



Provisioning Tasks

[Provisioning Tasks](#) 2

Revised: May 20, 2022

[← Back](#)

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 1: Provisioning a Supported Device in the Service Pack

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

Subscribing to Managed Device Service

The Cisco MSX Managed Device service pack allows you to onboard devices to the Cisco 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.

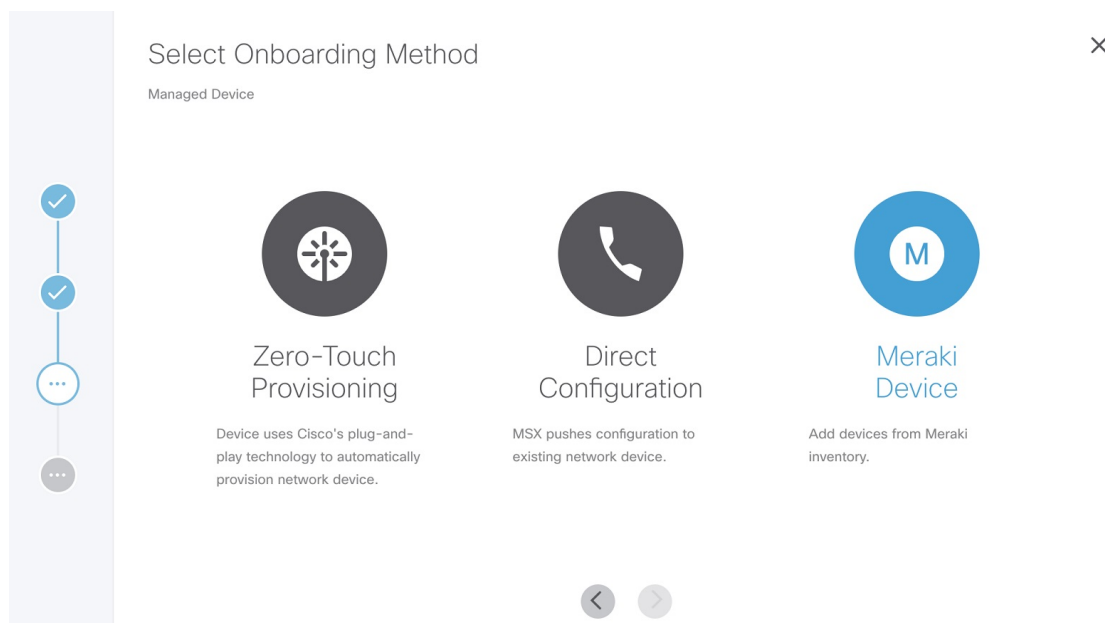
Step 4 Click **Get Started**.

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 1: Onboarding Method



- **Zero-Touch Provisioning**—The device automatically contacts and connects to Cisco 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** — If Meraki Organizations are attached, you can use this option to associate Meraki devices available in Meraki inventory within Cisco MSX, and associate to site and network details. For more information, see [Managing Meraki](#).

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

For Zero-Touch Provisioning:

- a) Enter the name of the device.
- b) 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.

- c) 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](#).

- d) 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 Cisco MSX that can be used as an alternative to CSR Hub to extend connectivity from Cisco 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 Cisco MSX** drop-down list, choose **Yes** to establish an encrypted management tunnel to connect devices to Cisco 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 Cisco 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 2: 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 3: Zero-Touch Provisioning-TLS Gateway

The screenshot shows a mobile application interface for adding device details. The title is 'Add Device Details' with a close button (X) in the top right. Below the title is a 'Managed Device' section. The main content area is titled 'ZERO TOUCH PROVISIONING' and contains the following fields and options:

- Device Name: * Router1
- Device Model: * CISCO CSR 1000v
- Serial Number: * 9999
- Provide Serial Number Later
- Add to compliance
- Tunnel Management: * TLS
- IP Address: *
- Gateway Pools: * StarBucksDC1

Below these fields is a table for interface configuration:

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

At the bottom of the form are navigation arrows (back and forward).

