



## **Cisco Managed Services Accelerator (MSX) 4.2 Managed Device Service Pack User Guide**

**First Published:** 2022-01-19

### **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

---

<b>CHAPTER 1</b>	<b>About this Document</b>	<b>1</b>
	About this Content	1
	Document Revision History	1
	Audience	1
	Related Documentation	1
	Bias-free Doc Disclaimer	2
	Full Cisco Trademarks with Software License	3
	What's New in Cisco MSX 4.2 Managed Device	4

---

<b>CHAPTER 2</b>	<b>Cisco MSX Managed Device Service Pack Overview</b>	<b>5</b>
	Cisco MSX Managed Device Service Pack	5

---

<b>CHAPTER 3</b>	<b>Getting Started with Managed Device Service Pack</b>	<b>7</b>
	Logging In and Out of the Cisco MSX Portal	7
	Role-Based Access in Cisco MSX	7
	Managing the Managed Device-Specific User Roles	8
	Managing User Roles	8
	Adding User Role	8
	Modifying User Role	10
	Managing Tenants Groups	11
	Managing Tenants	11
	Managing Users	12

---

<b>CHAPTER 4</b>	<b>Preparing Cisco MSX Before Provisioning Devices</b>	<b>15</b>
	Network Element Driver Package	15
	Uploading a NED Package	15

- Deleting a NED Package 18
- Replacing a NED Package 19
- Preparing Device Model 21
  - Preparing Device Model Information for New Device Type 23
- Importing Device Model 24

---

**CHAPTER 5**

**Managing Device Templates 27**

- Cisco MSX Managed Device Templates 27
- Managing Templates 27
  - Creating a Device Template 27
  - Adding Device Templates 27
  - Managing Template Access for Tenants 28
  - Deleting Managed Device Templates 30

---

**CHAPTER 6**

**Provisioning Tasks 31**

- Provisioning Tasks 31
  - Provisioning a Device Supported Out-of-the-Box by Managed Device 31
    - Subscribing to Managed Device Service 31
    - Applying Template from Cisco MSX Portal 44
    - Applying Template Using CSV File 45
    - Removing Templates from Device 49
    - Deleting a Device 49
    - Unsubscribing Managed Device Service 50
  - Provisioning a Device that is Not Supported Out-of-the-Box by Managed Device 50
    - Loading SNMP Configuration Template 51
    - Preparing Device Model Information for New Device Type 52

---

**CHAPTER 7**

**Device Compliance 53**

- Editing Standard Configuration 53
- Adding Standard Configuration Category 54
  - Deleting Standard Configuration Category 56
- Creating a ServiceNow Account 57
- Adding a Device to Compliance Monitoring 59
- Removing a Device from Compliance Monitoring 59

Configuring the Compliance for Devices	60
Remediating Non-compliant Values on a Device	61
Configuring Change Management Approvals	62
Updating Monitored Devices with Standard Configuration	62
Viewing Device Vulnerabilities	63
Viewing Monitored Devices	64
Converting Device Configuration to Device Template	65

**CHAPTER 8****Monitoring Managed Device 67**

Monitoring Managed Device Service Status on the Cisco MSX GUI	67
Monitoring Managed Device Service from Tenant Workspace	68
Understanding Managed Device Life Cycle Statuses	70
Viewing Site Metrics	71
Viewing Device Metrics	72

**CHAPTER 9****Managing Meraki 75**

Attaching Organizations	76
Editing or Detaching Organizations	77
Creating Networks	79
Viewing Meraki Networks for a Site	82
Assigning Meraki Network to a Site	83
Synchronizing Networks and its Devices	84
Editing or Deleting a Network	84
Configuring Switch Ports	86
Creating Switch Port Configuration	86
Important Notes on the Switch Port Configurations	89
Editing Switch Port Configuration	89
Applying Switch Port Configuration	90

**APPENDIX A****Additional Information 93**

Devices Supported by Managed Device Service Pack	93
Downloaded Sample JSON File from the Cisco MSX	94
Sample JSON File for Importing a Device Model on the New Device Type	99





# CHAPTER 1

## About this Document

---

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

This chapter contains the following topics:

- [About this Content, on page 1](#)
- [What's New in Cisco MSX 4.2 Managed Device , on page 4](#)

## About this Content

This section provides information about related documentation of Cisco MSX and trademarks used in this content.

## Document Revision History

*Table 1: Document Revision History*

Revision Date	Change Summary
November 30, 2021	This is the first release of this guide.

## Audience

This guide is designed for service provider operators and tenants who use Cisco Managed Service Accelerator (MSX) Cloud Connect service pack to deploy cloud connect services.

## Related Documentation

You can access Cisco MSX 4.2.0 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](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 MSX GUI and navigate to **My Profile > Swagger API**.

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

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

## Bias-free Doc Disclaimer



### Note

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.



## Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

## What's New in Cisco MSX 4.2 Managed Device

Features	Description
Configuring Change Management Approvals	<p>The Cisco MSX platform provides an approval process for configuration change requests made by a user. When the approval feature is enabled on MSX, a change request for any user action on MSX will be subjected to approval. If there is a change request on 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.</p> <p>For more information on configuring change management approvals, see 'Configuring Change Management Approvals' in <a href="#">Cisco MSX Administration</a>.</p>
Switch Port Configuration Management	<p>Cisco MSX now provides the ability to configure multiple switch ports using an out-of-box template with predefined variables. For more information, see <a href="#">Configuring Switch Ports</a>.</p>
Meraki Enhancements	<p>The MSX portal now allows you to attach or detach the Meraki network to a site. For more information, see <a href="#">Assigning Meraki Network to a Site</a></p>



## CHAPTER 2

# Cisco MSX Managed Device Service Pack Overview

---

Cisco Managed Services Accelerator (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 (NFV) and enables service providers to provide their customers with 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 the 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-the-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 Device). 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 users can quickly turn on, control, and assure cloud-based managed services offered by the service provider.

For detailed information about MSX solution, see [Cisco Managed Services Accelerator \(MSX\) Solution Overview Guide](#).

This chapter contains the following topic:

- [Cisco MSX Managed Device Service Pack, on page 5](#)

## Cisco MSX Managed Device Service Pack

The Managed Device service pack provides the ability for the service providers to manage the configurations of their customer devices through a self-service portal in an operator-driven configuration template environment.

The Cisco MSX Managed Device service pack allows you to onboard devices located at the customer premise (CPEs) and apply or manage configuration settings remotely from its Network Operations Center (NOC).

The service providers can prepare parameterized configuration template files and deploy them on the CPEs. Using the Managed Device service pack, device deployment and its configurations are simplified.

Some of the advantages are:

- Zero-touch provisioning for initial device connectivity through the PnP server process.
- Service provisioning of on-premise routers through devices and VNFs.

- User Interface portal for templates configuration, ordering service, and performance or fault monitoring.

The following are some of the key concepts in the Cisco MSX Managed Device service pack:

- **Device Models:** Device models are the pre-defined set of constructs available in Cisco MSX for devices, which enables the users to capture the essential metrics data for a device. Cisco MSX Managed Device service pack provides metrics for Cisco IOS devices.

To facilitate the metrics data collection for the new device types, the device model construct should be modified to capture the details that are utilized to collect metrics for these new device types. For more information, see the topic '[Preparing Device Model Information for New Device Type](#)'.

- **Device Templates:** The device templates have parameters that are used to define a device's complete operational configuration.

A device template, when applied to a service ordering workflow, gathers the parameter values entered during the service ordering process. These values are then passed to the MSX orchestration engine (NSO) to configure the devices.

The device templates are created from the device CLI configurations. For more information, see [Converting Device Configuration to Device Template](#).

- **Adding a Device:** Using the Managed Device service pack, service providers can onboard devices located at customer premises into their network to apply and manage configurations remotely from their Network Operations Centre (NOC). This functionality allows you to onboard the devices and to apply templates during the add device procedure. For more information, see the topic '[Adding a Device](#)'.
- **Bulk Imports:** The bulk import option allows you to import multiple devices at once into Cisco MSX. The Site Template file allows you to add multiple devices and also apply the templates. For more information, see the topic on '[Importing Multiple Devices](#)'.
- **Onboarding New Device Type:** Out-of-the-box, Managed Device service pack consists of Cisco IOS Network Elements Driver (NED), which allows to onboard any Cisco IOS-XE device in the MSX system. To extend the support to any other new device type, see the topic '[Provisioning a Device that is Not Supported Out-of-the-Box by Managed Device](#)'.
- **Support for Meraki:** Manage Meraki appliances and automate provisioning actions without the need for manual intervention. For more information, see [Managing Meraki](#).



## CHAPTER 3

# Getting Started with Managed Device Service Pack

---

This chapter provides information about how to get started with the Cisco MSX Managed Device service pack.

This chapter contains the following topics:

- [Logging In and Out of the Cisco MSX Portal, on page 7](#)
- [Role-Based Access in Cisco MSX, on page 7](#)
- [Managing the Managed Device-Specific User Roles, on page 8](#)

## Logging In and Out of the Cisco MSX Portal

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

*<https://<server-ip>msx> or <https://www.example.com/>*

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

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

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

## Role-Based Access in Cisco MSX

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

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

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

For more information on Cisco MSX out-of-the-box roles, see 'User and Role-Based Access in MSX' in [Cisco MSX Administration](#). For a complete list of all the permissions available in Cisco MSX, see [Cisco Managed Services Accelerator \(MSX\) Platform and Service Packs Permissions Addendum](#).

## Managing the Managed Device-Specific User Roles

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

To create a new role and assign it to users:

**Table 2: Procedure for Creating Managed Device Specific User Roles**

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

## Managing User Roles

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

### Adding User Role

To add a user role:

## Procedure

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, click **Roles**.  
The **Manage Roles** window appears.
- Step 3** Click **Add Role**.
- Step 4** Enter the Role Name, Display Name, and Description.
- Step 5** To assign permission for the roles, click **Category** and select the corresponding check box for the permission(s) that you must grant to the role.

The types of permission you can grant are:

**Table 3: Types of Permission**

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

The table below lists the Managed Device category of permissions.

**Table 4: Category of Permissions**

Display Name	Description
Templates	<p>Allow users to manage permission to add or modify the templates required for the Managed Device Sites. The templates can be added or modified only by using the Managed Service API.</p> <p>For more information on the Manage Device API, refer to the Swagger documentation accessible from the MSX Portal &gt; User Profile icon &gt; Account Settings &gt; Swagger &gt; SFI SDK &gt; Manage Device API.</p>
Managed Device Sites	<p>Allow users to manage permission to add or modify sites to apply the template, remove the template or deprovision device. The templates can be added or modified only by using the Managed Service API.</p> <p>For more information on the Manage Device API, refer to the Swagger documentation accessible from the MSX Portal &gt; User Profile icon &gt; Account Settings &gt; Swagger &gt; SFI SDK &gt; Manage Device API.</p>

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

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

**Step 6** Click **Save**.

## Modifying User Role

To modify a user role:

### Procedure

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, click **Roles**.  
The **Manage Roles** window appears.
- Step 3** Select the role that you want to modify and click the **Edit** icon.
- Step 4** To assign or revoke the permission for the roles, click **Category** and then select or unselect the corresponding check box for the permissions.  
The table below describes the type of permissions that you can grant:



Table 5: Types of Permission

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

**Step 5** Click **Save**.

---

## Managing Tenants Groups

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

To manage tenant groups:

### Procedure

---

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, click **Tenant Groups** to view the list of tenant groups with their details in the Manage Tenant Groups window.
- Step 3** Click **Add Tenant Group**.
- Step 4** Enter the Name and Display Name of the new tenant group.
- Step 5** (Optional) Enter the Description.
- Step 6** (Optional) From the **Associate Tenants** drop-down list, choose the tenant to associate with the new tenant group.

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

**Step 7** Click **Save**.

---

## Managing Tenants

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

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

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

To manage tenants:

### Procedure

---

**Step 1** Log in to the Cisco MSX Portal.

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

The **Tenants** window appears.

Displays the list of existing tenants with their details.

**Step 3** To add a new tenant:

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

The new tenant details appears in the Tenants window.

**Step 4** To update the tenant details:

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

**Step 5** To delete the tenant:

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

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

- c) Click **Delete**.
- 

## Managing Users

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



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

---

### Before you begin

You should have administrator privilege for managing users.

### Procedure

---

**Step 1** Log in to the Cisco MSX Portal.

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

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

**Step 3** To add user:

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

**Step 4** To assign a role:

**Note** For more information on categories and permissions for the Managed Device service pack, see [Managing Users](#).

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





## CHAPTER 4

# Preparing Cisco MSX Before Provisioning Devices

---

This chapter provides information about how to prepare Cisco MSX before provisioning the devices.

This chapter contains the following topics:

- [Network Element Driver Package, on page 15](#)
- [Preparing Device Model , on page 21](#)
- [Importing Device Model, on page 24](#)

## Network Element Driver Package



**Note** Download the NED package only when you onboard a new device type into Cisco MSX Managed Device service pack.

The Cisco Network Services Orchestrator (NSO) uses Network Element Drivers (NEDs) to orchestrate a multivendor network for different devices types and services. You can add a new NED after the Cisco MSX is installed and deployed into production.

The NED management functionality in Cisco MSX allows you to add, replace, and delete NED for device management.

The Cisco MSX service packs have a predefined set of NED package that is uploaded into NSO. The Managed Device service pack consists of Cisco IOS NED. Thus allows you to onboard any IOS-XE device. Similarly, for onboarding ASR9000, you need a new Cisco IOS-XR NED added into the Managed Device NSO using the NED management functionality.

This service pack also extends its support for devices such as Cisco IOS-XR, Cisco CAT, Cisco NX-OS, Cisco ASA, Juniper SRX, and FORTINET.

## Uploading a NED Package

To upload a new NED package using the Cisco MSX portal:

**Before you begin**

- Download the NED. Use the following [URL](#).
- Use 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 6: NED Package Files**

Downloaded NED Package Files	Name of Each NED Tar 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.
- Step 2** In the main menu, go to **Settings > NED Management**.  
Displays the list of NEDs that are currently installed in the system.
- Step 3** Click **Add NED**.  
The **Upload NED File** dialog box appears.
- Step 4** Upload the downloaded NED package files in their respective fields:

Figure 1: Uploading a NED File

**Upload NED File**

This action requires a restart, during that time all device operations will be unavailable. This action may take up to 10 minutes to complete.

**UPLOAD NED PACKAGE**

Choose file:\* ncs-4.7.6-juniper-junos-4.5.13.tar.gz

**VERIFY NED PACKAGE**

Choose file:\* ncs-4.7.6-juniper-junos-4.5.13.tar.gz.signature

Choose file: tailf.cer

**INSTALL NED PACKAGE**

Service Pack:\* Managed Device

Cancel
Upload

- In the **Upload NED Package** section, 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.

- In the **Verify NED Package** section, select the Signature file and Certificate file from the downloaded NED package and upload it.
- In the **Install NED Package** section, choose the **Managed Device** from the Service Pack drop-down list.

**Step 5** Click **Upload**.

The **Upload NED** dialog box appears 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.

The **Validating and Installing NED file** dialog box appears.

The installation process takes a few minutes to complete.

Displays the validation message after installing the NED file.

**Step 7** Click **Close**.

The **NED Management** home page displays the list of NEDs that are installed in the system.

**Note** Ensure that the newly installed NED is displayed on the home page.

## Deleting a NED Package

To delete a NED package using the Cisco MSX Portal:

### Before you begin

- Ensure that you delete all the sites that are using the NED.
- On deleting NED, the device models that use the NED namespace cannot be used in Managed Device anymore.

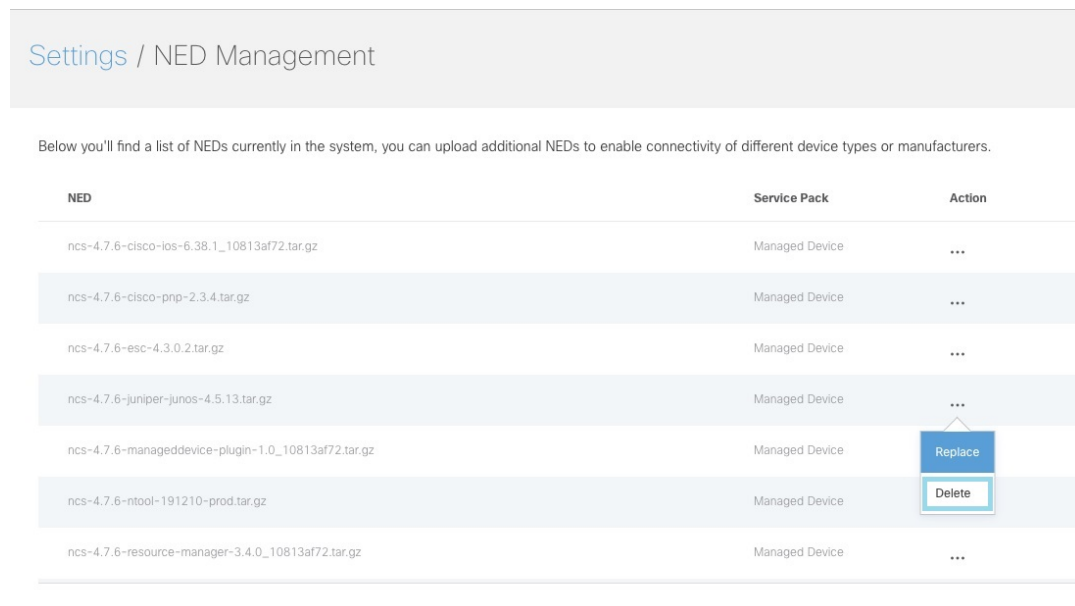
### Procedure

**Step 1** Log in to the Cisco MSX Portal.

**Step 2** In the main menu, go to **Settings > NED Management**.

Displays the list of NEDs that are currently installed in the system.

**Figure 2: Deleting NED**



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

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



**Step 4** Click **Delete**.

**Note** Now the NSO POD restarts; during this time, the device operations are unavailable.

The **Deleting and Uninstalling NED file** dialog box appears.

The deletion process takes a few minutes.

Displays the validation message after deleting the NED file.

**Step 5** Click **Close**.

---

## Replacing a NED Package

Replace option is used to upgrade or change an existing version of the NED package.

To replace a NED package using the Cisco MSX Portal:

### Procedure

---

**Step 1** Log in to the Cisco MSX Portal.

**Step 2** In the main menu, go to **Settings > NED Management**.

Displays the list of NEDs that are currently installed in the different service packs.

**Step 3** Select the NED and click **Replace**.

The **Replace NED File** dialog box appears.

Figure 3: Replacing NED

**Replace NED File**

This action requires a restart, during that time all device operations will be unavailable. This action may take up to 10 minutes to complete.

Package to be replaced: "ncs-4.7.6-cisco-ios-6.38.1\_10813af72.tar.gz".

**UPLOAD NEW NED PACKAGE**

Choose file:\* *Select NED file*

**VERIFY NED PACKAGE**

Choose file:\* *Select signature file*

Choose file: *Select certificate file*

**INSTALL NED PACKAGE**

Service Pack:\* *Managed Device*

**Cancel**      **Replace**

- Step 4** Upload the downloaded NED package files in their respective fields:
- In the **Upload NED Package** section, select the main NED file from the downloaded NED package and upload it.
  - In the **Verify NED Package** section, select the Signature file and Certificate file from the downloaded NED package and upload it.
  - In the **Install NED Package** section, choose the **Managed Device** from the Service Pack drop-down list.

**Step 5** Click **Replace**.

The **Replace NED** dialog box appears for you to confirm the replacement.

**Step 6** Click **Replace** again.

**Note** Now the NSO POD restarts; during this time, the device operations are unavailable.

The **Validating and Replacing NED File** dialog box appears.

Displays the validation message after replacing the NED file.

**Step 7** Click Close.

## Preparing Device Model

Cisco MSX Managed Device service pack supports out-of-the-box device models. To facilitate the SNMP metric collection for new device type, use the device model construct with several fields that capture all the necessary metrics data.

### Sample device model fields:

```
"deviceModelName": "", ---> Unique Name
"platformDeviceType": "", --> This is a global field and a big category where this particular
device belongs. For example "CPE".
"platformDeviceSubType": "", --> This is sub category. For example, Sub category of a Juniper
Device can be "SRX", "EX" etc..
"interfaces": [], ---> List of interfaces for the device model.
"lan": [], ---> Interfaces that can be categorized as LAN.
"wan": [], ---> Interfaces that can be categorized as WAN.
"nedId": "", --> NSO NED ID for this device
"deviceType": "", --> NSO Device-Type for this device
"directTemplate":"" --> This field allows you to apply configurations to a device while it
is onboarded to MSX. In this case, use this for applying SNMP configuration. Create a new
file and name it. Save the NSO XML template in this file. |
Note: Ensure that you keep a note of the file name used for the XML template. You can
reuse this later during device model preparation.
"deviceMetricConfigurations": [{
  "snmpDetails": { ----> This is needed to connect to the device. This step is for
preparing the CLI configuration for the SNMP support. Enter your choices for authentication
protocol, privacy protocol, user used, and so on. Ensure to make a note of it.
    "snmpAuthProto": "",
    "snmpVersion": "",
    "snmpPrivProto": "",
    "snmpUserName": ""
  },
  "platformDeviceType": "", ---> This must be similar to the device model section.
  "platformDeviceSubType": "", ---> This must be similar to the device model section.

  "snmpOidList": [], -----> The set of OIDs that is required to retrieve the data
  "snmpCpuMemoryUptimeQueryTemplate": { ---> This is a query template that explores
the data collected from SNMPBEAT and provides a representation on the UI based on device
OIDs and MIBs that are specific to this new device type.
}
}}
}
```

The two important fields in the data model construct are given in the table below:



**Note** This table contains the list of default OIDs that work only for specific Cisco devices. These OIDs may vary for the new device type. Therefore, the list of extra OIDs that helps to fetch the necessary data has to be imported into Cisco MSX.

