Device Management

Revised: May 19, 2022

Back

Managing Devices

To add a device into the Cisco DNA Center Inventory, you will use the Cisco MSX Enterprise Access service pack. Cisco MSX Enterprise Access supports the following types of devices:

- **Network Devices**—Supported network devices include Cisco routers, switches, and wireless devices such as wireless controllers (WLCs) and access points (APs).
- **Compute Devices**—Supported compute devices include the Cisco Unified Computing System (UCS), devices running Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS), and other data center devices.
- **Meraki Dashboard**—Dashboard to the Cisco cloud management platform for managing Cisco Meraki products.

Adding a Network Device

Before you add a device, you should have created an Enterprise Access subscription and added a Cisco DNA Center to Cisco MSX. For more information, see Subscribing to Enterprise Access Service and Attaching Cisco DNAC Controllers.

Procedure

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

Step 2 From the left pane, click **Tenant Workspace** and then choose a tenant from the drop-down list.

The dashboard page is displayed with the services added.

Step 3 Click **Enterprise Access**.

The list of Controllers attached to a tenant is displayed.

Step 4 From the list, choose a Controller.

The Controller information is displayed.

Step 5 Click the **Add actions** icon displayed at the top right corner of the screen, and then click **Add Network Device**.

A wizard is displayed with the instructions to add a device.

Step 6 From the **Control Plane** drop-down list, choose a Controller. This field is pre-populated with the current Controller, but you can change it.

Step 7 From the **Device Type** drop-down list, choose **Network Device**.

Step 8 Enter the Device Name and IP Address of the device.

Step 9 Click **Next**.

Step 10 From the **SNMP Version** drop-down list, choose the SNMP version. V2C is the default value. If you choose **V2C**, configure the following fields:

Table 1: SNMPv2c Credentials

Field	Description
Read Community	Read-only community string password used only to view SNMP information on the device.
Write Community	Write community string used to make changes to the SNMP information on the device.
SNMP Retries and Timeout	**Retries**— Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3. **Timeout**— Number of seconds Cisco DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

If you choose **V3**, configure the following fields:

Table 2: SNMPv3 Credentials

Field	Description
Username	Name associated with the SNMPv3 settings.
SNMP Mode	Security level that an SNMP message requires. Choose one of the following modes: • **Authentication and Privacy**; Provides both authentication and encryption. • **Authentication and No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication and No Privacy**: Does not provide authentication or encryption.
Authentication Type	Authentication type to be used. Enabled if you choose 'Authentication and Privacy' or 'Authentication and No Privacy' as the authentication mode. Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Authentication Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.

Field	Description
Privacy Type	Privacy type. Enabled if you choose 'Authentication and Privacy' as the authentication mode. Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.
SNMP Retries and Timeout	**Retries**: Number of attempts allowed to connect to the device. Valid values are from 1 to 3. The default is 3. **Timeout**: Number of seconds Cisco DNA Center waits when trying to establish a connection with a device before timing out. Valid values are from 1 to 300 seconds in intervals of 5 seconds. The default is 5 seconds.

Step 11 Click **Next**.

Step 12 Enter the HTTPS Configuration details. This section is optional.

- **Username**: Name used to authenticate the HTTPS connection.
- **Password**: Password used to authenticate the HTTPS connection.
- **Port**: Number of the TCP/UDP port used for HTTPS traffic.

Step 13 Click **Next**.

Step 14 Enter the CLI configuration details:

Table 3: CLI Credentials

Field	Description
Protocol	Network protocol that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**. If you plan to configure the NETCONF port, you need to choose **SSH2** as the network protocol.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network.

Field	Description
Enable Password	Password used to move to a higher privilege level in the CLI.
NETCONF	NETCONF port number. NETCONF requires that you configure SSH as the CLI protocol and define the SSH credentials.

Step 15 Click **Next**.

A Network Device is added to the Enterprise Inventory.

Adding a Compute Device

Before you add a device, you should have created an Enterprise Access subscription and added a Cisco DNA Center to Cisco MSX. For more information, see Subscribing to Enterprise Access Service and Attaching Cisco DNAC Controllers.

Procedure

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

Step 2 From the left pane, click **Tenant Workspace** and then choose a tenant from the drop-down list.

The dashboard page is displayed with the services added.

Step 3 Click **Enterprise Access**.

The list of Controllers attached to a tenant is displayed.

Step 4 From the list, choose a Controller.

The Controller information is displayed.