For the Direct onboarding type:

- a) In the **Device Name** field, enter the name of the device.
- b) 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.

- c) In the **IP Address** field, enter the IP address of the device.
- d) In the **Port** field, enter the port number.
- e) In the **User Name** field, enter the user name.
- f) In the **Password** field, enter the password.
- g) 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.

- h) Click **Next**.
- i) From the **Bring Up a Secure Management Tunnel to Cisco MSX** drop-down list, choose **Yes** to establish an encrypted management tunnel to connect devices to Cisco 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 Cisco 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 4: 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

At the bottom of the form, there is a table with columns 'WAN' and 'LAN' for selecting interfaces:

	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.

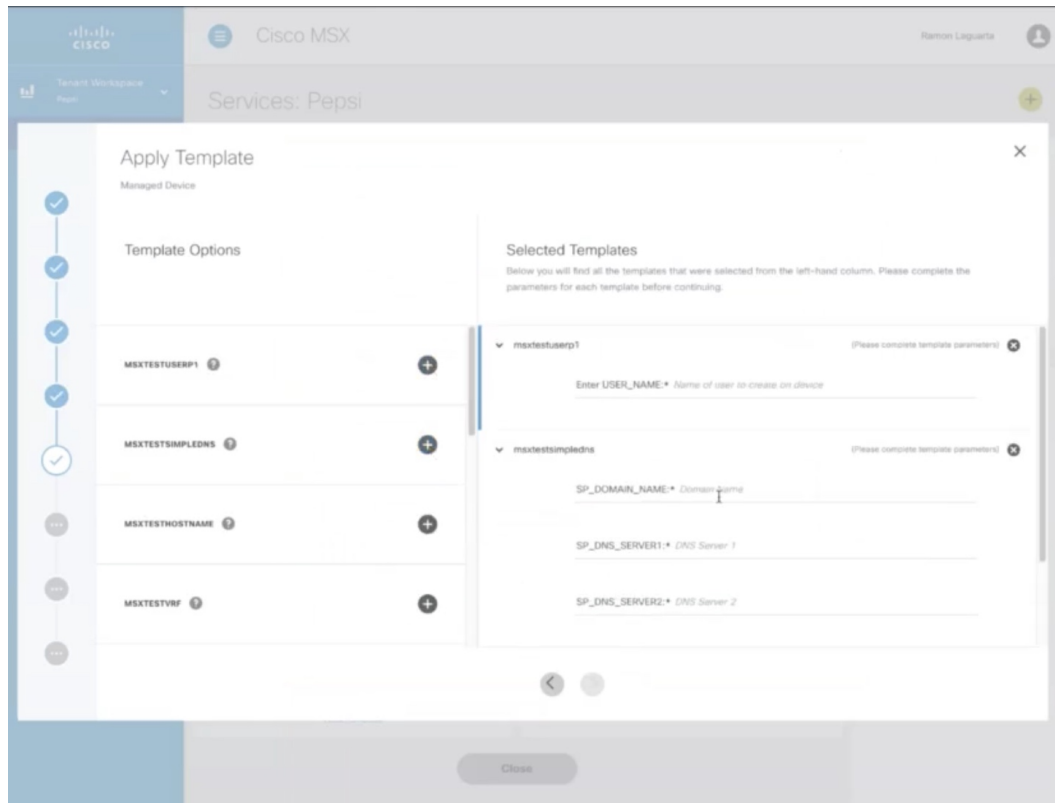
- c) Click > to move to the **Review and Submit** page.
- d) Review the details and click **Submit** to complete the process.

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 5: 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.