Table 7: SNMP OID and Query Template

Data Model Field	List of Default OID/Query Template	Metrics Data
snmpOidList	"oid":".1.3.6.1.2.1.1.3"	System / System Uptime
	"oid":".1.3.6.1.6.3.10.2.1.3"	snmpEngineBoots
	"oid":".1.3.6.1.4.1.9.9.109.1.1.1.1.6"	CPU / MEM
	"oid":".1.3.6.1.4.1.9.9.109.1.1.1.1.7"	CPU / MEM 1 min
	"oid":".1.3.6.1.4.1.9.9.109.1.1.1.1.8"	CPU / MEM 5 min
	"oid":".1.3.6.1.4.1.9.9.48.1.1.1"	CiscoMemoryPool
	"oid":".1.3.6.1.2.1.2.2.1"	InterfaceTable
snmpCpuMemoryUptimeQueryTemplate	"enterprises.2636.3.1.13.1.11.9.1.0.0"	Memory consumption value in terms of percentage (%)

**SNMP OID List:** In the Managed Device service pack, SNMP metrics are collected using the OIDs of the device type. OIDs are ISO specific, but the OIDs for CPU and memory are enterprise-specific.

The collected SNMP metric data are as follows:

- Interface traffic
- Interface BW utilization
- CPU
- Memory
- System Uptime

For examples:

Table 8: SNMP OID

Name of the Vendor	OID for CPU	Description
CISCO	1.3.6.1.4.1.9.9.109.1.1.1	(1.3.6.1.4.1) – This prefix is the standard OID and must not be changed. (9.9.109.1.1.1)-This is Cisco enterprise-specific code.
JUNIPER	1.3.6.1.4.1.2636.3.1.13.1.21	(1.3.6.1.4.1.) - This prefix is the standard OID and must not be changed. (2636.3.1.13.1.21) - This is Juniper enterprise-specific code.

**SNMP QUERY Template:** The Managed Device service pack can process the data that is collected as a part of SNMP polling using the Query Template. The metrics data is represented differently for each vendor. Query template is defined based on these returned metric values.

For example: The table below lists some of the sample query templates.

**Table 9: SNMP Query Template**

Name of Vendor	OID for Memory Usage Metrics	Description
JUNIPER SRX	"enterprises.2636.3.1.13.1.11.9.1.0.0"	Represents the memory usage value in terms of percentage (%).
Cisco ASA	".1.3.6.1.4.1.9.9.48.1.1.1"	<ul style="list-style-type: none"> <li>• Cisco has no OID for representing values in terms of percentage (%).</li> <li>• But, Cisco uses the query calculation on the data fields to calculate the memory metrics.</li> <li>• Execute this OID to get the metrics of both free memory and used memory. Use these two values to compute memory usage in terms of percentage (%).</li> </ul>

## Preparing Device Model Information for New Device Type

To facilitate the SNMP metric collection for the new device type, you can utilize the device model construct to collect metrics details.

For more details on how to build each SNMP field in the device model construct, see 'Sample device model field with description' in the [Preparing Device Model](#).

Sample device model construct of Juniper:

```
{
  "deviceModels": [{
    "deviceModelName": "Juniper SRX",
    "platformDeviceType": "",
    "platformDeviceSubType": "",
    "interfaces": [],
    "lan": [],
    "wan": [],
    "nedId": "",
    "deviceType": "",
    "directTemplate": ""
  }],
  "deviceMetricConfigurations": [{
    "snmpDetails": {
      "snmpAuthProto": "",
      "snmpVersion": ""
    }
  }
}
```

```

        "snmpPrivProto": "",
        "snmpUserName": ""
    },
    "platformDeviceType": "",
    "platformDeviceSubType": "",
    "snmpOidList": [],
    "snmpCpuMemoryUptimeQueryTemplate": {
    }
}
}

```

**Next step:**

After preparing the device model information (JSON file) for the new device type, upload this JSON file into Cisco MSX. For more information, see [Importing Device Model](#).

## Importing Device Model



**Note** For onboarding new device type, prepare the device model information and then import the JSON file into the Cisco MSX. For more information, see [Preparing Device Model Information for New Device Type](#).

Ensure that you update the device model as per the latest Cisco MSX version.

To import a device model:

### Procedure

- 
- Step 1** Log in to the Cisco MSX portal.
  - Step 2** From the left pane, choose **Settings**.  
The **Settings** window appears.
  - Step 3** Click **Device Model Management**.
  - Step 4** Click **Managed Device**.  
The **Managed Device Models** window is displayed.

**Figure 4: Device Model Table**

Manage Device Models

Device Models

	Device Model	NED ID	Date Added	Last Modified	Sites
<input type="radio"/>	3rd Party Test CISCO CSR 1000v	cisco-ios	2020-02-12	2020-02-12	0
<input type="radio"/>	3rd Party Test CISCO ISR 4451	cisco-ios	2020-02-12	2020-02-12	0
<input type="radio"/>	Catalyst 3000	cisco-ios	2020-02-12	2020-02-12	3
<input type="radio"/>	CISCO CSR 1000v	cisco-ios	2020-02-12	2020-02-12	32
<input type="radio"/>	CISCO IR 829	cisco-ios	2020-02-12	2020-02-12	0
<input type="radio"/>	CISCO ISR 1100	cisco-ios	2020-02-12	2020-02-12	0
<input checked="" type="radio"/>	CISCO ISR 3900	cisco-ios	2020-02-12	2020-02-12	0
<input type="radio"/>	CISCO ISR 4221	cisco-ios	2020-02-12	2020-02-12	0
<input type="radio"/>	CISCO ISR 4321	cisco-ios	2020-02-12	2020-02-12	0
<input type="radio"/>	CISCO ISR 4331	cisco-ios	2020-02-12	2020-02-12	0
<input type="radio"/>	CISCO ISR 4351	cisco-ios	2020-02-12	2020-02-12	0

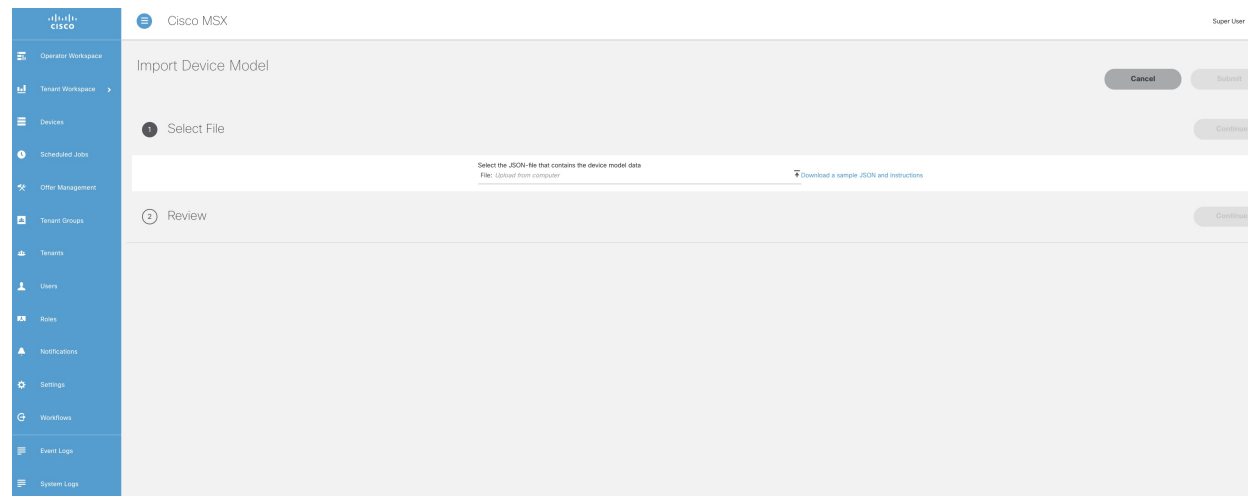
**Import Device Model**

The list of device model appears. These device models can be deleted or added again according to your requirement. Existing device models can be overwritten depending on the requirements of the interfaces used.

**Step 5** Click **Import Device Model**.

The **Import Device Model** is displayed.

**Figure 5: Import Device Model**



**Step 6** Upload the JSON file from your local file storage. This JSON file contains device model data.

The Managed Device service pack supports out-of-the box device models.

**Note** Download the sample JSON file and follow the instructions. You can modify the JSON file and upload with the same device model name. For more information, see '[Sample JSON File for Importing New Device Model](#)'.

To import device model for new device type, see [Sample JSON File for Importing a Device Model on the New Device Type](#).

For more information on the sample JSON file of the third-party device, see '[Sample JSON File for Importing a Device Model on the New Device Type](#)'.

**Step 7** Click **Review** to view the Device Model status. You can see the details about the interfaces and the capabilities of the WAN and LAN.

**Step 8** Click **Submit**.

Now the newly imported device model appears on the list of Device Model table.

#### Next Steps

- Add a device into the Cisco MSX. For more information, see '[Adding a Device](#)'.
-





## CHAPTER 5

# Managing Device Templates

---

This chapter provides information about how to manage Cisco MSX Managed Device templates.

This chapter contains the following topics:

- [Cisco MSX Managed Device Templates, on page 27](#)
- [Managing Templates, on page 27](#)

## Cisco MSX Managed Device Templates

The device template defines a complete operational configuration of the device. When the device template is applied to the service ordering workflow, the Cisco MSX service workflow gathers the parameter values; a tenant user enters these values during the service ordering process. These values are passed to NSO, which uses these values in the device configurations.

## Managing Templates

Cisco MSX Managed Device service pack provides the parameterized device templates. The template data is configured into the device and orchestrated. You can apply the template on the tenant site, remove the template, or deprovision the template.

## Creating a Device Template

The Cisco MSX platform allows you to convert both Cisco and non-Cisco native device configuration formats to device template formats. For more information, see [Converting Device Configuration to Device Template](#).

## Adding Device Templates

To add a Managed Device template in MSX:

### Procedure

---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Settings**.

- Step 3** In the **Settings** window, choose **Template Management**.
- Step 4** In the **Template Management** window, choose **Device Templates**.  
The **Template** window is displayed.
- Step 5** In the **Select A Configurational Template** section, click **New Template**.  
The **Add Template** window is displayed.
- Step 6** Enter the template name and description, then click **Continue**.

**Figure 6: Adding New Template**

The screenshot shows the 'Add Template' window in Cisco MSX. The window has a header with 'Cisco MSX' and 'Super User' with a profile icon. The main content area is titled 'Add Template' and has 'Cancel' and 'Submit' buttons. Below this is a progress bar with three steps: 1. Template Information (with an 'Edit' button), 2. Upload XML File (with a 'Continue' button), and 3. Configure Parameters (with a 'Continue' button). The 'Upload XML File' step is currently active. Below the progress bar, there is a prompt: 'Provide an XML file for your configuration template. Choose from an option below:'. There are two options: 'Enter web address: \* www.url.com' with a text input field, and 'Upload from computer: \* Click to browse'. A 'No File Selected' message is displayed above a 'Submit' button. At the bottom, there is a 'Continue' button for the next step.

- Step 7** In the **Upload XML File** section:
- Enter a URL that hosts the XML file, which is uploaded as a GET request.
  - Upload the XML file from your local file storage for the template configuration.
- Here, you can reuse the template XML file that was obtained while executing the workflow. For more information, see [Converting Device Configuration to Device Template](#).
- Step 8** Specify the template configuration parameters.  
Cisco MSX allows you to configure how the user will be prompted to enter the value for the variables. For example: You can create a drop-down list from which the users can choose the variable.
- Step 9** Click **Save**.

## Managing Template Access for Tenants

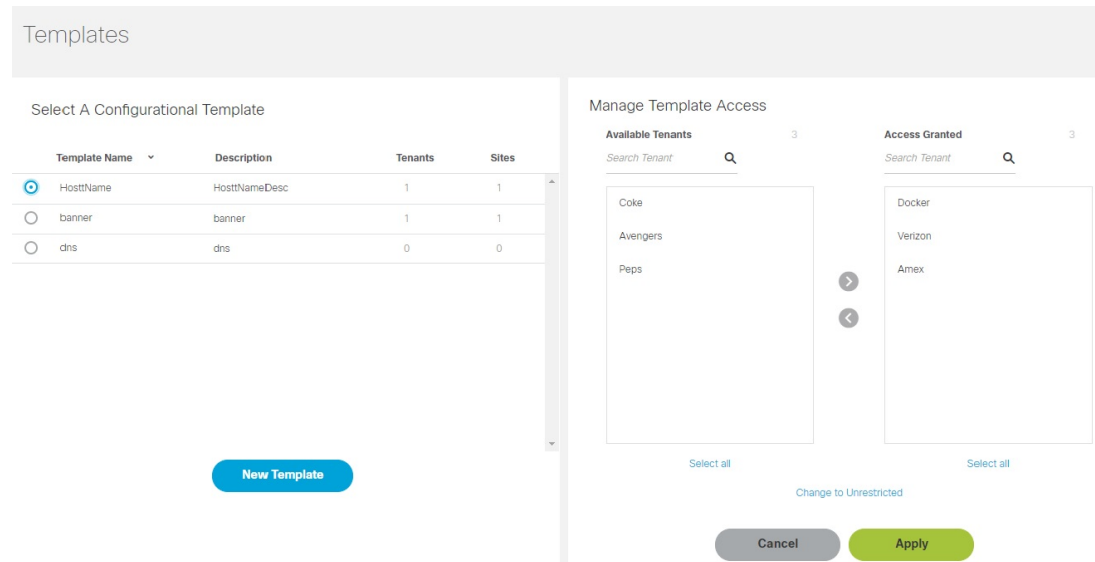
To assign or revoke template access for tenants:

## Procedure

---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Settings**.
- Step 3** In the **Settings** window, choose **Template Management**.
- Step 4** In the **Template Management** window, choose **Device Templates**.  
The **Template** window is displayed.
- Step 5** To assign template access to a tenant:
- In the **Select A Configurational Template** pane, select the template that you want to assign to a tenant.
  - In the **Manage Template Access** pane, select the tenant from the Available Tenants list.
  - Click >.  
The selected tenants move to the Access Granted list.
  - To assign the template access for all the tenants in the Available Tenants list, click **Select all**.  
**Note** You can click **Change to Unrestricted** to grant access for all the tenants to use the template.
  - Click >.  
All the tenants in the Available Tenants list are moved to the Access Granted list.
  - Click **Apply**.  
The tenant access is applied.
- Step 6** To revoke template access from the tenant:
- In the **Select A Configurational Template** pane, select the template for which you want to revoke access from the tenant.
  - In the **Manage Template Access** pane, select the tenant from the Access Granted list for whom you want to revoke access.
  - Click <.  
The tenant is moved from the Access Granted list to the Available Tenants list.
  - To revoke the template access for all the tenants for whom access is granted, click **Select all**.
  - Click <.  
Access is revoked for all tenants for whom access was granted. The tenants are moved from Access Granted list to Available Tenants list.
  - Click **Apply**.  
The tenant access is revoked.

Figure 7: Managing Template Access



## Deleting Managed Device Templates

Ensure that the template is not used by any tenant or site before deleting. Else, the deleting option to delete remains unavailable.

To remove a Managed Device template:

### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Settings**.
- Step 3** In the **Settings** window, choose **Template Management**.
- Step 4** In the **Template Management** window, choose **Device Templates**.  
The **Template** window is displayed with the list of templates.
- Step 5** Hover the mouse pointer over the template name that you want to delete, and click the **Delete** icon that appears on the right of the template name.
- Step 6** Click **Delete Template**.



## CHAPTER 6

# Provisioning Tasks

This section describes the tasks for provisioning Managed Device services pack in Cisco MSX.

This section contains the following topics:

- [Provisioning Tasks, on page 31](#)

## Provisioning Tasks

This section describes the tasks for provisioning Managed Device services pack in Cisco MSX.

This section contains the following topics:

## Provisioning a Device Supported Out-of-the-Box by Managed Device

Out-of-the-box, Managed Device service pack support for Cisco IOS-XE based devices by default.

*Table 10: Provisioning a Supported Device in the Service Pack*

Task	See
Onboarding the device.	<a href="#">Adding a Device</a>
Bulk provisioning	<a href="#">Importing Multiple Devices</a>
Configuring the template parameters to the default device using the MSX Portal.	<a href="#">Applying Template from Cisco MSX Portal</a>
Deconfiguring the applied template parameter from the device.	<a href="#">Removing Templates from Device</a>
Deleting and removing the site information from Cisco MSX.	<a href="#">Deleting Sites</a>

## Subscribing to Managed Device Service

The Cisco MSX Managed Device service pack allows you to onboard devices to the MSX platform and monitor their status and metrics. You can onboard a single device manually or multiple devices at once using the Bulk Import feature.

**Before you begin**

The prerequisites for the task are:

- A tenant and a tenant user are created.
- The device template is defined and is available for the tenant user.
- Import the device model.

**Procedure**

- 
- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Offer Catalog**. Alternatively, you can go to **Services** tile and click **View Offer Catalog**.
- The **Offer Catalog** window is displayed with the available services.
- Step 3** Click **Managed Device**.
- Step 4** Click **Subscribe**.
- The **Confirm Subscription** dialog box is displayed for you to confirm the subscription.
- Step 5** Click **Subscribe**.
- Step 6** Click **Continue**.

The Managed Device service pack is subscribed and is shown as a service in the **Services** tile.

**Next step:**

Now add a new device into the Cisco MSX. For more information, see [Adding a Device](#).

---

**Adding a Device**

To add a device:

**Before you begin**

If you are adding a Meraki device, make sure to create Meraki network. For more information, see [Creating Networks](#).

**Procedure**

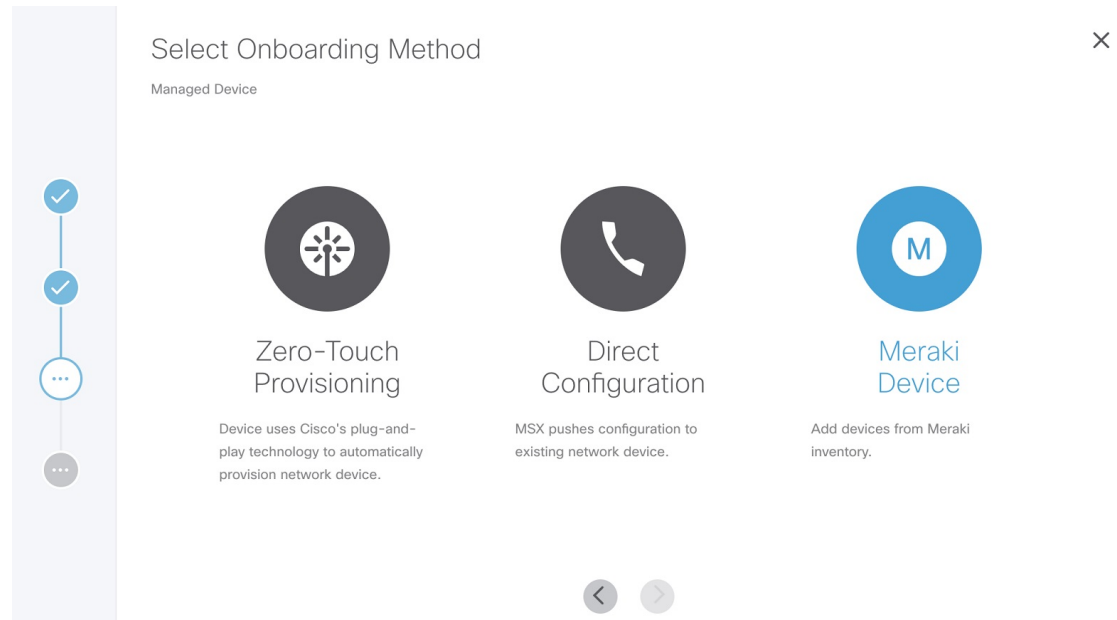
- 
- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Services**, and select a tenant, and click **Continue**.
- The list of services available for the tenant is displayed.
- Step 3** Click the Managed Device service panel to expand, and click the **ellipsis (...)** and choose **Add Device** from the menu. You can also click the **Add Device** button.
- The **Add New Device** wizard is displayed.

**Step 4** Click **Get Started**.  
The **Service Selection** window is displayed.

**Step 5** Select the **Managed Device** option, and click >.

**Step 6** Select the device **Onboarding Method** from the available options.

**Figure 8: Onboarding Method**



- **Zero-Touch Provisioning**—The device automatically contacts and connects to MSX either through Cisco Plug-and-Play using an initial configuration or redirected using `devicehelper.cisco.com`.
- **Direct**—Cisco MSX initiates a connection to the device directly using the device access details provided through the UI or Site Template file.
- **Meraki** — Add Meraki devices.

**Step 7** Specify the Device Details. Based on the selected onboarding type, enter the device details.

**For Zero-Touch Provisioning:**

- Enter the name of the device.
- From the **Device Model** drop-down list, choose the required device model.

The NED ID and Device Type are displayed based on the selected device model automatically.

- Enter the **Serial Number** of the device.

You can, optionally, enter the Serial Number after adding the device.

To add a serial number later, check the **Provide Serial Number Later** check box.

**Note** Cisco MSX onboards the device only after the serial number is added. For more information on adding a serial number, see [Adding a Serial Number](#).

- To add the device to compliance, check the **Add to compliance** check box.

Adding a device to compliance ensures that the device that is configured to a set of standards remains in that state until it is changed.

- e) From the **Tunnel Management** drop-down list, choose either **TLS** or **IPSec**. If you choose **TLS**, you have to choose an appropriate TLS gateway and enter the IP address of the device.

**Note** The TLS Gateway/Spoke services are optional deployments to MSX that can be used as an alternative to CSR Hub to extend connectivity from MSX out to data centers that cannot use traditional IPSec tunnels. If you require TLS Gateway functionality, there are setup steps that must be performed prior to using this feature. For more information, please contact your System Administrator.

- f) Enter the **IP Address** of the device.  
g) From the **Gateway Pools** drop-down list, choose an appropriate TLS gateway.  
h) From the **Bring Up a Secure Management Tunnel to MSX** drop-down list, choose **Yes** to establish an encrypted management tunnel to connect devices to MSX cloud. The encrypted tunnel can be used for sending the statistics report and other configuration details to the Cisco MSX or SP Network.