Step 5 Click the **Add actions** icon displayed at the top right corner of the screen, and then click **Add Compute Device**.

A wizard is displayed with the instructions to add a device.

Step 6 From the **Control Plane** drop-down list, choose a Controller. This field is pre-populated with the current Controller, but you can change it.

Step 7 From the **Device Type** drop-down list, choose **Compute Device**.

Step 8 Enter the Device Name and IP Address of the device.

Step 9 Click **Next**.

Step 10 From the **SNMP Version** drop-down list, choose the SNMP version. If you choose **V2C**, configure the following fields:

Note This section is optional, but if you choose an SNMP version, then you have to fill out the details.

Table 4: SNMPv2c Credentials

Field	Description
Read Community	Read-only community string password used only to view SNMP information on the device.
Write Community	Write community string used to make changes to the SNMP information on the device.

If you choose **V3**, configure the following fields:

Table 5: SNMPv3 Credentials

Field	Description
Username	Name associated with the SNMPv3 settings.
SNMP Mode	Security level that an SNMP message requires. Choose one of the following modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication and No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication and No Privacy**: Does not provide authentication or encryption.
Authentication Type	Authentication type to be used. Enabled if you choose 'Authentication and Privacy' or 'Authentication and No Privacy' as the authentication mode. Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5**: Authentication based on HMAC-MD5.
Authentication Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.
Privacy Type	Privacy type. Enabled if you choose 'Authentication and Privacy' as the authentication mode. Choose one of the following privacy types: • **AES128**: CBC mode AES for encryption. • **DES**: DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.

Field	Description
Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.

Step 11 Click **Next**.

Step 12 Enter the HTTPS Configuration details.

- **Username**: Name used to authenticate the HTTPS connection.
- **Password**: Password used to authenticate the HTTPS connection.
- **Port**: Number of the TCP/UDP port used for HTTPS traffic.

Step 13 Click **Next**.

Step 14 Enter the CLI configuration details. This section is optional for compute devices.

Table 6: CLI Credentials

Field	Description
Protocol	Network protocol that enables Cisco DNA Center to communicate with remote devices. Valid value is **SSH2**.
Username	Name that is used to log in to the CLI of the devices in your network.
Password	Password that is used to log in to the CLI of the devices in your network. For security reasons, enter the password again as confirmation.
Enable Password	Password used to move to a higher privilege level in the CLI. For security reasons, enter the enable password again.

Step 15 Click **Next**.

A Compute Device is added to the Enterprise Inventory.

Adding a Meraki Dashboard

Before you add a device, you should have created an Enterprise Access subscription and added a Cisco DNA Center to Cisco MSX. For more information, see Subscribing to Enterprise Access Service and Attaching Cisco DNAC Controllers.

Procedure

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

Step 2 From the left pane, click **Tenant Workspace** and then choose a tenant from the drop-down list.

The dashboard page is displayed with the services added.

Step 3 Click **Enterprise Access**.

The list of Controllers attached to a tenant is displayed.

Step 4 From the list, choose a Controller.

The Controller information is displayed.

Step 5 Click the **Add actions** icon displayed at the top right corner of the screen, and then click **Add Meraki Device**.

A wizard is displayed with the instructions to add a device.

Step 6 From the **Control Plane** drop-down list, choose a Controller.

Step 7 From the **Device Type** drop-down list, choose **Meraki Dashboard**.

Step 8 Enter the Device Name. The IP address is selected by default.

Step 9 Click **Next**.

Step 10 Enter the HTTPS Configuration details:

- **Meraki Api Key/Password**: Password used to authenticate the HTTPS connection.

Step 11 Click **Next**.

A Meraki Dashboard is added to the Enterprise Inventory.

Deleting a Device

You can delete devices from the Enterprise Inventory, as long as they have not already been added to a site.

Procedure

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

Step 2 From the left pane, click **Tenant Workspace** and then choose a tenant from the drop-down list.

Step 3 Under the **Tenant Workspace**, click **Devices**.

The list of devices attached to a tenant is displayed.

Step 4 Look for the device you want to delete, and then click the **more** icon.

Note You can filter the devices based on :

- Tenant Name
- Services
- Device Models

Step 5 Click **Delete Device**.

You are prompted before you delete a device.

Step 6 Click **Delete Device**.

Associating Templates to Network Profiles

Before you provision a device, you have to associate a template to a network profile.

Procedure

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

Step 2 From the left pane, click **Tenant Workspace** and then choose a tenant from the drop-down list.