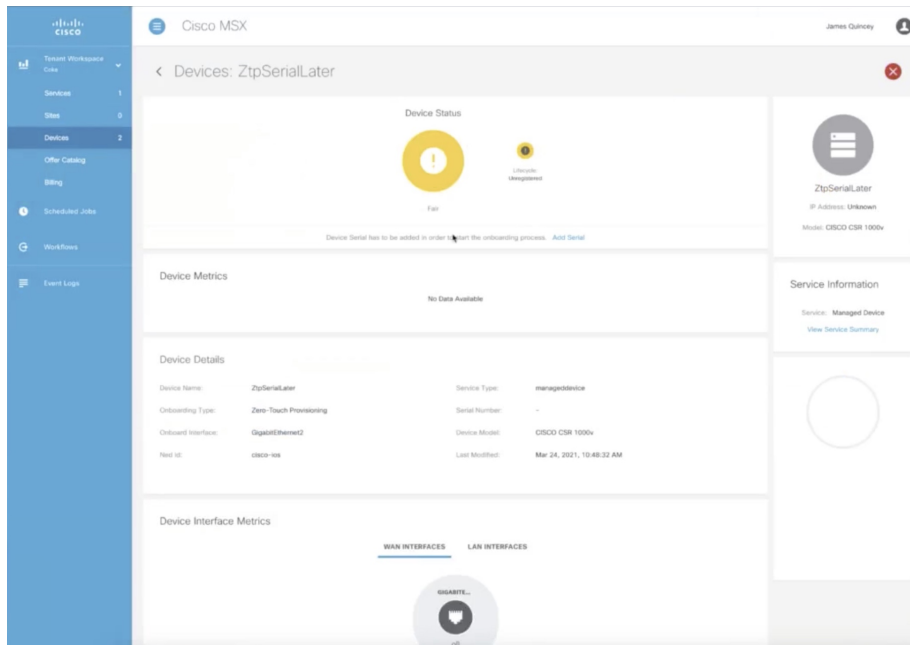
Step 2 From the left pane, choose **Tenant Workspace > Devices**.

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

Step 3 Choose a device from the list.

The device information is displayed.

Figure 6: 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

- Meraki devices cannot be included in the bulk import.
- 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.

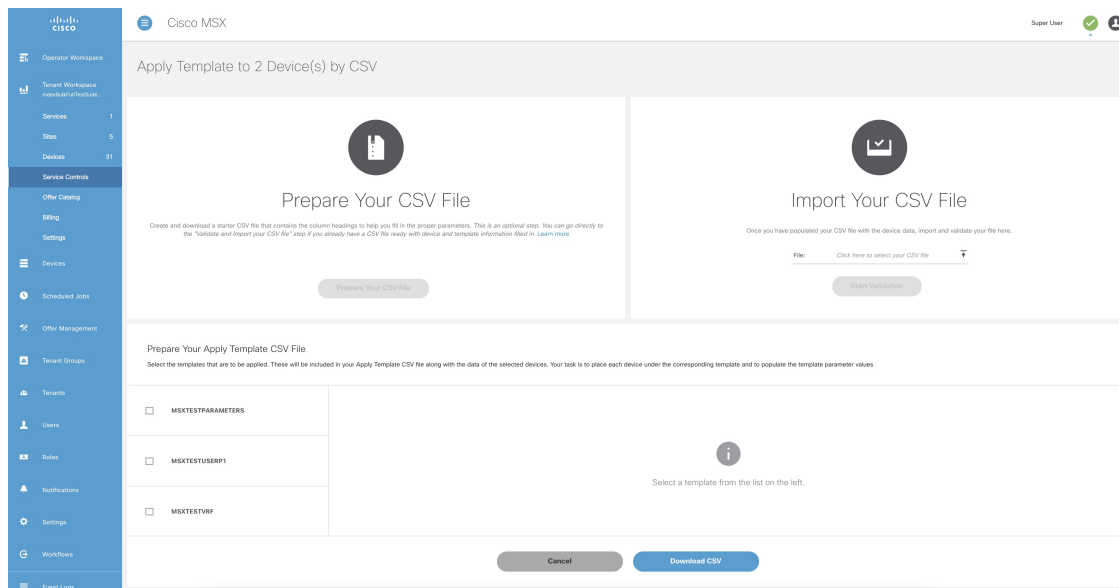
a) Click **Prepare your CSV file**.

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 7: 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 8: 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		GigabitEtherne	GigabitEthernet2						TRUE	NO	No Template	

Step 7

Import the Site Template file.