**Note** The secure management tunnel is enabled only when you select a device model with NED-ID as Cisco-IOS.

From the **Bring Up a Secure Management Tunnel to MSX** drop-down list, choose **No** to onboard the device without a management tunnel.

- i) From the **Onboarding Interface** drop-down list, choose the onboarding interface for monitoring WAN and LAN.

**Note** By default, if **WAN** is selected, you can change it to **LAN**. But, if **LAN** is selected by default, you cannot change it to **WAN**.

- To monitor the WAN, check the **WAN** check box.
- To monitor the LAN, check the **LAN** check box.
- To clear the entry, uncheck the **WAN/LAN** check box.

- j) Click **Next**.

**Note** The Managed Device home page displays the devices that have no serial number in both the List view and Map view. This device is in the unregistered state.

Only on adding the serial number, the device gets onboarded into the Cisco MSX. For more information on adding a serial number, see [Adding a Serial Number](#).



Figure 9: Zero-Touch Provisioning

## Add Device Details

✕

Managed Device

**ZERO TOUCH PROVISIONING**

Device Name:\* DemoPNP ?

---

Device Model:\* Catalyst 3000 ▼

---

Serial Number:\* Fv1013 ?

---

Provide Serial Number Later

Add to compliance

Bring up a secure management tunnel to MSX?:\* Yes ▼

---

Onboarding Interface: GigabitEthernet0/1 ▼

---

	WAN	LAN
GigabitEthernet0/1	<input checked="" type="checkbox"/>	
vlan10	<input type="checkbox"/>	
vlan20	<input type="checkbox"/>	
vlan30		<input type="checkbox"/>
vlan40		<input type="checkbox"/>

◀
▶

Figure 10: Zero-Touch Provisioning-TLS Gateway

The screenshot shows the 'Add Device Details' form for a Managed Device. The form is titled 'Add Device Details' and has a close button (X) in the top right corner. The form is divided into sections: 'ZERO TOUCH PROVISIONING' and 'Tunnel Management'. The 'ZERO TOUCH PROVISIONING' section includes fields for Device Name (Router1), Device Model (CISCO CSR 1000v), and Serial Number (9999). There are checkboxes for 'Provide Serial Number Later' and 'Add to compliance'. The 'Tunnel Management' section includes a dropdown menu for Tunnel Management (TLS) and an IP Address field. Below these fields is a table for interface configuration with columns for WAN and LAN. The table has two rows for GigabitEthernet1 and GigabitEthernet2, each with checkboxes for WAN and LAN.

	WAN	LAN
GigabitEthernet1	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet2	<input type="checkbox"/>	<input type="checkbox"/>

**For the Direct onboarding type:**

- In the **Device Name** field, enter the name of the device.
- From the **Device Model** drop-down list, choose the required device model.

The Device Type and NED ID are displayed based on the selected device model automatically.

- In the **IP Address** field, enter the IP address of the device.
- In the **Port** field, enter the port number.
- In the **User Name** field, enter the user name.
- In the **Password** field, enter the password.
- In the **Secondary Password** field, enter the secondary password.

**Note** The Secondary Password is required for Cisco IOS devices to enter into the privilege mode.

- Click **Next**.
- From the **Bring Up a Secure Management Tunnel to MSX** drop-down list, choose **Yes** to establish an encrypted management tunnel to connect devices to MSX Cloud. The encrypted tunnel can be used for sending statistics report and other configuration details to the Cisco MSX or SP Network. This option is available only for the Cisco IOS devices.

From the **Bring Up a Secure Management Tunnel to MSX** drop-down list, choose **No** to onboard the device without a management tunnel.

- j) From the **Onboarding Interface** drop-down list, choose the onboarding interface for monitoring the LAN and WAN.

**Note** By default, if **WAN** is selected, you can change it to **LAN**. But, if **LAN** is selected by default, you cannot change it to **WAN**.

- To monitor the WAN, check the **WAN** check box.
- To monitor the LAN, check the **LAN** check box.
- To clear the entry, uncheck the **WAN/LAN** check box.

**Figure 11: Direct Onboarding**

The screenshot shows the 'Add Device Details' form for a Managed Device. The form includes the following fields and options:

- Device Name: \* ManagedRouter
- Device Model: \* CISCO CSR 1000v
- IP Address: \* 127.0.0.1
- Port: \* 22
- User Name: \* admin
- Password: \* .....
- Secondary Password: \* .....
- Bring up a secure management tunnel to MSX?: \* Yes
- Onboarding Interface: GigabitEthernet2

	WAN	LAN
GigabitEthernet1	<input type="checkbox"/>	<input type="checkbox"/>
GigabitEthernet2	<input checked="" type="checkbox"/>	<input type="checkbox"/>

## Meraki

- On the **Select Site and Network** page, from the **Site Name** and **Meraki network** drop-down options, select a site and network you want to associate your Meraki devices to.
- On the **Add Meraki Devices** page, select the devices from the available list of active devices for the network that was selected in the previous step. You can filter the devices by device name and device model.

**Note** For network with appliance device type, you can add only maximum of two devices.

- c) Click > to move to the **Review and Submit** page.
- d) Review the details and click **Submit** to complete the process.

**Step 8**

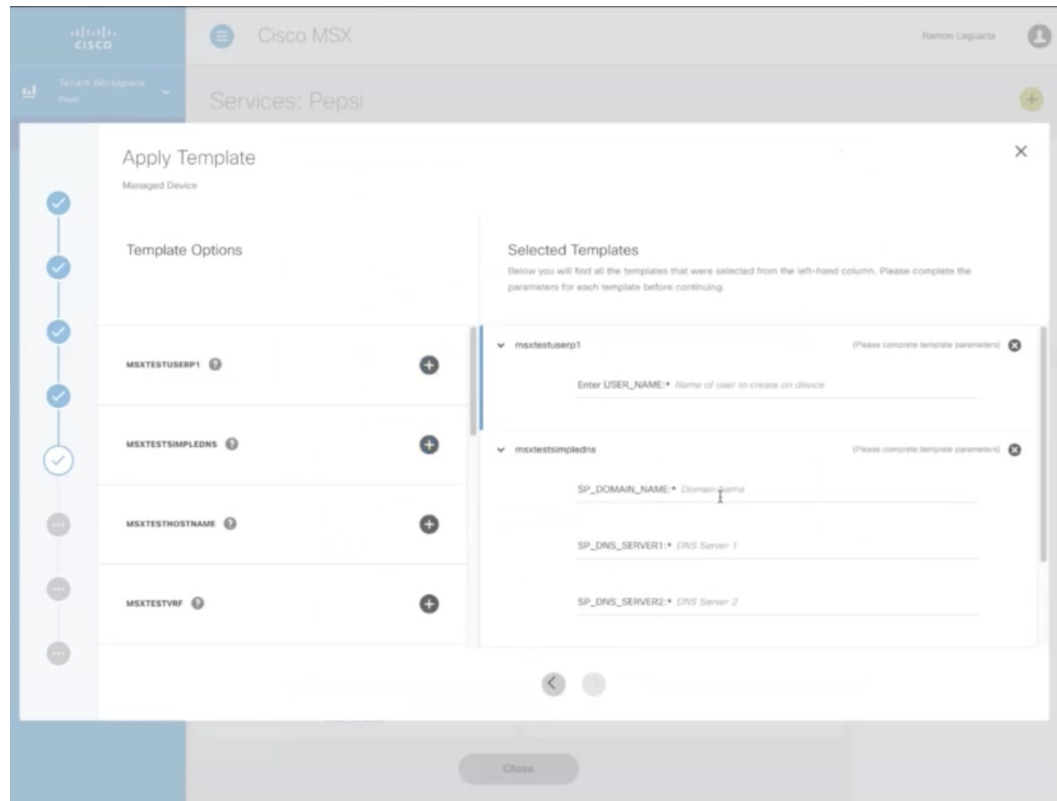
Click **Next**.

**Step 9**

In the **Select Template** section, you can select one or more templates that you want apply on the device from the **Template Options** pane.

The selected stack of templates appears on the **Selected Templates** pane.

**Figure 12: Select Templates**



- a. To apply multiple templates on the device:
  - In the **Template Option** pane, click the + icon to apply the desired device templates on the device.
  - In the **Selected Template** pane, enter the value for each template instance.
- b. To apply the same template more than once on the device:
  - In the **Template Option** pane, click the + icon to apply the desired device templates on the device.
  - In the **Selected Template** pane, enter the new set of values for each template instance.

**Note** Cisco MSX allows you to reapply the same template repeatedly with a new set of values for each template instance.

Each template in the stack is independent of the other template. These templates can be selected in any order.

The latest selected template appears first in the template stack. These configurations are applied to the device in an appropriate order.

**Note** You can revoke a specific template from the template stack to cancel any of the configurations that is applied to a template.

**Step 10** Click **Next**.

The device information you configured is displayed for review.

**Step 11** Click **Next**.

The device is added successfully and a message is displayed. From here, you can either view the device details or assign device to a site. Click **View Device** to view the details of the device.

**Step 12** Click **Assign Device to Site** to assign the device to a site.

Click **Do not show this introductory step again** to skip the introductory step. Next time this window will not be shown when you assign a site.

**Step 13** Click **Next**.

The **Select Site** window is displayed.

**Step 14** In the **Site name** field, search for the site name and select a site from the drop-down list.

**Step 15** Click **Next**.

The site is assigned to a device.

**Step 16** Click **Close**.

---

## Adding a Serial Number

Cisco MSX onboards devices only after the serial number is added. To add a serial number:

### Procedure

---

**Step 1** Log in to the Cisco MSX portal.

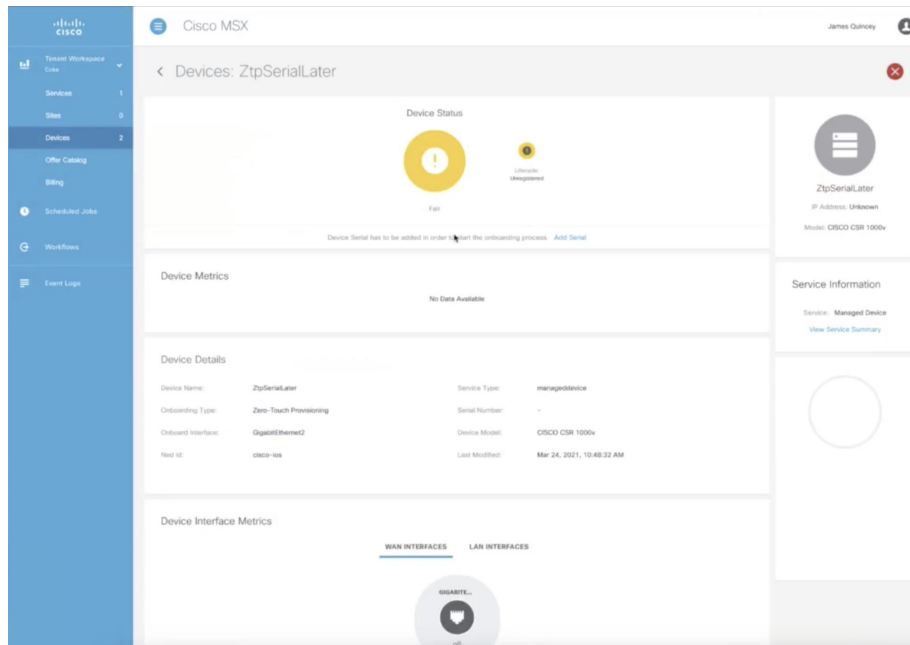
**Step 2** From the left pane, choose **Tenant Workspace > Devices**.

The **Devices** tile is displayed with the available devices.

**Step 3** Choose a device from the list.

The device information is displayed.

Figure 13: Adding a Serial Number



- Step 4** In the **Device Status** section, click **Add Serial**.  
The **Add Serial Number** dialog box is displayed.
- Step 5** Enter the serial number.
- Step 6** Click **Add Serial**.  
The serial number is added successfully and a message is displayed.
- Step 7** Click **Close**.

## Importing Multiple Devices

Cisco Managed Device service pack allows you to import multiple devices at once using the bulk import feature. The Site Template file is used to import multiple devices. This file has a custom header row, and each subsequent row in the file represents a device to be created. You need to enter the required data in the appropriate columns of the file and then import the Site Template file to Cisco MSX.



**Note** You must have a role that includes the `MANAGE_BULK_IMPORT` permission to perform the bulk import operation.

To avoid potential errors, disable the bulk import function if a bulk import job is already running. For example, if an error occurs when the bulk import job includes a device that is already provisioned, then the device gets duplicated in the Cisco MSX. Performing the jobs in sequence ensure that all the devices are added correctly by detecting and ignoring duplicate devices.

To download a Site Template:

## Procedure

**Step 1** Log in to the Cisco MSX portal.

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

The **Services** tile is displayed with the Managed Device service.

**Step 3** Click the **ellipsis (...)** and choose **Import Devices Using CSV** from the menu.

The **Import Managed Devices using CSV** window is displayed.

**Note** You can also access this feature from **Service Controls** pane. Choose **Tenant Workspace > Service Controls > Import Managed Devices using CSV**.

**Step 4** Prepare the Site Template file.

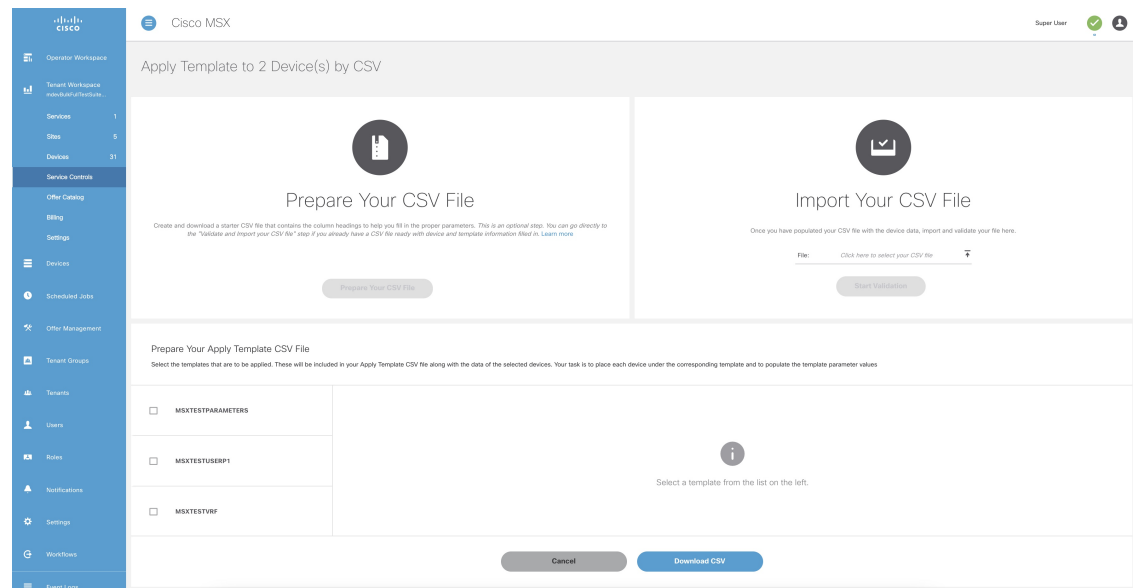
a) Click **Prepare your CSV file**.

The list of all the available templates for the tenant is displayed.

**Note** If templates are not currently available, add the device templates to the template library. For more information, see [Adding Device Templates](#).

b) Select the templates that are to be applied for the devices at the time of import.

**Figure 14: Site Template File Preparation**



**Step 5** Download a Site Template file.

a) Click **Download CSV**.

Only the tenant users with the access privilege can download the Site Template file.

For more information on assigning the template to tenant users, see [Managing Template Access for Tenants](#).

b) Save the file to your local file storage.

**Step 6** Edit the downloaded Site Template file.

The downloaded Site Template file contains only the selected templates. The header of this file depends on the templates you had selected.

You can manually add the devices and parameter values in the Site Template file. Each subsequent row represents a device to be created.

Using the Site Template file, you can apply single or multiple templates and reapply the same template repeatedly to the selected device.

- **For a single site:** You can add a single device and apply the templates. Enter the parameter values manually in the Site Template file. Now import this file into Cisco MSX.
- **For multiple sites:** You can add any number of devices and apply the templates for each device. Enter the parameter values manually for each template instance in the Site Template file. Now import this file into Cisco MSX.
- **Applying a single template multiple times on a device:** Cisco MSX enables you to reapply a single template multiple times to a device with a new set of values using a Site Template file. Enter the parameter values manually for every template instance. Use a comma to separate these parameter values in their respective fields of the Site Template file.

**Figure 15: Site Template File**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	Site Name	Device Name	Description	Location	Device Onboarding	Serial Number	Device Model	LAN Interface	WAN Interface	Onboarding I	Device IP Address	Device Port	Device Username	Device Password	Device Secondary	Enable Secure	Compliance	Templates To Apply	
2	Ottawa	Rem1	Ottawa	Ottawa	pnp	9TUQOEDDBUI	CISCO CSR 1000v		GigabitEthernet	GigabitEthernet2						TRUE	NO	No Template	

**Step 7** Import the Site Template file.

- a) Click **Import Your CSV File** to upload the prepared Site Template file from your local storage.

**Note** You can also access this feature from **Service Controls** pane. Choose **Tenant Workspace > Service Controls > Import Managed Devices using CSV**.

- b) Click **Start Validation**.

Once the file is uploaded, the device data is validated.

- If the device data in the Site Template file is valid, the **Validation Complete** dialog box appears. Click **Import Devices**. The device data is added to the Cisco MSX.
- If the device data in the Site Template file is invalid, the validation process detects and displays the errors.

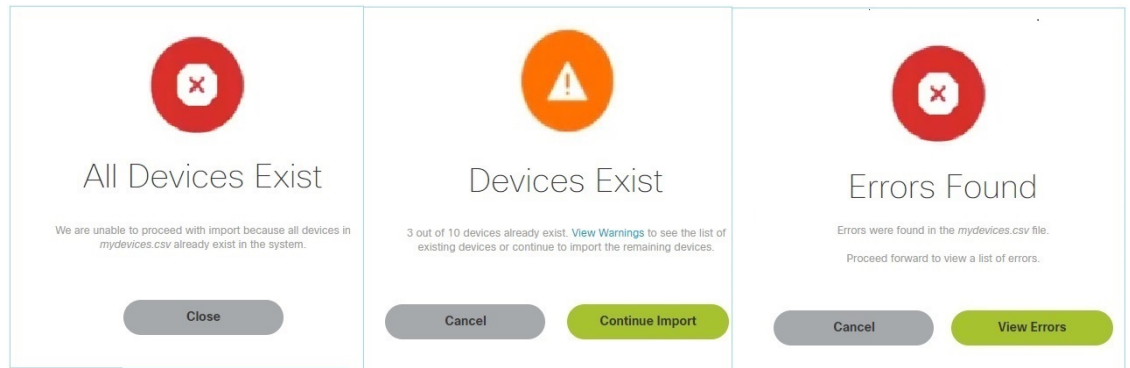
Cisco MSX spots the exact row number and specific field that has incorrect data and displays a detailed error list. Displays both errors and warning messages to the user.

- **Error message:** Indicates the wrong format, invalid entry, and templates that do not exist. Fix these errors to proceed further with the Site Template import.

**Warning message:** Indicates that the site exists in the Cisco MSX system. The warning message allows you to import other new sites that are added in this Site Template file.



Figure 16: Validation Messages



c) The validation messages are:

1. **All Device Exist:** Indicates that the devices added in the Site Template file are already found in the Cisco MSX, therefore unable to proceed further with the file import process.

Click **Close**.

Upload the Site Template file with the valid device data again.

2. **Devices Exist:** Indicates that a few of the devices in the Site Template file already exist in the Cisco MSX.

- Click **View Warnings**.

The **Device Data Errors** window appears. Displays the warning messages and their corresponding row numbers.

- Click **Download Error List** to download the error file.
- Click **Back to File Upload** to import the same Site Template file.
- Click **Cancel Import** to withdraw the file import and exit from the entire operation.

- Click **Continue Import** to import the existing Site Template file into the Cisco MSX.  
Displays the new device in the Managed Device home page.

3. **Error Found:** In this case, a combination of both warnings and error messages appear.

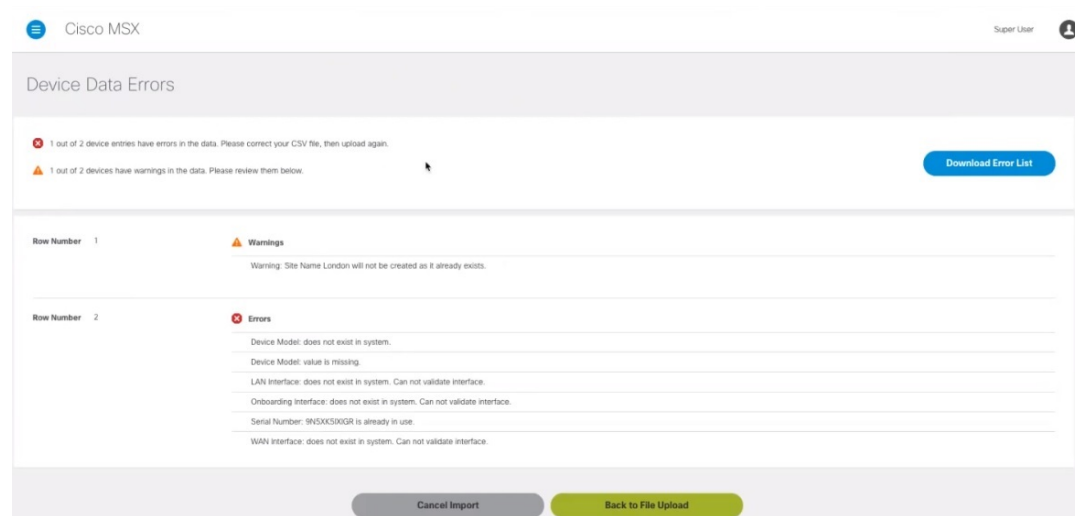
- Click **View Errors**.

