deviceInstanceId}*". • Trigger the process in Monitor MS using "*POST /monitor/api/v2/devicemetrics/notifications /monitorChangelog*" using the device connection information you got from the previous step.
Beats did not receive correct configs from Monitor MS • Heartbeat containers crashed, and so on.	Restart collecting data by calling "*POST /monitor/api /v2/devicemetrics/{deviceInstanceId}/start*".

Device Metrics are not Available

The table below lists the issues due to which the device metrics may not be available.

Table 10: No Device Metrics Available Issues

Problem	Solution
snmpbeat containers are not up	Make sure containers are up and running in Kubernetes.
Deployment issue-check deployment logs for more info	Depends on what you see in the deployment logs.

Problem	Solution
• Monitor MS failed to push device data to Cassandra • Monitor MS failed to populate “devicemetrics” for the device • Monitor MS failed to populate “deviceofmetrictype” for the device	Trigger the process on Monitor MS to push the device information to the database. • Get device connection info from Manage MS using “*GET /manage /api/v2/devices/connections/{deviceInstanceId}*”. • Trigger the process in Monitor MS using “*POST /monitor/api/v2/devicemetrics/notifications /monitorChangelog*” using the device connection information you got from the previous step.
Beats did not receive correct configs from Monitor MS	Restart collecting data by calling “*POST /monitor/api /v2/devicemetrics/{deviceInstanceId}/start*”.
SNMP authentication failure; means that the credentials in beat configs and on the device itself don’t match, so Day0 configs might not be pushed to the device properly.	Double check the Day0 configs to be pushed to the device on Kubernetes master under “*/data/vms/custom-templates/manageddevice/cfg*”.
No response from the device might mean that the device is not reachable	Double check the connectivity to the device by checking CSRHUB health and configs and device tunnels.
No response from the device might mean that SNMP port on device is not reachable	Make sure the security groups allow traffic on SNMP port (161).