- 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**.

- 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.

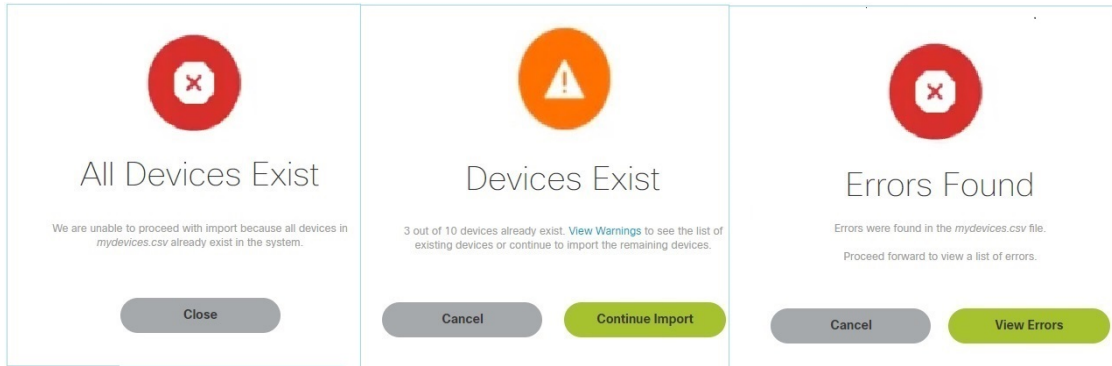
- If the device data in the Site Template file is invalid, the validation process detects and displays the errors.

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 9: 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.

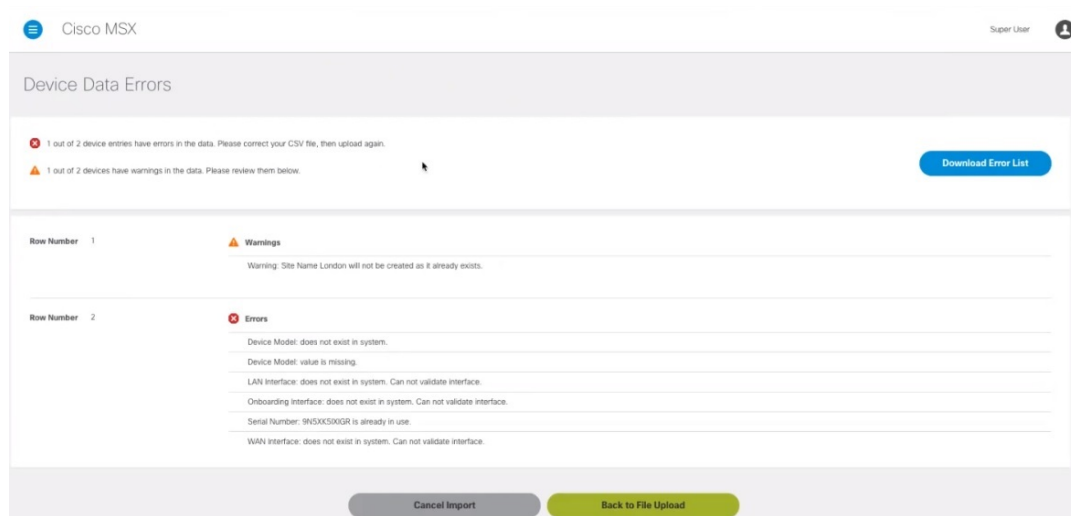
- Click **View Errors**.

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 10: 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 11: 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>

Cancel Submit

Step 5 Click **Submit**.