The **Device data error window** appears. Displays the list of all the validation errors with the corresponding row numbers.

- Click **Download Error List** to download the validation error file.

**Note** If you want to add more devices to the Site Template file after it is uploaded to Cisco MSX, you must add the details of these new devices to an existing Site Template file and upload the updated file to Cisco MSX again.

Figure 17: Device Data Errors



## Applying Template from Cisco MSX Portal

To apply template to a device:

### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the list of devices.
- Step 3** Click the **ellipsis (...)** that is located far right on the same row and then choose **Apply Template**.  
The **Apply Template** window is displayed.
- Step 4** From the **Apply Template** window, select one or more templates that you want to apply on the device.  
The selected stack of templates appears on the **Selected Templates** pane.
  - a.** To apply the same template more than once on a device:
    - In the **Template Options** pane, click the + icon to apply the desired device templates on the device.
    - In the **Selected Template** pane, enter the new set of values for each template instance.

For example: If you select a template, Cisco MSX allows you to reapply the same template multiple times with a new set of values for the template instance.

**Figure 18: Apply Template**

Apply Template

Template Options	Selected Templates
<p>Below you'll find template options, which you can select as often as you would like.</p> <p>MSXTESTNOPARAMS ? +</p> <p>MSXTESTUSERP15 ? +</p> <p>MSXTESTSIMPLEDNS ? +</p> <p>MSXTESTOPENDNS ? +</p>	<p>Below you will find all the templates that were selected from the left-hand column. Please complete the parameters for each template before continuing.</p> <p>msxtestnoparams ✕</p>

**Step 5** Click **Submit**.

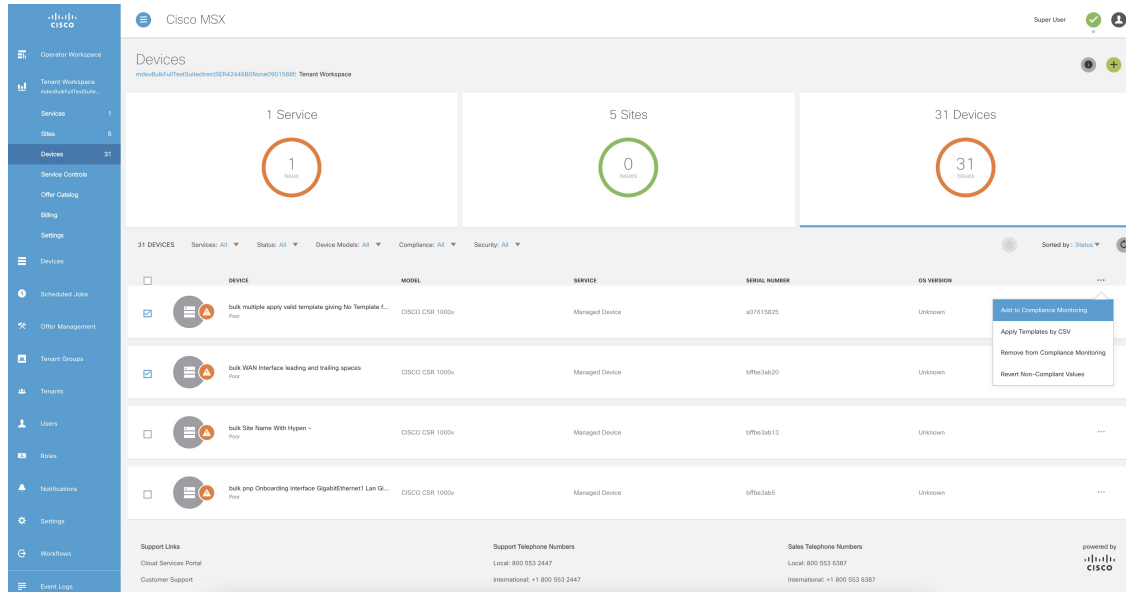
## Applying Template Using CSV File

To apply template on multiple devices using CSV file:

### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the list of devices.
- Step 3** Select multiple devices from the list.
- Step 4** Click the **ellipsis (...)** that is located far right on the column header and then choose **Apply Template by CSV**.

Figure 19: Applying Template Using CSV File



**Step 5** Prepare the Site Template file.

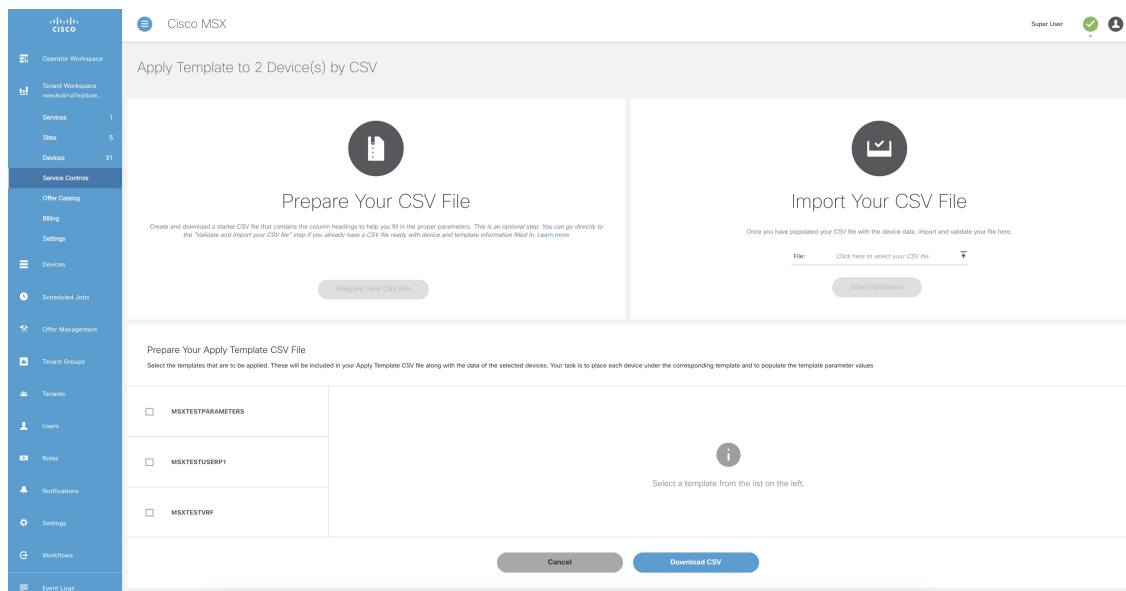
- a) Click **Prepare your CSV file**.

The list of all the available templates for the tenant is displayed.

**Note** If templates are not currently available, add the device templates to the template library. For more information, see [Adding Device Templates](#).

- b) Select the templates that are to be applied for the devices at the time of import.

Figure 20: Site Template File Preparation



**Step 6** Download a Site Template file.

- a) Click **Download CSV**.

Only the tenant users with the access privilege can download the Site Template file.

For more information on assigning the template to tenant users, see [Managing Template Access for Tenants](#).

- b) Save the file to your local file storage.

**Step 7** Edit the downloaded Site Template file.

The downloaded Site Template file contains only the selected templates. The header of this file depends on the templates you had selected.

You can manually add the devices and parameter values in the Site Template file. Each subsequent row represents a device to be created.

Using the Site Template file, you can apply single or multiple templates and reapply the same template repeatedly to the selected device.

- **For a single site:** You can add a single device and apply the templates. Enter the parameter values manually in the Site Template file. Now import this file into Cisco MSX.
- **For multiple sites:** You can add any number of devices and apply the templates for each device. Enter the parameter values manually for each template instance in the Site Template file. Now import this file into Cisco MSX.
- **Applying a single template multiple times on a device:** Cisco MSX enables you to reapply a single template multiple times to a device with a new set of values using a Site Template file. Enter the parameter values manually for every template instance. Use a comma to separate these parameter values in their respective fields of the Site Template file.

**Figure 21: Site Template File**

	A	B	C	D	E	F	G	H	I
1	Device Id	Device Name	Templates To Apply	DNS:SP_DNS_SERVER1	DNS:SP_DNS_SERVER2	DNS:SP_DOMAIN_NAME			
2	15f90617-71	MDdevice2	DNS	8.8.8.8	8.8.1.1	cisco.com			
3	c235edc5-b1	MDDevice1	DNS	8.8.8.8	8.8.1.1	cisco.com			

**Step 8** Import the Site Template file.

- a) Click **Import Your CSV File** to upload the prepared Site Template file from your local storage.

**Note** You can also access this feature from **Service Controls** pane. Choose **Tenant Workspace > Service Controls > Apply Templates to Managed Devices using CSV**.

- b) Click **Start Validation**.

Once the file is uploaded, the device data is validated.

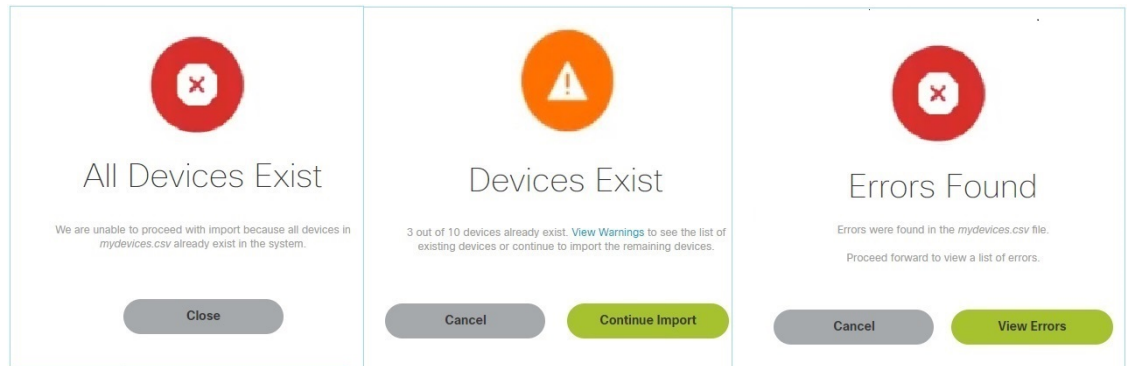
- If the device data in the Site Template file is valid, the **Validation Complete** dialog box appears. Click **Import Devices**. The device data is added to the Cisco MSX.
- If the device data in the Site Template file is invalid, the validation process detects and displays the errors.

Cisco MSX spots the exact row number and specific field that has incorrect data and displays a detailed error list. Displays both errors and warning messages to the user.

- **Error message:** Indicates the wrong format, invalid entry, and templates that do not exist. Fix these errors to proceed further with the Site Template import.

**Warning message:** Indicates that the site exists in the Cisco MSX system. The warning message allows you to import other new sites that are added in this Site Template file.

Figure 22: Validation Messages



c) The validation messages are:

1. **All Device Exist:** Indicates that the devices added in the Site Template file are already found in the Cisco MSX, therefore unable to proceed further with the file import process.

Click **Close**.

Upload the Site Template file with the valid device data again.

2. **Devices Exist:** Indicates that a few of the devices in the Site Template file already exist in the Cisco MSX.

- Click **View Warnings**.

The **Device Data Errors** window appears. Displays the warning messages and their corresponding row numbers.

- Click **Download Error List** to download the error file.
- Click **Back to File Upload** to import the same Site Template file.
- Click **Cancel Import** to withdraw the file import and exit from the entire operation.
- Click **Continue Import** to import the existing Site Template file into the Cisco MSX.

Displays the new device in the Managed Device home page.

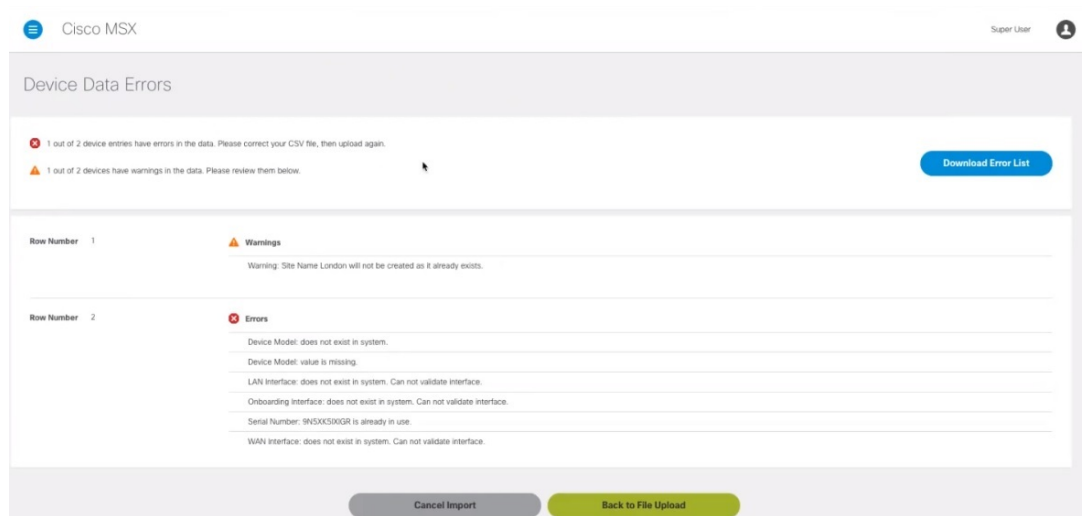
3. **Error Found:** In this case, a combination of both warnings and error messages appear.

- Click **View Errors**.

The **Device data error window** appears. Displays the list of all the validation errors with the corresponding row numbers.

- Click **Download Error List** to download the validation error file.

Figure 23: Device Data Errors



## Removing Templates from Device

To remove templates from a device:

### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the list of devices.
- Step 3** From the list, select the device for which you want to remove the template.
- Step 4** Click the **ellipsis (...)** that is located far right on the same row and then choose **Remove Templates**.  
The **Remove Templates** confirmation dialog box appears for you to confirm the removal of all the templates from the device.
- Step 5** Click **Remove Template**.  
The applied templates are removed from the device.

## Deleting a Device

To delete a device:

**Procedure**

- 
- Step 1** Log in to the Cisco MSX portal.
  - Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the list of devices.
  - Step 3** From the list view, select the device that you want to delete.
  - Step 4** Click the **ellipsis (...)** that is located far right on the same row of the device and then choose **Delete Device**.  
The **Delete Device** confirmation dialog box appears.
  - Step 5** Click **Yes** to delete the device from Cisco MSX.
  - Step 6** Click **Delete Site**.
- 

## Unsubscribing Managed Device Service

To unsubscribe Managed Device service pack:

**Procedure**

- 
- Step 1** Log in to the Cisco MSX portal.
  - Step 2** From the left pane, choose **Tenant Workspace > Services**.  
The **Services** tile is displayed with the Managed Device service.
  - Step 3** Click the **ellipsis (...)** and choose **Unsubscribe** from the menu.  
The **Unsubscribe from Managed Device** dialog box is displayed.
  - Step 4** Click **Unsubscribe**.
- Note** Unsubscribing to the Managed Device service deletes all devices and Meraki networks associated with the service.
- 

## Provisioning a Device that is Not Supported Out-of-the-Box by Managed Device

*Table 11: Steps Involved in Provisioning New Device Type in Managed Device*

Task	See
The Managed Device consists of Cisco IOS NED by default to onboard any Cisco IOS-XE devices. The NED package is decided based on the new device type that is to be onboarded. Upload the new NED into the Managed Device NSO.	<a href="#">Uploading a NED Package</a>



Task	See
Preparing the SNMP device template.	<a href="#">Loading SNMP Configuration Template</a>
Preparing the device model construct (JSON file) to collect the SNMP metrics data for the new device type that is to be onboarded into Cisco MSX.	<a href="#">Preparing Device Model Information for New Device Type</a>
The JSON file now has all the necessary device model fields. Upload this file into the Cisco MSX Portal to capture the SNMP metric data of the new device type.	<a href="#">Importing Device Model</a>
Onboard the new device type in the Managed Device service pack.	<a href="#">Adding a Device</a>

## Loading SNMP Configuration Template

To load SNMP configuration template:

### Procedure

**Step 1** Convert CLI configuration into the NSO XML template for a new device type using the procedure explained [here](#). For more information on workflow, see [Creating Device Template](#).

Convert some of the tags in the XML template to variables. The tags are:

- snmp-user
- snmp-priv-password
- snmp-auth-password

**Note** While preparing the CLI configuration for SNMP support, ensure that you make a note of authentication protocol, privacy protocol, and user name.

```
"snmpAuthProto": "AuthProto",
"snmpVersion": "3",
"snmpPrivProto": "aes",
"snmpUserName": "username"
```

**Step 2** Add the SNMP template to custom-templates folder on kubernetes-master node.

a) To navigate to kubernetes master node, execute the following:

```
cd /data/vms/custom-templates/manageddevice/templates/
```

b) Create a .xml file. Add the NSO XML contents into this file and save it.

For example: junos-snmp.xml file

**Note** Ensure that you make a note of the .xml file name. The XML file will be later reused while preparing the device model information.

**Step 3** Reload the NSO. The XML template should be loaded into NSO database system.

- a) Log in to NSO POD and connect to NCS\_CLI.
- b) To reload NSO, execute the following:

```
vmsnso@ncs> request packages reload
```

- c) To verify if the XML template is loaded successfully, execute the following:

```
vmsnso@ncs> show packages package custom-templates templates
templates [ junos-snmp ]
```

### Next Steps

- Preparing device model information. For more information, see [Preparing Device Model Information for New Device Type](#).

## Preparing Device Model Information for New Device Type

To facilitate the SNMP metric collection for the new device type, you can utilize the device model construct to collect metrics details.

For more details on how to build each SNMP field in the device model construct, see 'Sample device model field with description' in the [Preparing Device Model](#).

Sample device model construct of Juniper:

```
{
  "deviceModels": [{
    "deviceModelName": "Juniper SRX",
    "platformDeviceType": "",
    "platformDeviceSubType": "",
    "interfaces": [],
    "lan": [],
    "wan": [],
    "nedId": "",
    "deviceType": "",
    "directTemplate":""
  }],
  "deviceMetricConfigurations": [{
    "snmpDetails": {
      "snmpAuthProto": "",
      "snmpVersion": "",
      "snmpPrivProto": "",
      "snmpUserName": ""
    },
    "platformDeviceType": "",
    "platformDeviceSubType": "",
    "snmpOidList": [],
    "snmpCpuMemoryUptimeQueryTemplate": {
    }
  }
  ]
}
```

### Next step:

After preparing the device model information (JSON file) for the new device type, upload this JSON file into Cisco MSX. For more information, see [Importing Device Model](#).



## CHAPTER

# 7

## Device Compliance

---

This chapter provides information about device compliance.

This chapter contains the following topics:

- [Editing Standard Configuration, on page 53](#)
- [Adding Standard Configuration Category, on page 54](#)
- [Creating a ServiceNow Account, on page 57](#)
- [Adding a Device to Compliance Monitoring, on page 59](#)
- [Removing a Device from Compliance Monitoring, on page 59](#)
- [Configuring the Compliance for Devices, on page 60](#)
- [Remediating Non-compliant Values on a Device, on page 61](#)
- [Configuring Change Management Approvals, on page 62](#)
- [Updating Monitored Devices with Standard Configuration, on page 62](#)
- [Viewing Device Vulnerabilities, on page 63](#)
- [Viewing Monitored Devices, on page 64](#)
- [Converting Device Configuration to Device Template, on page 65](#)

## Editing Standard Configuration

The Standard Configuration is the set of values that must be compliant across devices added to compliance monitoring. Devices that are added to Compliance monitoring will have their configuration validated against the Standard Configuration. Any deviations from the Standard Configuration will be reported immediately in the system and users are alerted. Devices are also monitored in real-time for any remote changes that may deviate from the Standard Configuration. The values in the Standard Configuration will be applied to all configured device types.

Standard Configuration involves two parts. The first part is defining the Standard Configuration by creating a set of categories, which is described in [Adding Standard Configuration Category](#). After you create the Standard Configuration categories, the second part is providing any dynamic values required, which is described below.

To edit standard configuration values:

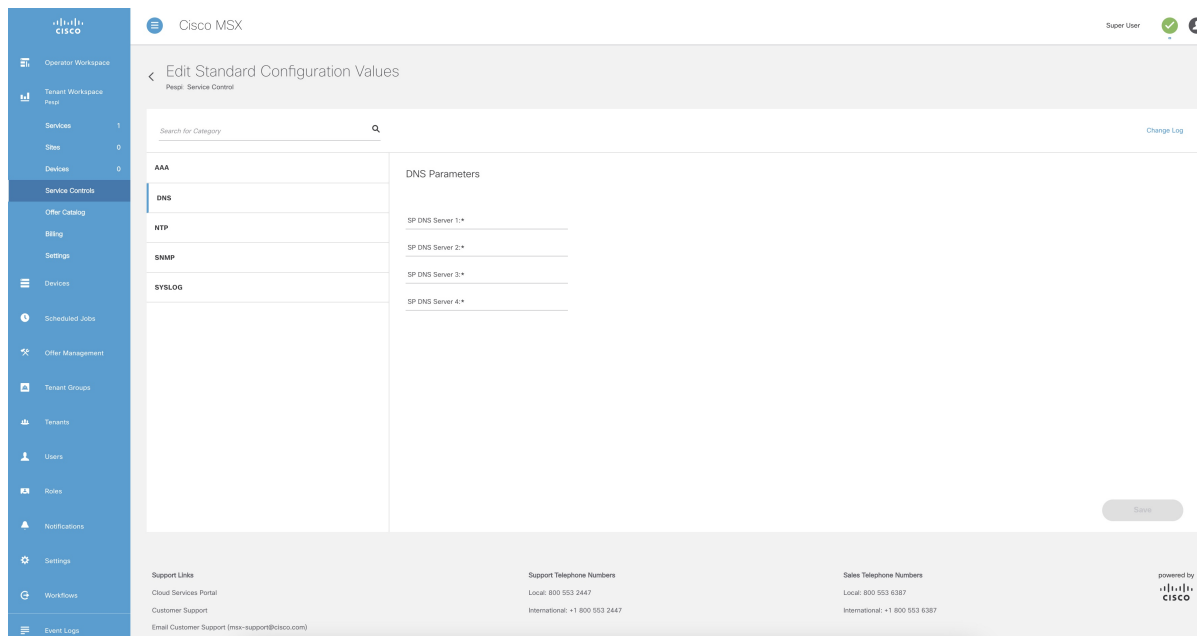
### Procedure

---

- Step 1** Log in to the Cisco MSX portal.