The dashboard page is displayed with the services added.

Step 3 Click **Enterprise Access**.

The list of Controllers attached to a tenant is displayed.

Step 4 From the list, choose a Controller.

The Controller information is displayed.

Step 5 In the **Templates** section, look for the template you want to associate, and then click the **more** icon.

Step 6 Click **Add to Network Profile**.

A wizard is displayed with the instructions to associate a template.

Step 7 From the **Network Profile** drop-down list, choose a network profile.

Note Not all network profile types are supported. If a network profile is not supported, go to Cisco DNA Center and add a network profile. For the list of device types and network profiles, see Device Type and Network Profile Mapping.

There are scenarios where a template is supported but the resulting network profiles are not available in Cisco DNA Center. In such scenarios, go to Cisco DNA Center and create one or add one to a site.

Step 8 Click **Add to Network Profile**.

Step 9 Click **Okay**.

Device Type and Network Profile Mapping

The table below lists the mapping between the device types and network profile types.

Table 7: Mapping between the Device Types and Network Profile Types

Device Type	Network Profiles Types				
	NFVIS	**Routing**	**Switching**	**Firewall**	**Wireless for Profile**
NFVIS	Yes	—	—	—	—
Routers	—	Yes	—	—	—
Switches and Hubs	—	—	Yes	—	—
Security	—	—	—	Yes	—
Wireless Controller	—	—	—	—	Yes

Provisioning a Device

Note This section describes provisioning non-wireless devices. For provisioning wireless LAN controllers, see WLAN Provisioning.

By provisioning a device, you can push a configuration template to a device. A template is optional to provision wireless controller or router, but mandatory for other devices. Before you provision a device with template, ensure that you have created a template and attached a network profile to it. For more information on creating templates, see Creating a Configuration Template.

Procedure

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

Step 2 From the left pane, click **Tenant Workspace** and then choose a tenant from the drop-down list.

Step 3 Under **Tenant Workspace**, click **Devices**.

The list of devices attached to a tenant is displayed.

Step 4 Look for the device you want to provision, and then click the **more** icon.

Note You can filter the devices based on:

- Tenant Name
- Services
- Device Models

Step 5 Click **Push Template**.

A wizard is displayed with the instructions to provision a device.

Step 6 From the **Site** drop-down list, choose a Cisco DNA Center site.

Note If a device has no site, you can choose the site, and it will assign the device to the site in Cisco DNA Center. If a device has a site that is already assigned, the site will be pre-populated, and the field will be disabled.

Step 7 From the **Network Profile** drop-down list, choose a network profile.

Note Cisco MSX shows only network profiles that apply to a device. For example, if site A has two network profiles, one for switches and the other for routers, and if you try to provision a wireless controller on Site A, you will not see any profiles because none of them apply for wireless controllers.

Step 8 Click **Next**.

Step 9 (Optional) From the **Template** drop-down list, choose a configuration template to apply to the device.

The variables that you can change are displayed.

Note Template variable names are followed by the name of its data type in brackets. Currently, it supports String, Integer, IP address, and MAC address. Along with single text input, template variables also support 'Single Select' and 'Multi Select' where you can select one key (for Single Select) or multiple keys (for Multi Select) from a list of keys in the drop-down list. The keys and their corresponding values are defined in Cisco DNA Center (in template editor).

Step 10 Enter the values in the fields shown.

Step 11 Click **Show Template** to see the template.

Step 12 Click **Next** to apply the template.

The template application process started successfully.

Step 13 Click **Close**.

Deleting a Template

This procedure shows how to delete a template from Cisco DNA Center.

Note You can delete the template with any user as long as they have MANAGE_CONTROL_PLANE permission.

Procedure

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

Step 2 From the left pane, click **Tenant Workspace** and then choose a tenant from the drop-down list.

The dashboard page is displayed with the services added.

Step 3 Click **Enterprise Access**.

The list of Controllers attached to a tenant is displayed.

Step 4 From the list, choose a Controller.

The Controller information is displayed.

Step 5 In the **Templates** section, look for the template you want to delete, and then click the **more** icon.

Step 6 Click **Delete**.

You are prompted before you delete the template.

Step 7 Click **Delete**.

Template is successfully deleted.

Note If a template is assigned to a network profile, you cannot delete it. If you still want to delete it, go to Cisco DNA Center and remove it from the network profile.

Step 8 Click **OK**.

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.