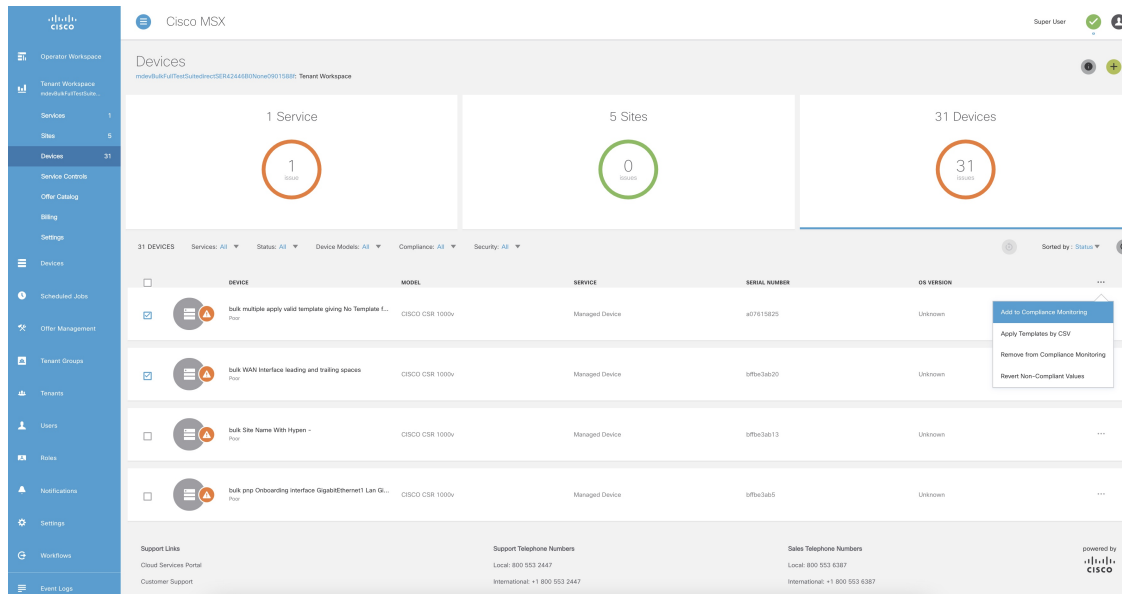
Applying Template Using CSV File

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 12: Applying Template Using CSV File



Step 5

Prepare the Site Template file.

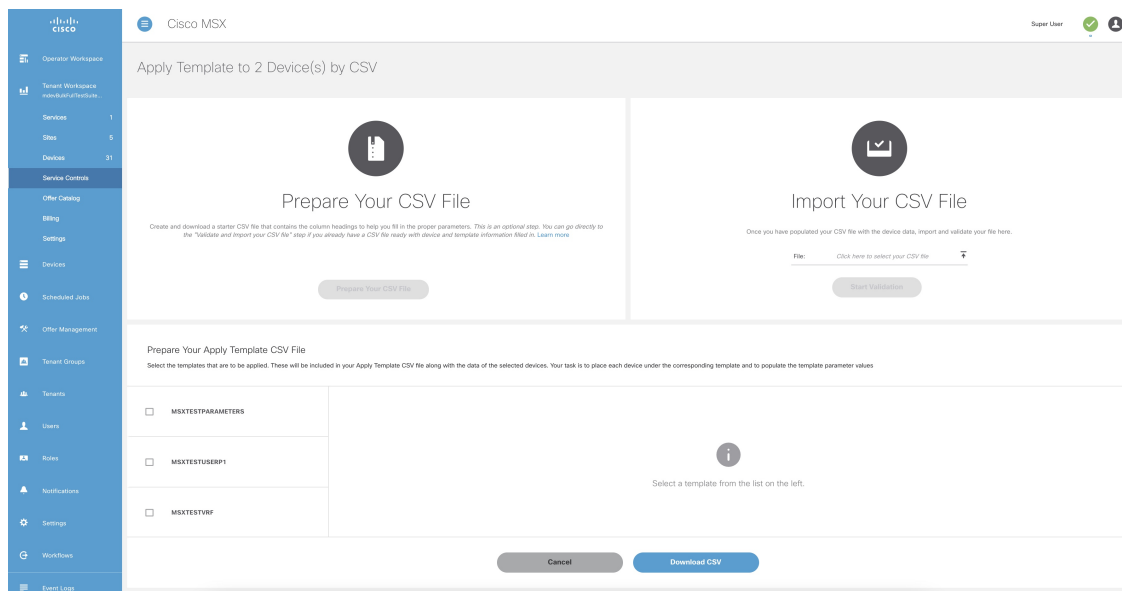
- a) Click **Prepare your CSV file**.