- Step 2** From the left pane, choose **Tenant Workspace > Service Controls > Edit Standard Configuration Values**. The **Edit Standard Configuration Values** window is displayed with the compliance categories.

**Figure 24: Edit Standard Configuration Values**



- Step 3** From the list, click a category you want to edit. You can also search for a category using the search box. The category parameters are displayed.
- Step 4** Edit the parameter values.
- Step 5** Click **Save**.

The parameter values are saved to the Standard Configuration.

## Adding Standard Configuration Category

A category is a set of configurations, per device type specified, which is to be compliant across all the configured device types. A category consists of templates that specify the device configuration (per device type) and optional parameters to provide values through the UI as opposed to hard-coded in the template. A combination of both is supported, as well as all template hard-coded values. The template configuration will be compared with the device types under compliance.

A category may have one or many device types supported. Only device types under compliance with a specified template configuration will be tested for compliance. It is possible to have different compliance checks per device type, by supplying different templates in a category. A category can also have just one template for a device type, and multiple categories can be defined, one per device type and compliance configuration.

To add a new category to Standard Configuration:



**Note** You need the following permissions to modify the Standard Configuration:

- Standard Configuration Manage
- Device Templates Manage

## Procedure

**Step 1** Log in to the Cisco MSX portal.

**Step 2** From the left pane, choose **Tenant Workspace > Settings > Define Standard Configuration**.

The **Define Standard Configuration** window is displayed.

**Figure 25: Define Standard Configuration Settings**

**Step 3** Click **New Category**.

**Step 4** In the **Category Name** field, enter a category name.

**Step 5** To create a template, click **COMPLIANCE TEMPLATE** tab.

**Step 6** From the **NED ID** drop-down list, choose a NED ID. The NED represents the device type you want the device template configuration to apply. You can specify multiple NEDs, each with their own specific device template or just a single NED and template.

**Step 7** Enter the configuration in the textbox provided.

**Step 8** Click **Generate Parameters** to generate parameters from the configuration you entered in the template textbox. Parameters that are not already included in the Parameters tab only will be generated.

**Step 9** You can add more than one template to a category. To add another template, click the plus (+) icon. Similarly, to delete a template, click the minus (-) icon.

**Note** To see the template that you already added, scroll down to the bottom of the screen.

**Step 10** To add parameters, click **PARAMETERS** tab and then click **Add Parameter**.

The fields to enter parameter details are displayed.

**Step 11** Enter the **Parameter Name**, **Parameter Description**, and **Parameter Label** in the fields displayed.

**Step 12** From the **Parameter Type** drop-down list, choose a parameter type.

**Step 13** Click the **Optional** radio button if the parameter is optional. Click the **Required** radio button if the parameter is mandatory. Click the **Read Only** radio button if the parameter is a read-only parameter. If you click **Read Only**, then enter the default value of the parameter. This value will be displayed as a read-only value when users access the standard configuration.

**Step 14** You can add more than one parameter to a category. To add another parameter, click the plus (+) icon. Similarly, to delete a parameter, click the minus (-) icon.

**Note** To see the parameter that you already added, scroll down to the bottom of the screen.

**Step 15** Click **Save Category**.

The new category you added will be displayed at the left pane.

**Note** You can specify only one template per NED type for a category.

---

## Deleting Standard Configuration Category

You can delete a category from the Standard Configuration.

To delete a category:

### Procedure

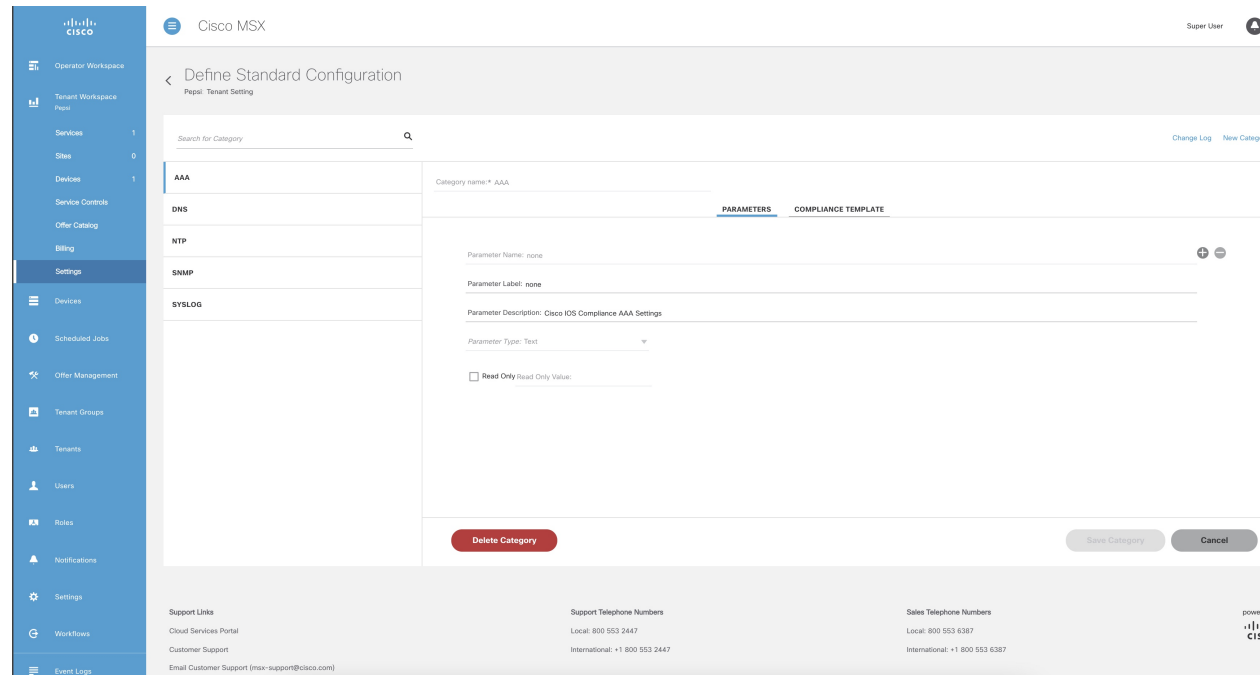
---

**Step 1** Log in to the Cisco MSX portal.

**Step 2** From the left pane, choose **Tenant Workspace > Settings > Define Standard Configuration**.

The **Define Standard Configuration** window is displayed.

Figure 26: Define Standard Configuration Settings



- Step 3** Click a category from the left pane.  
The category information is displayed.
- Step 4** Click **Delete Category**.  
The **Category Deletion** dialog box is displayed.
- Step 5** Click **Delete**.  
A message 'Standard Configuration Category Deleted Successfully' is displayed.

## Creating a ServiceNow Account

You can create a ServiceNow account for generating incident tickets for compliance drift and remediation actions.

For more information on integrating incident tracking system with Cisco MSX, see [Integrating Incident Tracking System with Cisco MSX](#)

To create a ServiceNow account:



**Note** You need the following permission to update ServiceNow settings:

- Incidents Manage

## Procedure

### Step 1

Log in to the Cisco MSX portal.

### Step 2

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

The **ServiceNow** window is displayed.

**Figure 27: ServiceNow Settings**

The screenshot displays the 'ServiceNow Settings' configuration page. The form includes the following fields and controls:

- Domain\***: Domain (text input)
- Client Id\***: Client Id (text input)
- Client Secret\***: Client Secret (password input with eye icon)
- User Name\***: User Name (text input)
- Password\***: Password (password input with eye icon)
- Caller**: Caller (text input)
- Proxy**: Proxy: <https://proxy.someservice.com/> (text input)

Buttons: 'Clear Credentials' and 'Save'.

Footer information:

- Support Links**: Cloud Services Portal, Customer Support, Email Customer Support (msx-support@cisco.com)
- Support Telephone Numbers**: Local: 800 553 2447, International: +1 800 553 2447
- Sales Telephone Numbers**: Local: 800 553 6387, International: +1 800 553 6387
- powered by CISCO

### Step 3

In the **Domain** field, enter the FQDN of your ServiceNow instance.

### Step 4

In the **Client Id** field, enter the client ID provided by ServiceNow.

### Step 5

In the **Client Secret** field, enter the client secret provided by ServiceNow.

### Step 6

In the **User Name** field, enter the username to log in to the ServiceNow instance.

### Step 7

In the **Password** field, enter the accompanying password for logging into the ServiceNow instance.

### Step 8

In the **Caller** field, enter the caller name. The Caller is the person contacting the Service Desk to get an incident registered. We recommend creating a ServiceNow user called 'MSX' (in ServiceNow) and providing 'MSX' as the Caller in the ServiceNow settings.

### Step 9

(Optional) In the **Proxy** field, enter a proxy URL.

### Step 10

Click **Save**.

A message 'ServiceNow Configuration Saved Successfully' is displayed.

**Note** You can delete the configuration by clicking the **Clear Credentials** button. Once you delete a ServiceNow account, MSX will clear the credentials from the system and disconnect access to ServiceNow. You will not be able to send incident tickets, receive service notifications, or any services from ServiceNow across your organization.



## Adding a Device to Compliance Monitoring

Compliance monitoring for devices ensures any deviation from the defined set of compliant values (the Standard Configuration) is detected and reported immediately to system administrators. The deviations can be auto-remediated or invoked by user interaction. A full audit log is available to view activities related to compliance deviation and remediations.

To add a device to compliance monitoring:

### Procedure

---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the list of devices.
- Step 3** Choose a device or devices from the list.
- Step 4** If you choose a single device, click the **ellipsis (...)** that is located far right on the same row and then choose **Add to Compliance Monitoring**. If you choose multiple devices, click the **ellipsis (...)** that is located far right on the column header, and then choose **Add to Compliance Monitoring**.  
The **Add Devices to Compliance Monitoring** dialog box is displayed. The dialog box provides information about how many devices are already monitored and how many will be added for monitoring.
- Step 5** Click **Add to Monitoring**.  
A confirmation message is displayed.
- Note** If you choose a device that is not eligible for compliance, you cannot add that device for compliance monitoring. Remove the unsupported devices from your selection and try again.
- Step 6** Click **Close**.
- 

## Removing a Device from Compliance Monitoring

You can remove a device or devices from compliance monitoring. After you remove a device from compliance monitoring, it will not be monitored for any changes that deviate from the Standard Configuration.

To remove a device from compliance monitoring:

### Procedure

---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the list of devices.

**Step 3** Choose a device or devices from the list.

**Step 4** If you choose a single device, click the **ellipsis (...)** that is located far right on the same row and then choose **Remove from Compliance Monitoring**. If you choose multiple devices, click the **ellipsis (...)** that is located far right above all devices, and then choose **Remove from Compliance Monitoring**.

The **Remove Device from Compliance Monitoring** dialog box is displayed. The dialog box provides information about how many devices will be removed from monitoring.

**Step 5** Click **Remove from Monitoring**.

A confirmation message is displayed.

**Step 6** Click **Close**.

## Configuring the Compliance for Devices

You can configure the compliance remediation settings of devices. You can either choose automatic remediation or user initiated remediation.

To configure compliance settings:

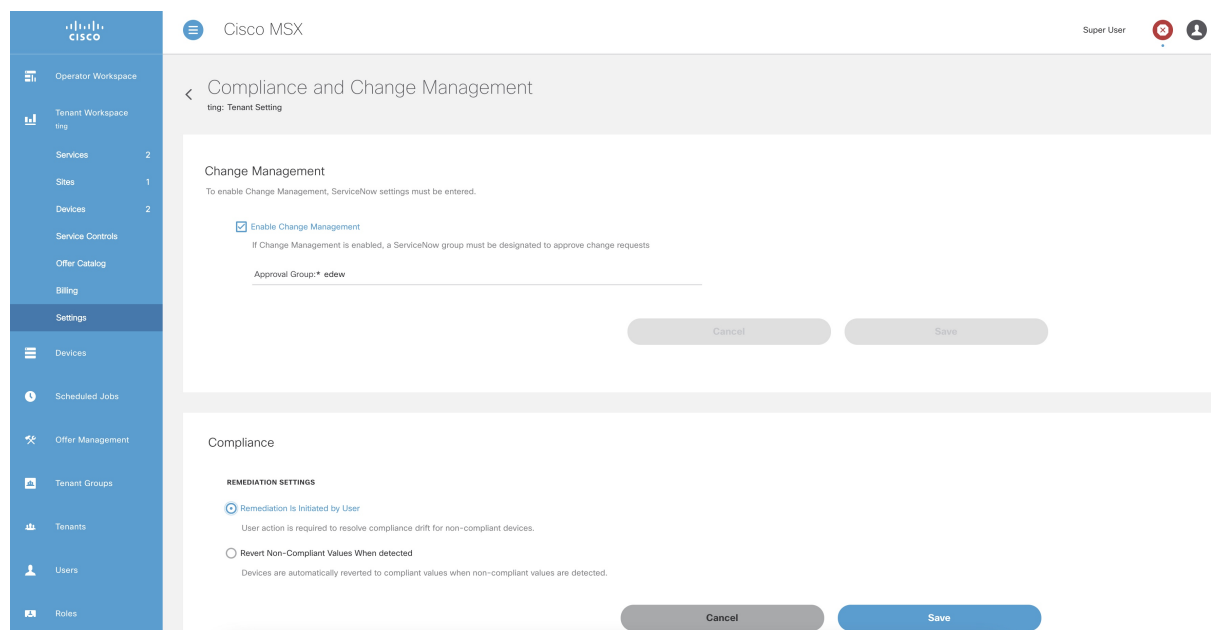
### Procedure

**Step 1** Log in to the Cisco MSX portal.

**Step 2** From the left pane, choose **Tenant Workspace > Settings > Compliance and Change Management**.

The **Compliance and Change Management** window is displayed.

**Figure 28: Compliance and Change Management**



- Step 3** In the **REMEDICATION SETTINGS** section, click the **Remediation is Initiated by User** radio button if user initiation is required for remediation. If you choose this option, the values will not be reverted to standard values until you initiate it from your side.
- a) Click **Save**.
- A message 'Compliance Settings were Saved Successfully' is displayed.
- Step 4** Click the **Revert Non-compliance Values When Detected** radio button if you want automatic remediation. If you choose this option, devices are automatically reverted to standard configuration values when non-compliant values are detected. You will be notified of the changes.
- a) Click **Save**.
- A message 'Compliance Settings were Saved Successfully' is displayed.
- 

## Remediating Non-compliant Values on a Device

Deviations on a device from the Standard Configuration can be remediated in two ways. The first option is to revert the changes on the device to the Standard Configuration values. The second option is to accept the non-compliance values on the device. This action will track the exception for this device and not warn again if the device is checked again for deviation drift. Changing the Standard Configuration value will negate any exceptions stored for a device against the changed Standard Configuration value.

To remediate non-compliance values:

### Procedure

---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.
- The **Devices** tile is displayed with the list of devices.
- Step 3** From the list, click a device.
- The device metric page lists the device information.
- Step 4** From the **Compliance** section, click **Remediate**.
- The **Remediate Non-Compliant Values** window is displayed. From the remediation options, you can either choose **Revert to Standard Configuration Values** or **Accept Non-compliant Values**.
- Step 5** Click **Revert to Standard Configuration Values** if you want to revert the values to standard configuration.
- a) Click **Next**.
- The **Scheduling Options** window is displayed. You can remediate now or schedule the remediation for a later date.
- b) Click **Remediate Now** to remediate the values immediately. Click **Next**.
- Review the remediation details and click **Next**. The remediation process initiates and a message 'Remediation Initiated' is displayed.

- c) Click **Schedule Remediation** to schedule the remediation for a later date.
- d) If you click **Schedule Remediation**, you can either schedule a new job or add to an existing job.
- e) To schedule a new job, click the **New Schedule Job** radio button.

In the **Schedule Job Name** field, enter a name for the schedule job.

In the **Date and Time** field, choose a date and time.

- f) To add to an existing job, click the **Add to Existing Scheduled Job** radio button.

From the **Schedule Job** drop-down list, choose an existing schedule job.

- g) Click **Next**.

The **Review Remediation** window is displayed.

- h) Review the remediation details and click **Next**.

The remediation process initiates and a message 'Remediation Initiated' is displayed.

- i) Click **Done**.

**Step 6** Click **Accept Non-compliant Values** if you want to accept the values as compliant despite their differences with the standard configurations.

- a) Click **Next**.

The **Review Remediation** window is displayed.

- b) Review the remediation details and click **Next**.

The remediation process initiates and a message 'Remediation Initiated' is displayed.

- c) Click **Done**.
- 

## Configuring Change Management Approvals

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

For more information on configuring change management approvals, see 'Configuring Change Management Approvals' in [Cisco MSX Administration](#).

## Updating Monitored Devices with Standard Configuration

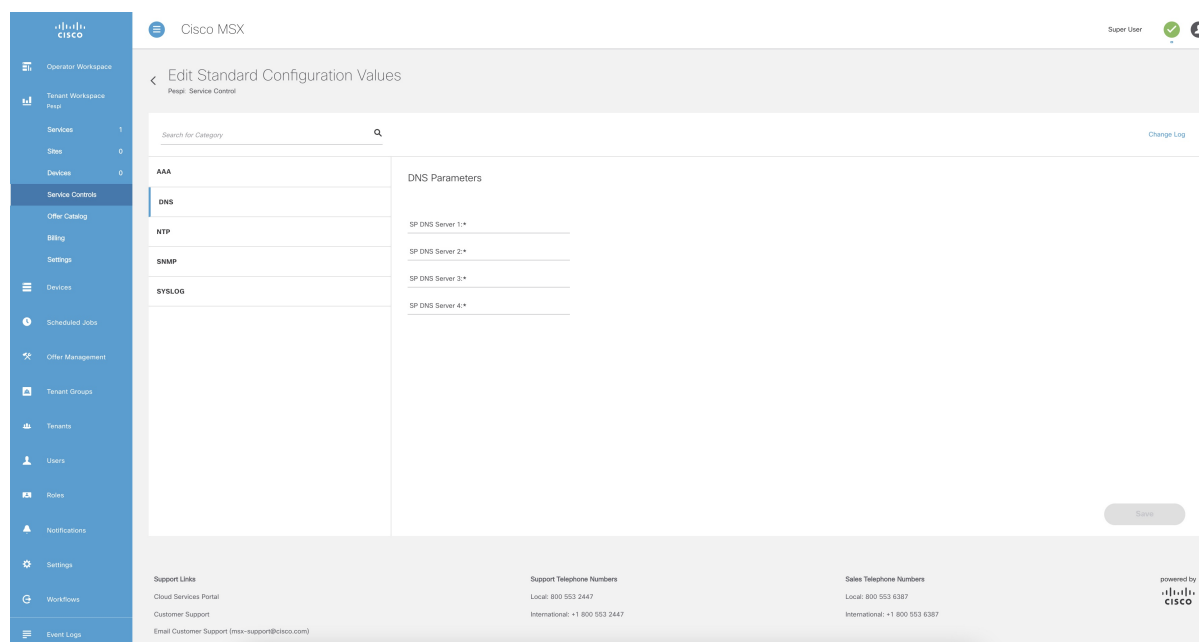
You can update all the monitored devices with standard configuration.

To push standard configuration to monitored devices:

## Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Service Controls > Edit Standard Configuration Values**. The **Edit Standard Configuration Values** window is displayed.

**Figure 29: Edit Standard Configuration Values**



- Step 3** Click **Update Monitored Devices**. The **Push Standard Config to Monitored Devices** window is displayed.
- Step 4** Click **Update Devices**. A message 'Standard Configuration Saved Successfully' is displayed.

## Viewing Device Vulnerabilities

The Cisco MSX platform now detects and reports the software compliance vulnerabilities for both the Cisco devices and third-party software devices. You can see the vulnerability details in the Device Metric page.

For more information on how vulnerabilities are detected, see [Managing the Device Compliance Vulnerability Using API](#).

To view the device vulnerabilities:

### Procedure

---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the list of devices.
- Step 3** From the list, click a device.  
The device metric page lists the device information. Go to **Vulnerabilities** tile to see the device vulnerabilities.
- 

## Viewing Monitored Devices

You can view the devices under compliance monitoring. The device listing page allows you to filter the devices based on device compliance. The following filtering options are available:

- **All**: Displays all the devices.
- **Non-compliant**: Displays all non-compliant devices.
- **Monitored**: Displays all devices that are monitored for compliance.
- **Eligible**: Displays all the devices that are eligible for compliance.

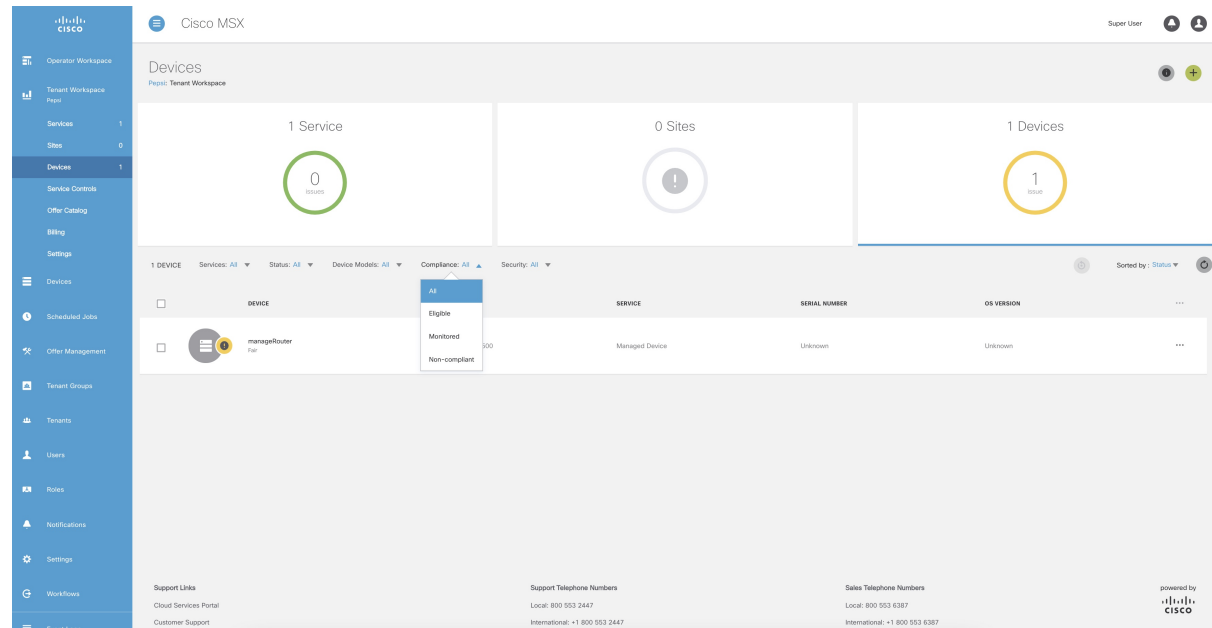
To view all the devices under compliance monitoring:

### Procedure

---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the list of devices.