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 13: 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 14: 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**.

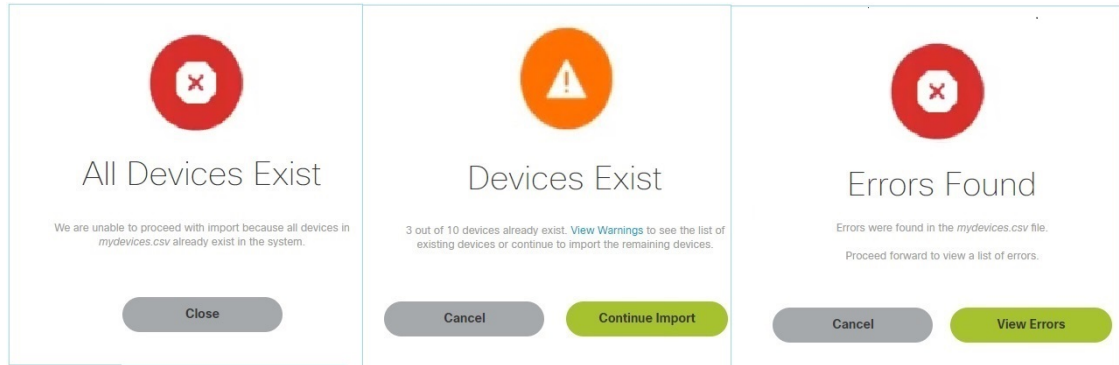
- b) Click **Start Validation**.

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 15: 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.

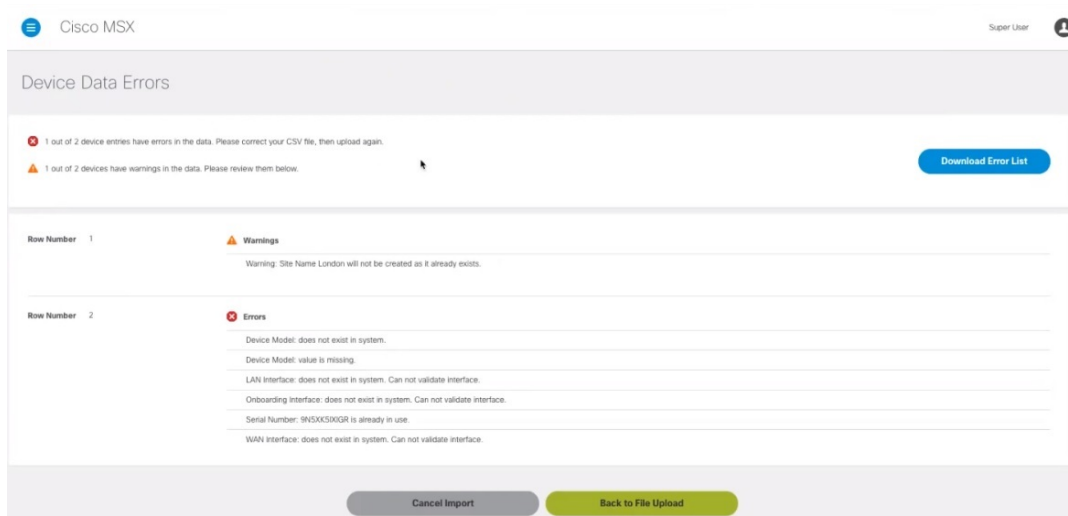
3. **Error Found:** In this case, a combination of both warnings and error messages appear.

- 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 16: 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 2: 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.	Uploading a NED Package
Preparing the SNMP device template.	Loading SNMP Configuration Template
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.	Preparing Device Model Information for New Device Type

Task	See
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.	Importing Device Model
Onboard the new device type in the Managed Device service pack.	Adding a Device

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:

- smmp-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](#).

[↩ Back](#)



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

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

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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