Figure 30: Viewing Monitored Devices



**Step 3** To filter the devices based on a compliance criteria, choose a filtering option from the **Compliance** drop-down list.

The list of devices under compliance monitor is displayed.

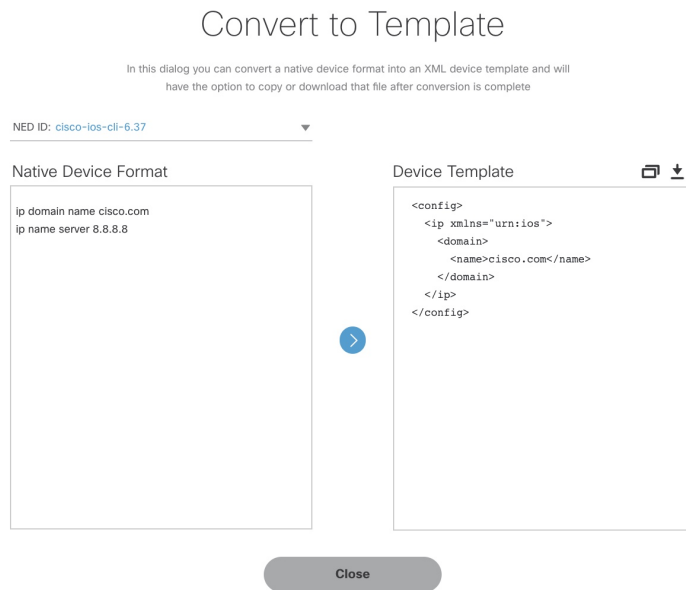
## Converting Device Configuration to Device Template

The Cisco MSX platform allows you to convert both Cisco and non-Cisco native device configuration formats to device template formats. You can import these converted templates into the centralized template service, and any services like MD can use those templates. This feature also allows you to copy or download the converted configuration.

To convert device configuration to device template:

### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Settings > Template Management > Device Templates**.  
The **Templates** window is displayed.
- Step 3** In the **Select A Configurational Template** section, click the **ellipsis (...)** and choose **CLI to Template** from the menu.  
The **Convert Device Configuration to Template** window is displayed.



**Figure 31: Convert to Template**

- Step 4** From the **NED IDs** drop-down list, choose a NED ID.
- Step 5** In the **Native Device Format** pane, enter the native device configuration.
- Step 6** Click **Convert**.  
The **Device Template** pane displays the converted configuration in XML format.
- Step 7** Click the **Copy** icon to copy the configuration to clipboard.
- Step 8** Click the **Download** icon to download the configuration file.
- Step 9** Click **Close**.





## CHAPTER 8

# Monitoring Managed Device

---

This chapter provides information about how to monitor various managed device services.

This chapter contains the following topics:

- [Monitoring Managed Device Service Status on the Cisco MSX GUI, on page 67](#)
- [Understanding Managed Device Life Cycle Statuses, on page 70](#)
- [Viewing Site Metrics, on page 71](#)
- [Viewing Device Metrics, on page 72](#)

## Monitoring Managed Device Service Status on the Cisco MSX GUI

Cisco MSX 4.0 uses tenant-centric GUI for the Managed Device service pack. The tenant-centric portal displays both the Operator Workspace and Tenant Workspace.

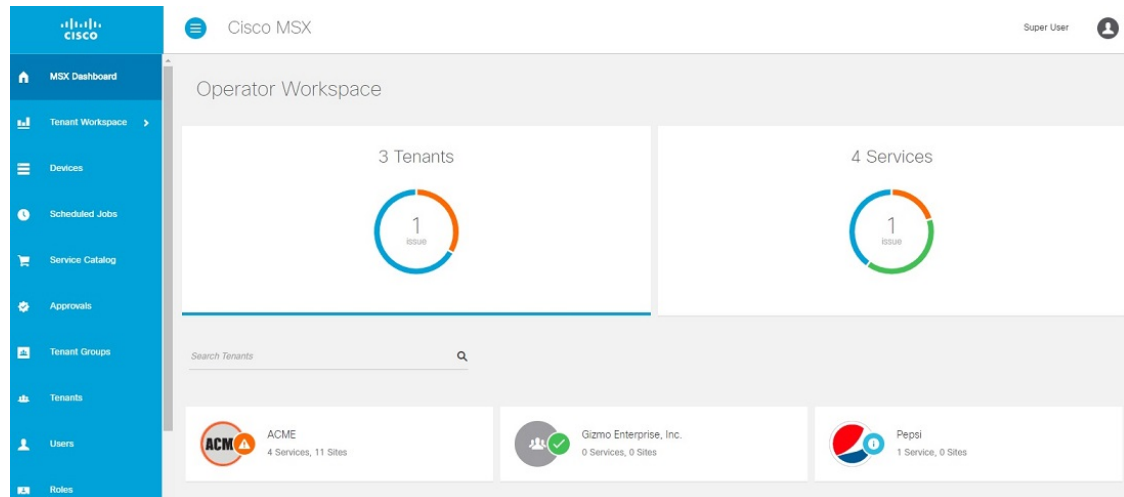
Tenant-centric GUI has the following workspaces:

- Operator workspace—Which lists all the tenants and the services these tenants have subscribed to.
- Tenant Workspace—Which allows tenants to access information related to their subscribed services.

### Operator Workspace

The Operator Workspace has dashlets such as Tenants and Services. The tenant-centric portal is role-based and is accessible by both tenants and operators. For more information, see [Managing Specific User Roles in Managed Device](#).

Figure 32: Operator Workspace



**Tenants**—Displays all the existing tenants for the logged in user.

**Services**—Displays all the service packs that are provisioned by tenants.

### Tenant Workspace

The following are the menus that are available in the Tenant Workspace:

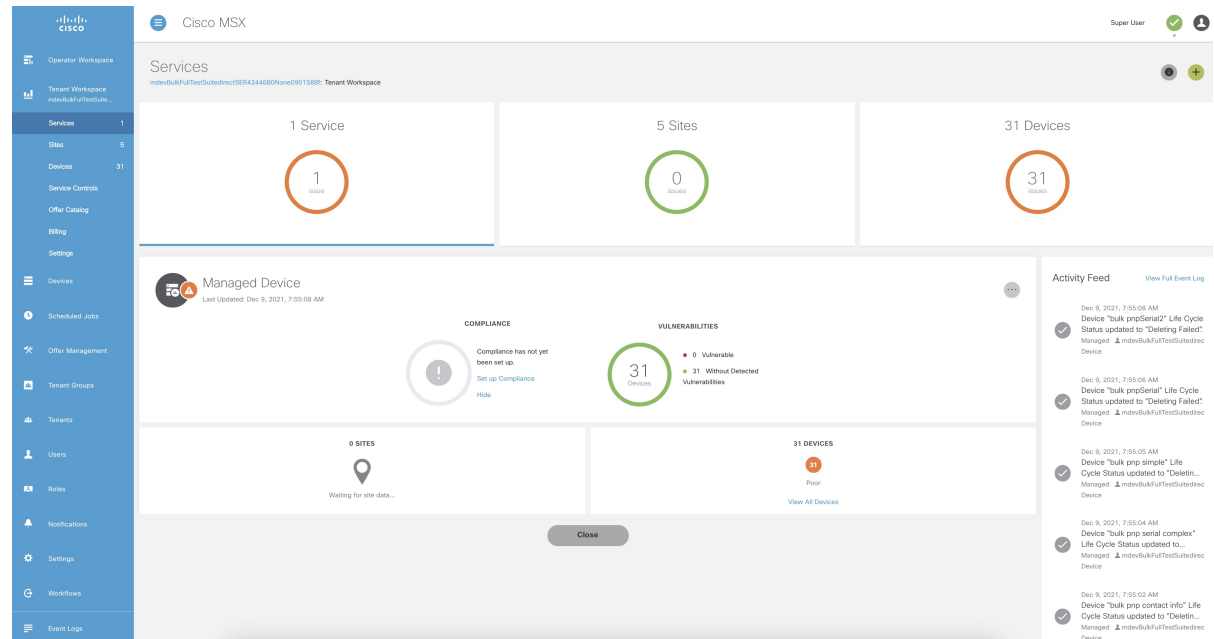
- **Services**— Display the status of all services subscribed by a tenant.
- **Sites**—Display the sites a specific tenant is associated with and the overall health status of the sites.
- **Devices**—Display devices available at all sites for a particular tenant.
- **Service Controls**—Display the custom service controls that are used by the services.
- **Offer Catalog**—Displays existing subscriptions and allows subscribing to new services.

Select the desired tenant to view the subscribed Services, Sites, and Status of the respective tenant. For more information, see [Monitoring Managed Device Service from Tenant Workspace](#).

## Monitoring Managed Device Service from Tenant Workspace

The tenant-centric portal displays the status of all the Services, Sites, and Devices of the selected tenant.

Figure 33: Tenant Workspace



## Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Operator Workspace**.  
The **Operator Workspace** home page appears displaying all the Tenants and Services.
- Step 3** Select the required tenant.  
The **Services** home page of the Tenant Workspace appears with the list of all the provisioned service pack. Displays the Services, Sites, and Devices of the selected tenant.
- Note** From the **Services** home page of the Tenant Workspace, you can monitor the status of the Cisco MSX Enterprise Access, Managed Device, and other service packs.
- Step 4** From the **Tenant Workspace** main menu, choose **Sites** to monitor the status of the sites.  
The map view appears with all the available sites of the selected tenant. Hover the mouse pointer over the site to know the status.
- Step 5** From the **Tenant workspace** main menu, choose **Devices** to monitor the status of the devices.  
The list view of all the available devices of the selected tenant appears, displaying the information such as Devices, Services, Serial Number, IP Address, Model, and Configuration.
- From the list view, select a device to view device summary.  
**Note** In the main menu, click **Tenant Workspace** to return to the tenant-centric portal.
  - From the list view, click the **ellipsis (...)** that is located far right on the same row of the selected device.

- Step 6** From the **Tenant Workspace** main menu, choose **Service Controls** to view the custom service controls that are used by the services.
- Step 7** From the **Tenant Workspace** main menu, choose **Offer Catalog** to view the existing subscriptions and subscribe to new services.

## Understanding Managed Device Life Cycle Statuses

The Managed Device service pack provides drill-down views of the operational state of the sites.

To view the device status:

### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The **Devices** tile is displayed with the available devices.
- Step 3** Choose a device from the list.  
The device information is displayed. The table below shows the color indicators to describe the site status:

**Table 12: Color Indicators for Several Site Status**

Serial Number	Status	Color Indicator	Notes
1.	Up	Green	Service is Up at this site, device is reachable and metrics can be viewed.
2.	Down	Red	Service is Down at this site and device may not be reachable to view any metrics information.
3.	Onboarding	Turquoise	<ul style="list-style-type: none"> <li>• Waiting for the ZTP device to call-home to MSX.</li> <li>• Initiating connection from MSX for the Direct connection onboarding method.</li> </ul>
4.	Onboarded	Blue	Device has been onboarded to MSX and ready for applying the configuration template.
5.	Failed	Orange	Device onboarding to MSX has failed and will require the operator to debug and restore the device.

Serial Number	Status	Color Indicator	Notes
6.	Provisioning	Purple	Configuration template is being applied to the device.
7.	Provisioned	Blue	Configuration template has been successfully applied to the device.
8.	Deleting	Purple	Site deletion is in progress. This could include restoring the device configuration to Day-1 upon successful deletion.
9.	Unregistered	Yellow	Initially, the site is created without providing a device serial number. Therefore, the device exists in an unregistered state.  After adding the device serial number, the device transitions from the unregistered state to UP state.

## Viewing Site Metrics

Cisco MSX Managed Device service pack provides the capability to monitor the site status.

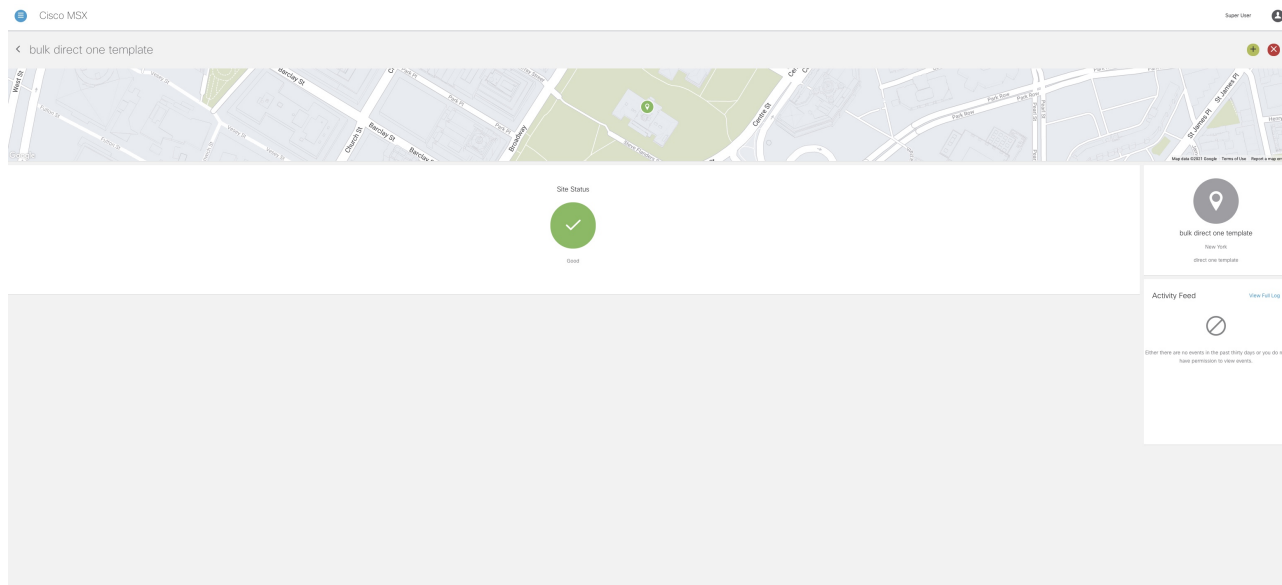
When the third-party device is on-boarded to Managed Device, device metrics are automatically calculated based on the device model.

To view the site metrics:

### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Sites**.  
The list of sites associated with a tenant is displayed.
- Step 3** Select any one of the sites to view the detailed site status.  
This page lists all the site metrics along with status of the selected site.  
Under the **Managed Device** section of the page, you can view the list of Meraki networks that were assigned to this site.  
For information on adding Meraki network, see [Creating Networks](#).

Figure 34: Site Metrics



## Viewing Device Metrics

Cisco MSX Managed Device service pack provides the capability to monitor the device status.

When the third-party device is on-boarded to Managed Device, device metrics are automatically calculated based on the device model.

To view the device metrics:

### Procedure

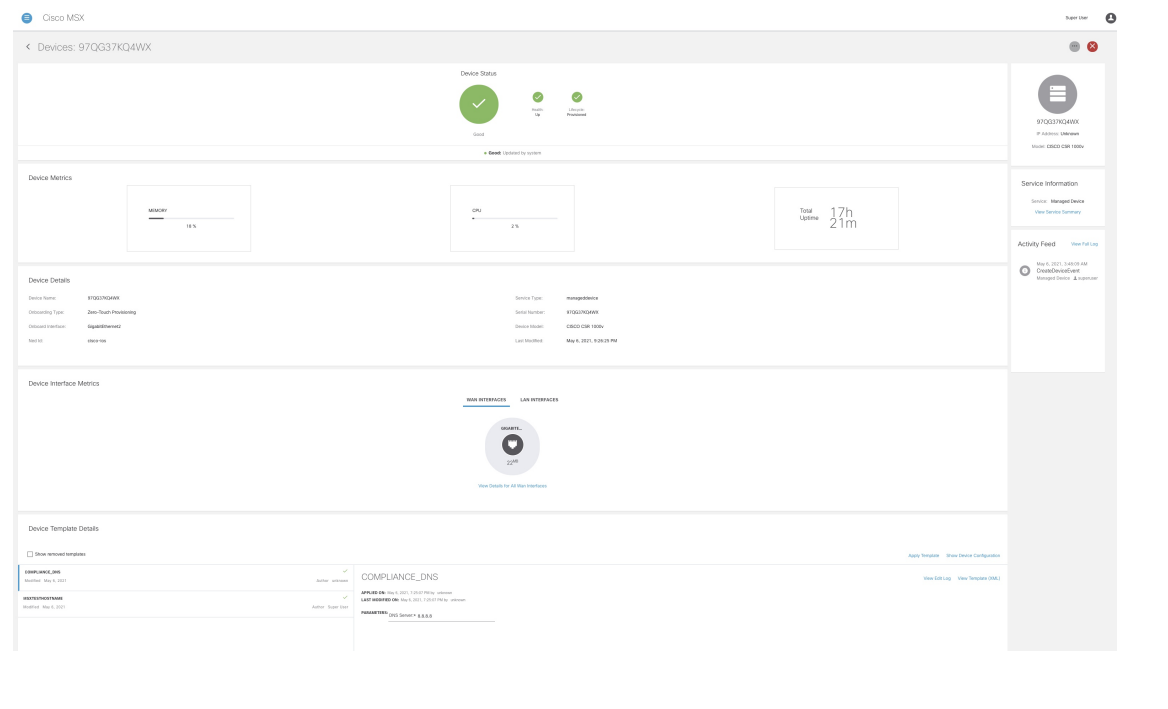
- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.  
The list of devices associated with a tenant is displayed.
- Step 3** Select a device from the list.  
The status of the selected device and other metrics are displayed.

**Note** For Meraki devices, you will see additional details such as Network ID, Serial Number, and Device Uplink Details. The following table lists the mapping between the Meraki status and MSX overall device status that is displayed on the MSX portal:

Meraki Status	MSX Device Status
Offline	Down
Online	Up
Alerting	Down
Dormant	Down
Others	Unknown

For more information on Meraki status, see *Cisco Meraki documentation*.

**Figure 35: Device Metrics**









## CHAPTER 9

# Managing Meraki

Using Cisco MSX Managed Devices services, operators can manage organizations (attach, edit, or delete) and create networks comprising Meraki devices and services. An organization implies Meraki networks managed by one or more accounts. For deploying a Meraki solution, it is essential to consider an organizational structure that will use this solution. It is recommended to have one organization per customer or one organization per service. For more information on when to use multiple organizations, see the section, 'Building a Scalable Meraki Solution' in *Cisco Meraki* documentation.

The following are the Meraki wireless and combined device types currently supported on Cisco MSX:

- **MX -Security and SD-WAN:** The Meraki MX is an enterprise security & also equipped with SD-WAN capabilities that enable administrators to maximize network resiliency and bandwidth efficiency. The following are the MX devices supported on MSX.
  - MX64, MX65, MX67, and MX68 required for a small branch setup
  - MX84 and MX100 required for a medium branch setup
  - MX250 and MX450 required for a large branch/campus setup
  - vMX device types for virtual devices
- **MR- Wireless LAN:** [MR device types](#) for cloud-managed WLAN access points.
- **MS - Switches:** [MS device types](#) are cloud-managed access and aggregation switches series of access switches. Using these switches, thousands of switch ports can be configured and monitored instantly, over the web.
- [Attaching Organizations, on page 76](#)
- [Editing or Detaching Organizations, on page 77](#)
- [Creating Networks, on page 79](#)
- [Viewing Meraki Networks for a Site, on page 82](#)
- [Assigning Meraki Network to a Site, on page 83](#)
- [Synchronizing Networks and its Devices, on page 84](#)
- [Editing or Deleting a Network, on page 84](#)
- [Configuring Switch Ports, on page 86](#)

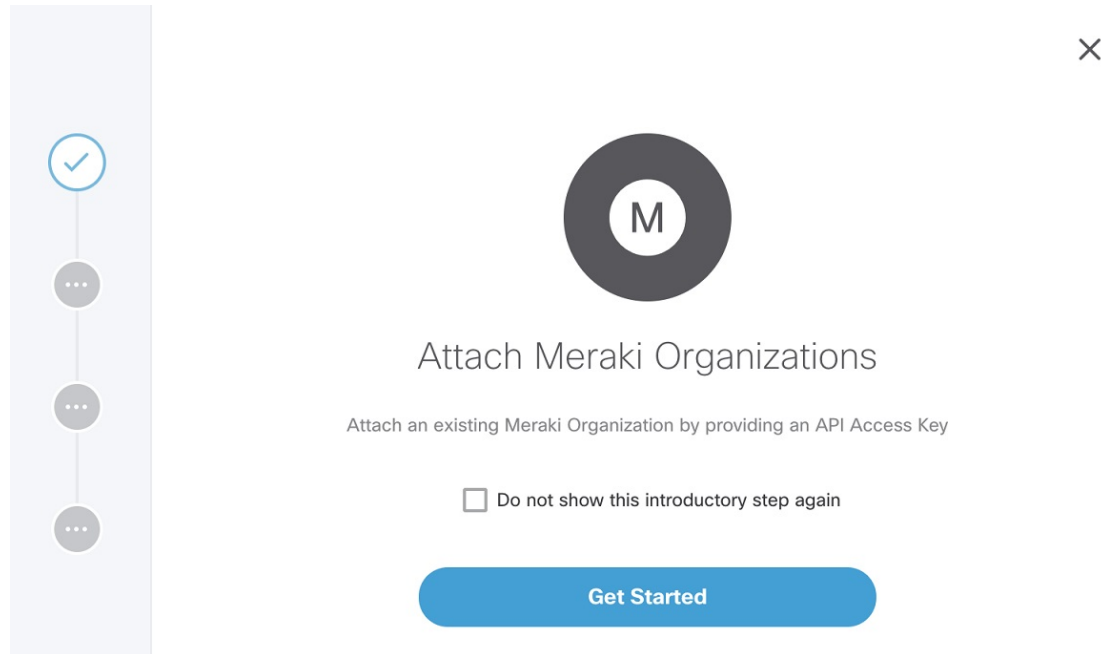
# Attaching Organizations

You can associate one or more organizations to the tenant's control plane. Organization implies a collection of networks that are part of a single organizational entity. These networks, in turn, can have multiple devices.

To attach organizations in MSX:

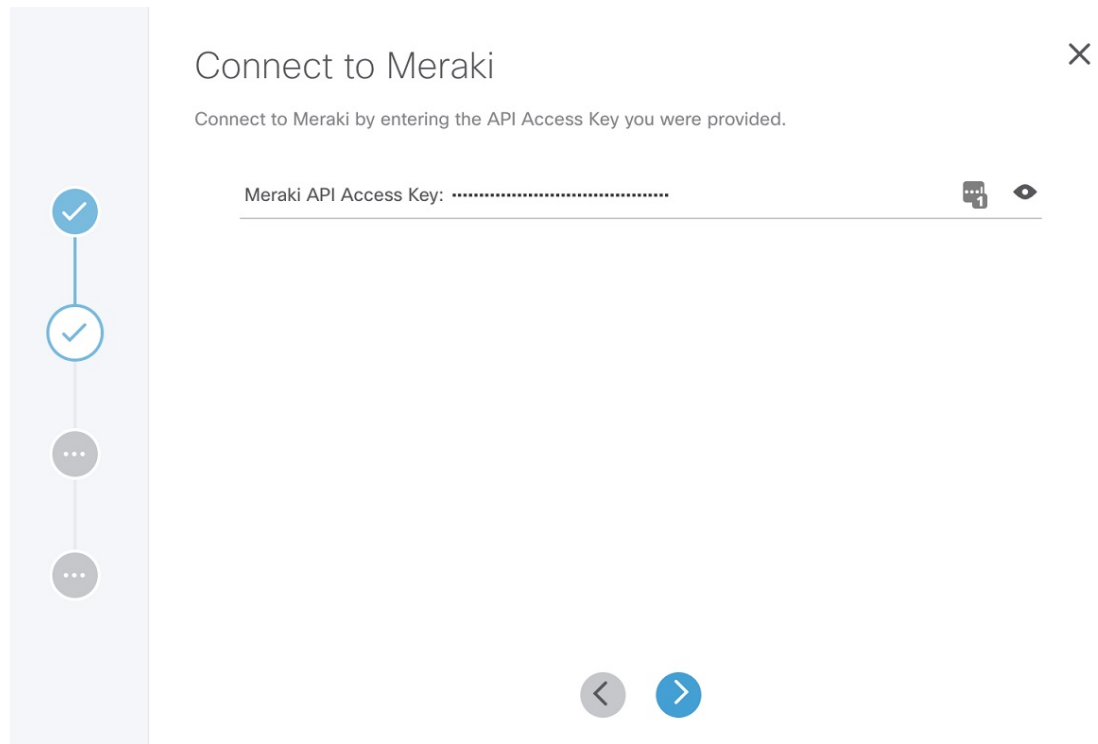
## Procedure

- Step 1** Log in to the Cisco MSX portal using your credential.
- Step 2** From the left pane, choose **Tenant Workspace > Settings > Meraki Organizations**.  
The **Meraki Organization** page is displayed.
- Step 3** Click **Attach Organizations**.  
The Attach Meraki Organizations dialog box is displayed.



- Step 4** Click **Get Started**.
- Step 5** Enter the Meraki API Access Key on the **Connect to Meraki** page.  
Use the eye icon to view and validate the API key.

**Note** You can get the Meraki access key by logging in to the Meraki dashboard. Click **User > My Profile > Generate New API Access Key** to generate a new key.



**Step 6** Click > to move to the next page.

**Step 7** On the **Select Meraki Organization** page, select up to five organizations to attach to your Meraki control plane. The drop-down lists the available organizations for the access key you had provided in the previous step. In case you want to attach more than five organizations, you can do so at the end of this process by selecting **Attach Another Organization** option.

**Step 8** Click > to move to the next window and initiate the attaching process. You can close the window or click **Attach Another Organization** to add more organizations to the control plane.

All the organizations added to the tenant's control plane is displayed in **Tenant Workspace > Settings > Meraki Organizations**.

## Editing or Detaching Organizations

To edit or detach an attached organization in MSX:

### Procedure

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

**Step 2** From the left pane, choose **Tenant Workspace > Settings > Meraki Organizations**.

The **Meraki Organization** page is displayed with the list of organizations that were added to the tenant's control plane.

**Step 3** Select a row and click on the ellipsis (...) and choose **Edit Access Key** to edit the Organization details that were provided while attaching the organization to your tenant's control plane.

The screenshot shows a table titled "Meraki Organizations" with a "+" icon in the top right corner. The table has four columns: STATUS, ORGANIZATION NAME, ORGANIZATION ID, and LAST SYNC. There are two rows of data, both with a green dot and "Up" in the STATUS column. The first row has "NYC QUEENS 2" as the ORGANIZATION NAME and "634444597505821823" as the ORGANIZATION ID. The second row has "NYC QUEENS 1" as the ORGANIZATION NAME and "634444597505821822" as the ORGANIZATION ID. An ellipsis (...) is visible at the end of the second row, and a dropdown menu is open, showing options: Detach, Edit Access Key (highlighted in blue), Sync with Meraki, and View Organization in Meraki.

**Step 4** On the **Edit Access Key** dialog box, click **Meraki API Access Key** field to clear the previous key and enter a new key and click **Save**. Click **Cancel** to retain the old key.

The screenshot shows a dialog box titled "Edit Access Key". Below the title, there is a message: "API Access Key has been previously saved. Once the current key is clicked on, it will be cleared and a new one can be entered. Review your organization(s) after changing the user key." Below this message, there is a text input field labeled "Meraki API Access Key:" followed by a series of dots representing a masked key. To the right of the input field is a small icon of a speech bubble with the number "1" inside. At the bottom of the dialog box, there are two buttons: "Cancel" and "Save".

**Detaching Organizations:**

If you want to detach or disassociate an organization from a tenants control plane, click on the ellipsis (...) and choose **Detach**.

The screenshot shows the same "Meraki Organizations" table as in Step 3. In this instance, the dropdown menu is open for the first row (NYC QUEENS 2), and the "Detach" option is highlighted in blue. The other options in the menu are "Edit Access Key", "Sync with Meraki", and "View Organization in Meraki".

# Creating Networks

A network is a logical container of multiple devices that can be created for a site and can be a combination of devices.

## Before you begin

Make sure you have an organization attached within MSX. For more information, see [Attaching Organizations](#).

## Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Sites**.  
The list of sites associated with a tenant is displayed.
- Step 3** Select any one of the sites to view the detailed site status.  
This page lists all the site metrics along with status of the selected site.
- Step 4** Under the **Managed Device** section on the page, click + > **Create New Meraki Networks** to associate a new network to the selected site.

The screenshot displays the 'Site Status' page for 'PS Queens School 2' (NY-27, Queens, NY, USA). The site status is 'Good'. Below the status, there is a 'Managed Device' section with a table of devices. A dropdown menu is open over the table, showing options to 'Create New Meraki Network' and 'Assign Meraki Network'. The 'Activity Feed' on the right shows recent events, including the creation of the site and the addition of devices.

NETWORK NAME	NETWORK TYPE	ORGANIZATION	TAGS
Houston-Branch	appliance, switch	MSX-SDWAN	12214_Harmony_Ha ...

The **Create New Meraki Network** wizard is displayed to set up networks to manage multiple devices.

- Step 5** Click **Get Started**.  
The **Meraki Network Information** dialog box is displayed.
- Step 6** Enter the following details on the **Meraki Network Information** page.
- **Network name:** Specify a name for your new network.
  - **Organization:** Choose the organization that you want to associate your network to from the drop-down list.

- **Meraki Network Tags:** This field displays all the tags currently available in Meraki. You can also add new tags. Type a new tag and click on the **Add New** option that appears as you type a new tag to save the new tag.

Meraki Network Information ✕

Select a logical Meraki Organization for your new network. Organizations are treated independently with its own licensing, inventory, users, and configurations. The optional network tags are Meraki specific and can help group and identify networks.

Network Name:\* United Co ?

Organization:\* NYC MANHATTAN 1 ▼

**MERAKI NETWORK TAGS**

02 ✕ geo ▼

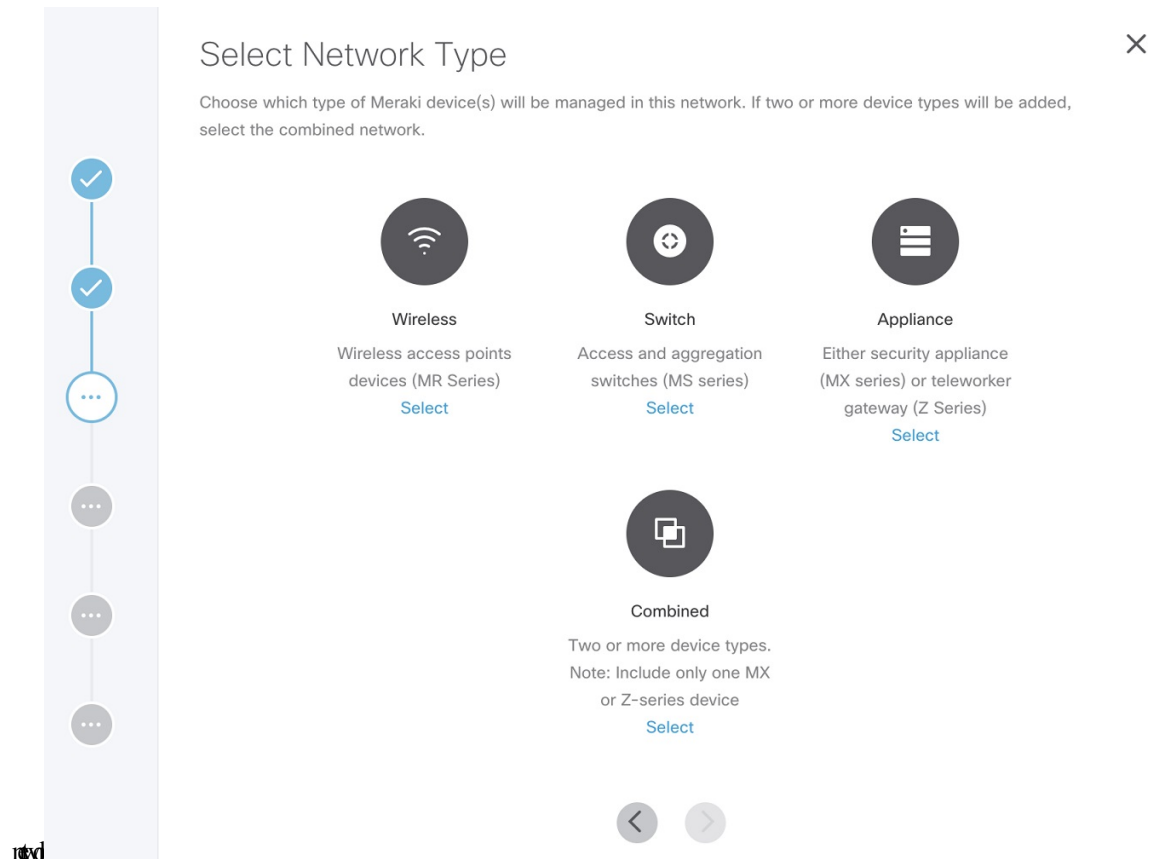
[Add new: geo](#)

< >

**Step 7** Click > to move to the **Select Network Type** page.

**Step 8**

In the **Select Network Type** page, choose the type of Meraki devices (Wireless, Switch, Appliance) that will be managed in this new network. Choose the **Combined** option to add different device types to your

**Step 9**

Click > to move to the **Select Initial Configuration for Network** page.

**Step 10**

Set up a network. Choose from one of the following options to setup the network configurations:

- **No Configurations:** Create a network without any template configurations, but later you can attach a configuration template to this network.
- **Clone from Network:** Create a network with configuration settings copied from an existing network to a new network. On the **Select Meraki Network to Clone** page, select a network from the list of available networks from where the configuration settings must be copied. The network list shown depends on the network type you chose in Step 8. The network list can be narrowed down by searching with specific tags in the **Meraki Network Tags** field. After cloning, any configuration changes made to the source network are not inherited into the new network.
- **Clone from Template:** Create a network with configuration copied from an existing template into a new network. On the **Select Meraki Template to Clone** page, select the template from the **Template Name** drop-down list from where the configuration must be copied. The options shown in the drop-down depends on the network type you chose in Step 8. After cloning, any configuration changes made to the source network are not inherited into the new network.
- **Attach to Template:** Create a network and then associate it to an existing template. On the **Select Meraki Template to Attach** page, select a template from the **Template Name** drop-down list to which the network can be attached. The options shown in the drop-down depends on the network type you chose

in Step 8. If you use this option, any changes in the source template are automatically applied to all the associated networks.

**Step 11** Click > to move to the **Review and Submit** page.

**Step 12** Review the details and click **Submit** to complete the process.

## Viewing Meraki Networks for a Site

Cisco MSX Managed Device service pack provides the capability to monitor the site status and the networks associated to the sites.

To view the site details:

### Procedure

**Step 1** Log in to the Cisco MSX portal.



- Step 2** From the left pane, choose **Tenant Workspace > Sites**.  
The list of sites associated with a tenant is displayed.
- Step 3** Select any one of the sites to view the detailed site status.  
This page lists all the site metrics along with status of the selected site.  
Under the **Managed Device** section of the page, you can view the list of Meraki network assigned to this site.
- 

## Assigning Meraki Network to a Site

A Meraki network must be assigned to a site in the following cases:

- When a control plane is attached, and you want to plot network to different site locations.
- When a site is deleted, the network gets unmapped, and you want to associate this network with a site.
- When you want to attach Meraki devices to a site.



**Note** You can assign up to 5 networks to a site that can be managed separately.

---

Using this procedure, you can assign networks to a single organization at a time. However, if you wish to attach sites to more organizations, you must repeat this procedure. To attach a network to a site:

### Before you begin

Associate one or more organizations to the tenant's control plane. For more information, see [Attaching Organizations](#).

### Procedure

---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Sites**.  
The list of sites associated with a tenant is displayed.
- Step 3** Select any one of the sites to view the detailed site status.  
This page lists all the site metrics along with status of the selected site.
- Step 4** Under the Managed Device section on the page, click + > **Assign Meraki Network** to assign networks already available in a Meraki organization to a selected site.  
The **Assign Meraki Network to Site** wizard is displayed to associate networks to a site.
- Step 5** Click **Get Started**.  
The **Select Meraki Network** dialog box is displayed.

- Step 6** Select an organization to which the network needs to be assigned, and select one or more available networks for a site. Narrow down the networks using network name and network type.
- Step 7** Click > to move to the **Review and Submit** page.
- Step 8** Review the details and click **Submit** to complete the process.

Under the **Managed Device** section of the page, you can view the list of Meraki network assigned to the site. The **Tenant Workspace > Site** tab will also list the devices assigned for a Meraki network.

#### Unassigning a Network from a Site

You can use the unassign option to disassociate a network and later associate it to another site.

From the Managed Device section of the **Site Details** page, select a Meraki network row, click on the ellipsis (...), and choose **Unassign Network**. This will remove the networks and devices attached to the site.

## Synchronizing Networks and its Devices

In MSX, you can synchroninze Meraki details into MSX at:

- Organization-level: Use the **Sync with Meraki** option in **Tenant > Setting > Organization** to sync all networks and devices available within an Organization.
- Network-level: Using the APIs in the **Meraki-Control-Plane-Controller** section of **Merakiservice** APIs, you can do the following:
  - Synchronize only a list of networks and the devices in the network. Provide the list of network IDs for which the synchronization needs to be performed. Use the POST `/merkai/api/v1/controlplanes/{controlPlaneID}/synchronize` for the synchronization.
  - Schedule a synchynchronization task



**Note** Only users with Meraki Synchronization (Manage) permission under Meraki Service section can perform the synchronization within MSX.

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

## Editing or Deleting a Network

To edit and delete a Meraki network:

#### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Sites**.

The list of sites associated with a tenant is displayed.

**Step 3** Select any one of the sites to view the detailed site status.

This page lists all the site metrics along with status of the selected site.

Under the **Managed Device** section of the page, you can view the list of Meraki network assigned to this site.

**Step 4** Select a network, and click on the ellipsis (...) and select **Edit Network** to edit the network details. You can add or edit the existing network tags, and also change template for a network using the **Edit Meraki Network** dialog box.

The screenshot shows a 'Managed Device' status of 'Good'. Below it is a table with columns: NETWORK NAME, NETWORK TYPE, ORGANIZATION, and TAGS. A row is visible for 'Houston-Branch' with type 'appliance, switch' and organization 'MSX-SDWAN'. The TAGS column shows '12214\_Harmony\_Ha' and an ellipsis menu. The dropdown menu is open, showing options: Edit Network, Unassign Network, Delete Network, and View Network in Meraki.

## Edit Meraki Network

Meraki Network Name: United Co

Network Type: wireless

Organization: NYC MANHATTAN 1

Meraki Network Tags: 02 x geo x

---

NETWORK CONFIGURATION

Template Name: No Configuration

Cancel Save

### Deleting the Network:

Click on the ellipsis (...) and select **Delete** to delete the selected network.

---

## Configuring Switch Ports

Cisco MSX provides the ability to create configuration and deploy them to multiple switch ports using the pre-defined templates that are available within the Cisco MSX.

**Note**

- Currently, this functionality is available only for Switch Ports for Meraki.
  - Only user roles with **Switch Configuration (Manage)** permission can manage the switch port configurations from MSX. Users with the **(View)** permission can only view the configurations.
- 

## Creating Switch Port Configuration

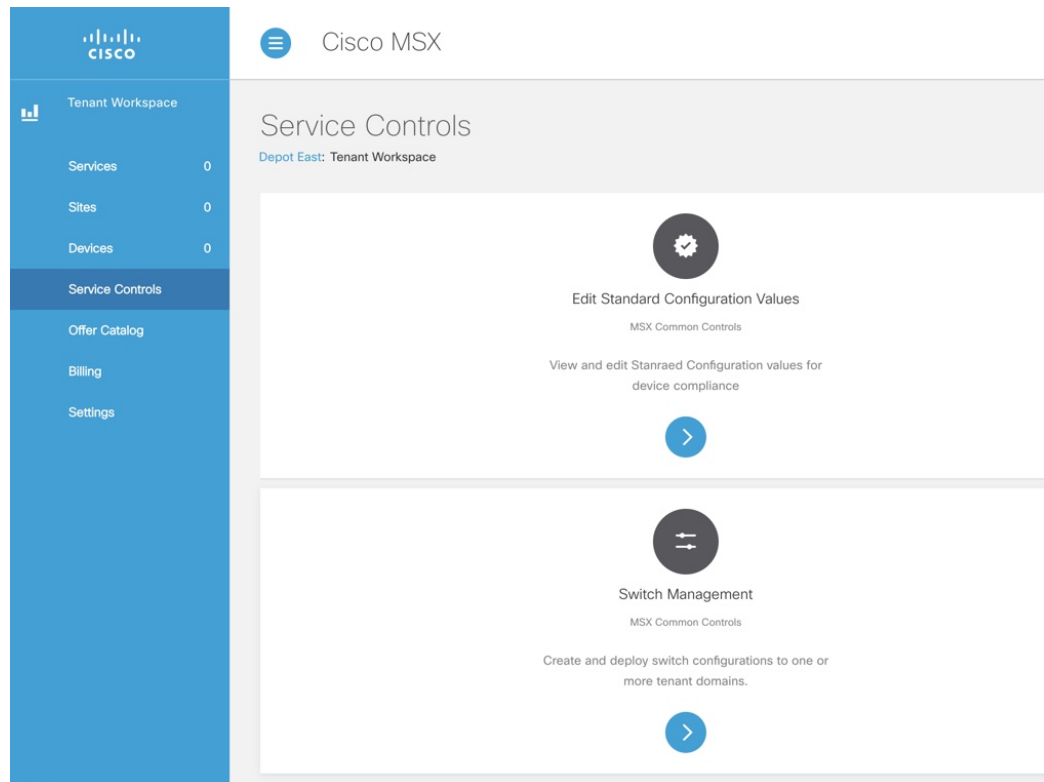
Cisco MSX provides a switch configuration feature template to create new port configurations and apply them to the ports within a tenant hierarchy. Use this template to create configurations with which you can turn ports on/off, enable spanning tree (RSTP), define port types (access/trunk), and specify VLANs (data and voice). Feature template is helpful in scenarios when the switches or the ports in organizations are configured in a similar manner. Once the new configurations are created and tagged appropriately, you can apply these configurations to ports or devices across a tenant hierarchy that uses the same tags.

To create a new switch port configuration using out-of-the-box template available within MSX:

**Procedure**

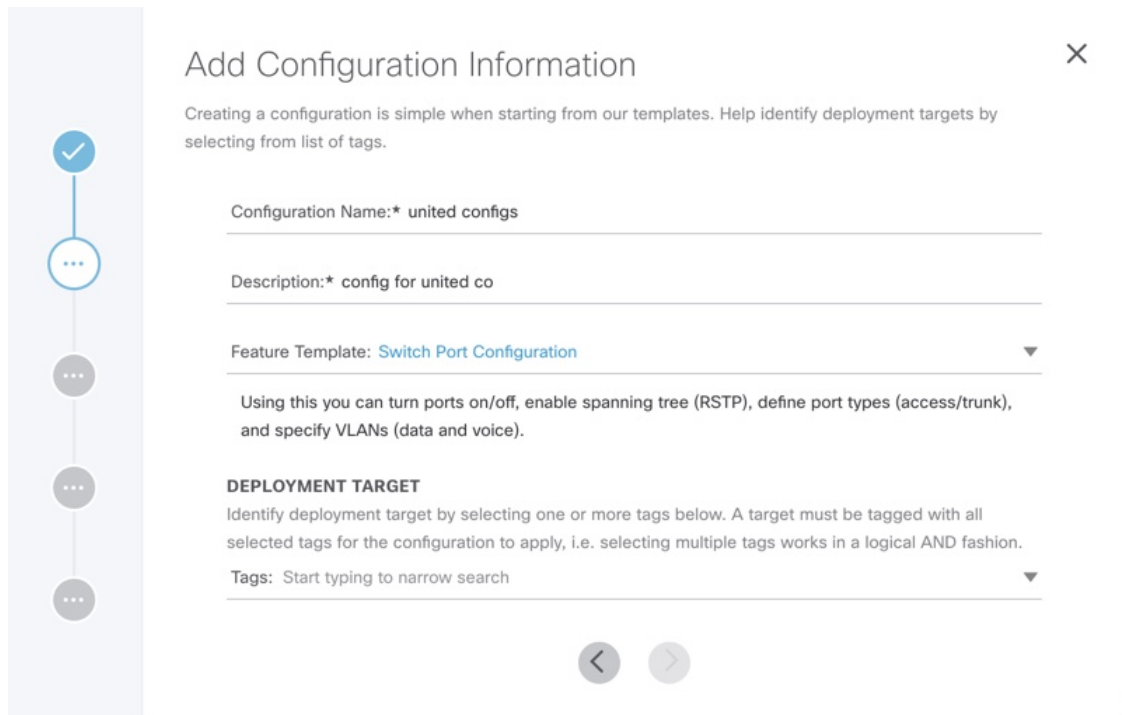
---

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Service Controls**.
- Step 3** Select **Switch Management** to create new switch configurations.



**Step 4** On the **Switch Management** page, click + or **New Configuration** option to create a new switch configuration. The **Create Configuration**wizard is displayed.

**Step 5** Click **Get Started**.  
The **Add Configuration Information** window is displayed.



### Add Configuration Information ✕

Creating a configuration is simple when starting from our templates. Help identify deployment targets by selecting from list of tags.

Configuration Name:\* united configs

Description:\* config for united co

Feature Template: Switch Port Configuration ▼

Using this you can turn ports on/off, enable spanning tree (RSTP), define port types (access/trunk), and specify VLANs (data and voice).

**DEPLOYMENT TARGET**

Identify deployment target by selecting one or more tags below. A target must be tagged with all selected tags for the configuration to apply, i.e. selecting multiple tags works in a logical AND fashion.

Tags: Start typing to narrow search ▼

< >

**Step 6** Enter a unique name for the new port configuration and its description, and select an existing feature template. Next, select one or more tags that categorize entities based on common criteria. Tags can be region-based or department-based. Examples of Tags in a School system can be Classroom, Auditorium, and so on. The configurations will be only applied to target entities that uses all the specified tags.

**Note** If no tags are displayed, make sure there is a Meraki organization attached to the MSX instance. For more information, see [Attaching Organizations](#). Also, make sure that the target entities are configured with tags outside of MSX. For example, for Meraki the Switch Ports can be configured with tags using the Meraki Dashboard.

**Step 7** Click > to move to the **Enter Configuration** page.

**Step 8** Enter further configurations based on the template that was selected to create this new configuration. These configurations apply to tenants that use the same tags. If locked, tenants would not be able to modify these values.

**Note** Some of the fields on the **Enter Configuration** page require additional settings on the Meraki dashboard. For more information, see [Important Notes on Switch Port Configurations](#).

**Step 9** Click > to move to the **Review and Save** page.

**Step 10** Review the details and click **Submit** to complete the process.

Under the **Switch Management** page, you can view the newly created switch port configuration, and apply these configuration to a destination target.



## Important Notes on the Switch Port Configurations

The following are important notes for the Storm Control field that is displayed on the **Enter Configuration** page:

- **Storm Control Configurations:**

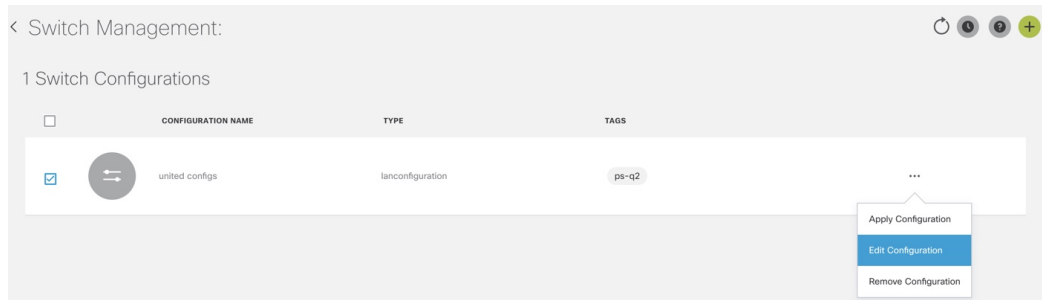
- Storm control configuration options for enhanced storm control are supported only on MS Series switches; MS210, MS225, MS250, MS350, MS355, MS390, MS400 series switches with firmware MS10.0 and higher.
- For storm control functionality to work on MSX, it must be enabled on a network from the Meraki dashboard. For more information, see [Enabling Storm Control](#).

## Editing Switch Port Configuration

To edit switch port configuration:

### Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Service Controls**.
- Step 3** Select **Switch Management** to edit new switch configurations.  
The **Switch Management** page lists configurations that were created and saved.
- Step 4** Select a configuration and click on the ellipsis (...) > **Edit Configuration**.  
The **Edit Configuration** window is displayed.



**Step 5** Edit to modify an existing switch port configurations. These configurations apply to tenants that use the same tags. If locked, tenants would not be able to modify these values.

**Step 6** Click > to move to the **Review and Save** page.

**Step 7** Review the details and click **Submit** to complete the process.

Under the **Switch Management** page, you can view the edited switch port configuration, and apply these configuration to a destination target.

## Applying Switch Port Configuration

After creating and tagging the switch port configuration appropriately, you can use these parameters to deploy configurations on similarly tagged target entities, such as switch ports. The target entities should be configured with tags outside of MSX. For example, for Meraki the Switch Ports can be configured with tags using the Meraki Dashboard.

To apply a new switch port configuration:

### Before you begin

Make sure the entities where the configurations have to be applied are pre-configured with tags outside of MSX. For example, for Meraki, the Switch Ports can be tagged from the Meraki Dashboard. For more information, see [Manage Tags](#) in Meraki Documentation.

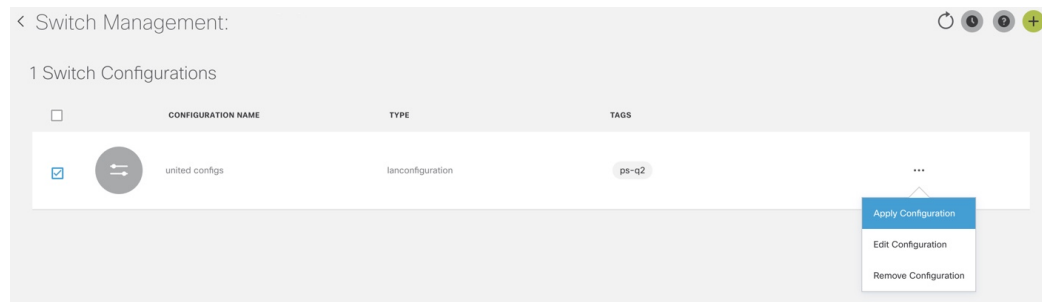
### Procedure

**Step 1** Log in to the Cisco MSX portal.

**Step 2** From the left pane, choose **Tenant Workspace > Service Controls > Switch Management** tile.

**Step 3** On the **Switch Management** page, select a configuration, and click the **ellipsis (...)**, and choose **Apply Configuration**.





**Step 4** Click **Apply Configuration** to deploy the configuration on entities that use similar tags across a tenant hierarchy.

**Step 5** To track the status of the deployment, from the **Switch Management** page, click on the clock icon on the top right side to display the list of user actions. Click the **ellipsis (...)** and choose **View Details**.

The **Deployment Activity** page displays the **Status** of applied configurations for entities that used similar tag(s). You can filter the list by Status or sort this list in a particular order.





## APPENDIX **A**

### Additional Information

---

This section lists the devices currently supported by the Managed Devices service on Cisco MSX and information on the JSON file required to support additional device models on MSX.

- [Devices Supported by Managed Device Service Pack, on page 93](#)
- [Downloaded Sample JSON File from the Cisco MSX, on page 94](#)
- [Sample JSON File for Importing a Device Model on the New Device Type, on page 99](#)

### Devices Supported by Managed Device Service Pack

Cisco MSX Managed Device service pack supports various device types, such as:

- CISCO CSR 1000v
- CISCO IR 829
- CISCO ISR 1100
- CISCO ISR 4221
- CISCO ISR 4321
- CISCO ISR 4331
- CISCO ISR 4351
- CISCO ISR 4431
- CISCO ISR 4451
- Catalyst 300 switch
- CISCO IOS XR
- CISCO NX-OS
- CISCO CAT
- CISCO ASA
- Cisco Meraki. For the Meraki devices supported on MSX, see [Managing Meraki](#).
- Catalyst 9000

- JUNIPER SRX
- FORTINET



**Note** For adding a new device model, see *Importing Device Model*.

## Downloaded Sample JSON File from the Cisco MSX

The downloaded sample JSON file for importing a new device model:

```
{
  "deviceModels": [
    {
      "//comment_1": "'deviceModelName' is where the actual device model needs to be filled,
'CISCO ISR 4451', 'CISCO IR 829' are used here for as examples.",
      "//comment_2": "The List 'interfaces' is for device models where there is no distinction
between wan and lan interfaces, i.e. any interface can be selected as WAN or LAN. Ex: ISR
4451, ISR 4431 etc.",
      "//comment_3": "Lists 'wan' and 'lan' are for device models where the interfaces are
classified as WAN and LAN and cannot be interchangeably used. Ex: IR 829, ISR 11xx etc.",
      "//comment_4": "Lists 'interfaces', 'wan' and 'lan' are mutually exclusive, i.e. if
interface names are populated in 'interfaces' list, they cannot be populated in 'wan' or
'lan' lists and vice versa.",
      "//comment_5": "'wan' and 'lan' lists can be empty when 'interfaces' is populated and
'interfaces' can be empty when 'wan' and 'lan' are populated. If 'interfaces' is populated,
then 'wan' and 'lan' entries must also exist in 'interfaces'",
      "//comment_6": "Because on-boarding interface will be picked from the list of
'interfaces' or from 'wan' list, either of them ('interfaces' or 'wan') lists is mandatory
but 'lan' list is not mandatory.",
      "//comment_7": "'ned-id' is mandatory parameter which SP has to enter, MSX 3.5 release
supports cisco-ios ned only, this ned covers all the Cisco devices running ios and ios-xe.",

      "//comment_8": "Multiple device models can be defined in single JSON file upload.",
      "//comment_9": "Maximum number of interfaces which can be defined is 20, individually
10 each for lan and wan type.",
      "//comment_10": "Overwriting the device model is allowed only if no devices are using
the device model.",
      "//comment_11": "MSX install comes with pre loaded device model definitions, which
can be overwritten provided no devices are using the device model.",
      "//comment_12": "Device Type was added in 3.7.0 this is a required field. This must
be one of: cli, netconf, snmp or generic",
      "//comment_13": "directSecureTemplate was added in 3.7.0 this is a required filed.In
this the User has to provide both the secure credentials and onboarding template",
      "//comment_14": "directTemplate was added in 3.7.0 this is a required field.In this
User needs to provide just the onboarding template to be applied on to the device",
      "//comment_15": "pnpDayZeroFile was added in 3.7.0 this is a required field.If provided
from UI, then it should be pushed to the device instead the one generated from NSO",
      "//comment_16": "platformDeviceType is added in 3.8.0 and is tied to a deviceType for
collecting health metrics",
      "//comment_17": "platformDeviceSubType is added in 3.8.0 and is tied to a deviceType
for collecting health metrics",
      "deviceModelName": "CISCO ISR 4451",
      "interfaces": [
        "GigabitEthernet0/0/1",
        "GigabitEthernet0/0/0",
        "GigabitEthernet0/0/2",
        "GigabitEthernet0/0/3"
      ]
    }
  ]
}
```

```

],
"lan": [],
"wan": [],
"nedId": "cisco-ios",
"deviceType": "cli",
"directSecureTemplate": "TestDirectSecureTemplate",
"directTemplate": "TestDirectTemplate",
"pnpDayZeroFile": "TestPnpDayZeroFile",
"platformDeviceType": "CPE",
"platformDeviceSubType": "ISR",
"snmpDetails": {
  "snmpAuthProto": "sha",
  "snmpVersion": "3",
  "snmpPrivProto": "PrivateProto",
  "snmpUserName": "Username"
}
},
{
  "deviceModelName": "CISCO IR 829",
  "interfaces": [],
  "lan": [
    "Vlan1"
  ],
  "wan": [
    "GigabitEthernet0"
  ],
  "nedId": "cisco-ios",
  "deviceType": "cli",
  "directSecureTemplate": "TestDirectSecureTemplate",
  "directTemplate": "TestDirectTemplate",
  "pnpDayZeroFile": "TestPnpDayZeroFile",
  "platformDeviceType": "CPE",
  "platformDeviceSubType": "ISR",
  "snmpDetails": {
    "snmpAuthProto": "sha",
    "snmpVersion": "3",
    "snmpPrivProto": "PrivateProto",
    "snmpUserName": "Username"
  }
},
{
  "deviceModelName": "CISCO All Interfaces Model",
  "interfaces": [
    "GigabitEthernet0",
    "GigabitEthernet1",
    "GigabitEthernet2",
    "GigabitEthernet3"
  ],
  "lan": [
    "GigabitEthernet0"
  ],
  "wan": [
    "GigabitEthernet1",
    "GigabitEthernet2"
  ],
  "nedId": "cisco-ios",
  "deviceType": "cli",
  "directSecureTemplate": "TestDirectSecureTemplate",
  "directTemplate": "TestDirectTemplate",
  "pnpDayZeroFile": "TestPnpDayZeroFile",
  "platformDeviceType": "CPE",
  "platformDeviceSubType": "ISR"
},
{

```

```

    "deviceModelName": "Cisco ASA",
    "platformDeviceType": "CPE",
    "platformDeviceSubType": "ASA",
    "interfaces": [
      "Adaptive Security Appliance 'GigabitEthernet0/1' interface",
      "Adaptive Security Appliance 'GigabitEthernet0/2' interface",
      "Adaptive Security Appliance 'mgmt_int' interface"
    ],
    "lan": [],
    "wan": [],
    "nedId": "cisco-asa",
    "deviceType": "cli",
    "directTemplate": "ASA_CONFIG_TEMPLATE"
  }
],
"deviceMetricConfigurations": [
  {
    "//comment_1": "(Required) 'platformDeviceSubType' is a string that maps the device metric configuration to matching device model.",
    "//comment_2": "(Required) 'platformDeviceType' is used to identify what type of device. This is used in conjunction with subtype to match device metric configurations.",
    "//comment_3": "(Required) 'snmpDetails' provides information on how to connect to the device using SNMP. It will provide information like snmp version, snmp auth protocol, snmp username, etc",
    "//comment_4": "(Optional) 'snmpOidList' provides a list of oid to append to existing list to collect data from. In certain cases of 3rd party device you might have to specify which OID to collect data from.",
    "//comment_5": "(Optional) 'snmpCpuMemoryUptimeQueryTemplate' is the query template defined to retrieve and transform CPU, Memory Free/Used and Uptime. In some cases query might have to be updated based on device type.",
    "//comment_6": "'snmpCpuMemoryUptimeQueryTemplate' is expected as a JSON object.",
    "//comment_7": "If an existing device metric configuration for subtype exists, we will overwrite if you proceed.",
    "//comment_8": "NOTE: You may have to create a config template and upload it to NSO to configure SNMP on device on onboarding. To do this use 'directTemplate' attribute in device model",
    "snmpDetails": {
      "snmpAuthProto": "md5",
      "snmpVersion": "3",
      "snmpPrivProto": "PrivateProto",
      "snmpUserName": "Username"
    },
    "platformDeviceType": "CPE",
    "platformDeviceSubType": "JUNOS",
    "snmpOidList": [
      ".1.3.6.1.4.1.2636.3.1.13.1.21",
      ".1.3.6.1.4.1.2636.3.1.13.1.11"
    ],
    "snmpCpuMemoryUptimeQueryTemplate": {
      "size": 0,
      "query": {
        "bool": {
          "must": [
            {
              "match": {
                "deviceId": "{{ device_id }}"
              }
            },
            {
              "match": {
                "serviceId": "{{ service_id }}"
              }
            }
          ]
        }
      }
    }
  }
]

```

```

        "range": {
          "@timestamp": {
            "gte": "now-5m",
            "lt": "now"
          }
        }
      ]
    }
  },
  "aggs": {
    "per_interval": {
      "date_histogram": {
        "field": "@timestamp",
        "interval": "5m"
      },
      "aggs": {
        "UptimeMS": {
          "max": {
            "field": "sysUpTimeInstance"
          }
        },
        "UptimeHours": {
          "bucket_script": {
            "buckets_path": {
              "uptime": "UptimeMS"
            },
            "script": {
              "inline": "params.uptime / 360000"
            }
          }
        },
        "5minCPU": {
          "avg": {
            "field": "jnxOperating5MinLoadAvg.9.1.0.0"
          }
        },
        "PctMemUsed": {
          "avg": {
            "field": "jnxOperatingBuffer.9.1.0.0"
          }
        }
      }
    }
  }
},
{
  "snmpDetails": {
    "snmpAuthProto": "sha",
    "snmpVersion": "3",
    "snmpPrivProto": "Privateproto",
    "snmpUserName": "Username"
  },
  "platformDeviceType": "CPE",
  "platformDeviceSubType": "ASA",
  "snmpCpuMemoryUptimeQueryTemplate": {
    "query": {
      "bool": {
        "must": [
          {
            "match": {
              "deviceId": "{{ device_id }}"
            }
          }
        ]
      }
    }
  }
}

```

```

    },
    {
      "match": {
        "serviceId": "{{ service_id }}"
      }
    },
    {
      "range": {
        "@timestamp": {
          "lt": "now",
          "gte": "now-5m"
        }
      }
    }
  ]
},
"aggs": {
  "per_interval": {
    "date_histogram": {
      "field": "@timestamp",
      "interval": "5m"
    },
    "aggs": {
      "5minCPU": {
        "avg": {
          "field": "cpmCPUTotal5minRev.6"
        }
      },
      "UptimeHours": {
        "bucket_script": {
          "buckets_path": {
            "uptime": "UptimeMS"
          },
          "script": {
            "inline": "params.uptime / 360000"
          }
        }
      },
      "UsedMem": {
        "avg": {
          "field": "System memory.ciscoMemoryPoolUsed"
        }
      },
      "PctMemUsed": {
        "bucket_script": {
          "buckets_path": {
            "used": "UsedMem",
            "free": "FreeMem"
          },
          "script": {
            "inline": "params.used / params.free * 100"
          }
        }
      },
      "UptimeMS": {
        "max": {
          "field": "sysUpTimeInstance"
        }
      },
      "FreeMem": {
        "avg": {
          "field": "System memory.ciscoMemoryPoolFree"
        }
      }
    }
  }
}

```



```

    }
  }
},
"size": 0
}
]
}

```

## Sample JSON File for Importing a Device Model on the New Device Type

Sample JSON file:

```

{
  "deviceModels": [{
    "deviceModelName": "Juniper JUNOS",
    "platformDeviceType": "CPE",
    "platformDeviceSubType": "JUNOS",
    "interfaces": [
      "ge-0/0/0",
      "gr-0/0/0"
    ],
    "lan": [],
    "wan": [],
    "nedId": "netconf",
    "deviceType": "netconf",
    "directTemplate": "junos-snmp"
  }],
  "deviceMetricConfigurations": [{
    "snmpDetails": {
      "snmpAuthProto": "md5",
      "snmpVersion": "3",
      "snmpPrivProto": "PrivProto",
      "snmpUserName": "Username"
    },
    "platformDeviceType": "CPE",
    "platformDeviceSubType": "JUNOS",
    "snmpOidList": [".1.3.6.1.4.1.2636.3.1.13.1.21", ".1.3.6.1.4.1.2636.3.1.13.1.11"],
    "snmpCpuMemoryUptimeQueryTemplate": {
      "size": 0,
      "query": {
        "bool": {
          "must": [
            {
              "match": {
                "deviceId": "{{ device_id }}"
              }
            }
          ],
          "range": {
            "@timestamp": {

```

```
        "gte": "now-5m",
        "lt": "now"
    }
  }
]
},
"aggs": {
  "per_interval": {
    "date_histogram": {
      "field": "@timestamp",
      "interval": "5m"
    },
    "aggs": {
      "UptimeMS": {
        "max": {
          "field": "sysUpTimeInstance"
        }
      },
      "UptimeHours": {
        "bucket_script": {
          "buckets_path": {
            "uptime": "UptimeMS"
          },
          "script": {
            "inline": "params.uptime / 360000"
          }
        }
      },
      "5minCPU": {
        "avg": {
          "field": "enterprises.2636.3.1.13.1.21.9.1.0.0"
        }
      },
      "PctMemUsed": {
        "avg": {
          "field": "enterprises.2636.3.1.13.1.11.9.1.0.0"
        }
      }
    }
  }
}
}
}]
}
```