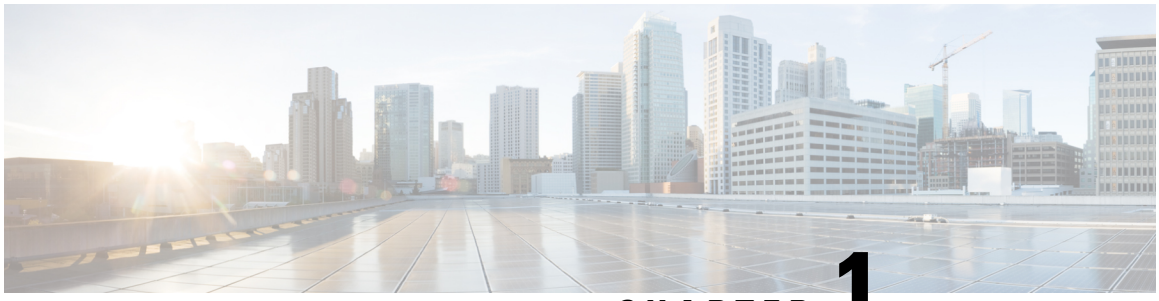
# Cisco Managed Service Accelerator (MSX) 4.3 Enterprise Access Service Pack User Guide

**First Published:** 2022-05-20

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

# CONTENTS



CHAPTER 1

# Getting Started with Enterprise Access Service Pack

This chapter has the following sections:



## Cisco MSX Enterprise Access Service Pack Overview

Cisco MSX Enterprise Access provides consistent management and automation of an Enterprise Network Fabric (wired and wireless network infrastructure). Cisco MSX Enterprise Access allows service providers to offer managed intent-based policy and network segmentation as well as traditional LAN and WAN provisioning from one central place. Cisco MSX Enterprise Access also provides the network health at the global enterprise level by transparently aggregating all the enterprise network domains in one single pane of glass.

These are the benefits of using Cisco MSX Enterprise Access:

- Enables enterprise customers to monitor the health of their network.
- Gives network architects the tools to orchestrate key business functions like onboarding, secure segmentation, IoT integration, and guest access.
- Enables policy-based automation from the edge to the cloud.
- Automates user and device policy for any application across the wireless and wired network via a single network fabric.
- Automated Configuration of Cisco DNA Center Appliances.

# Audience

This guide is designed for service provider operators and tenants who use Cisco MSX Enterprise Access service pack to deploy Enterprise Access services.

# What's New in Cisco MSX Enterprise Access

There are no new features in this release.

# Logging in to Cisco MSX

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

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

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

To log out, click Logout, on the right hand side settings menu.

# Cisco MSX Service Pack-Specific User Roles

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

The permissions allow users to customize various aspects of a service workflow, such as managing tenants, notifications, integration with BSS systems, and managing announcements.

The role-based access permissions are categorized into:

- **Service Pack Specific Permissions**: Include permissions for controlling various settings of the service packs.
- **Services, Configurations, and Devices Specific Permissions**: Include permissions for configuring various settings of 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 users, remote users, tenants, roles, and provider settings.

In Cisco MSX Enterprise Access Service Pack, you need to create a new role and assign the permissions that are required to order, operate, and view the Enterprise Access services. Table 1: Enterprise Access-Specific Permissions, on page 3 lists the Enterprise Access specific permissions.

*Table 1: Enterprise Access-Specific Permissions*

| Permission | Associated Tasks |
|---|---|
| View (Control Plane) | Allows you to:<br>• View control planes and Cisco DNA Center details.<br>• View Cisco DNA Center site hierarchy |
| Manage (Control Plane) | Allows you to:<br>• Attach control plane<br>• Edit control plane<br>• Detach control plane<br>• View Cisco DNA Center details with additional information like address, control plane ID (for internal use and debugging)<br>• Launch the Cisco DNA Center by clicking on the tile, which takes you to the appropriate page in the Cisco DNA Center.<br>• View list of templates<br>• Create templates<br>• Assign template to a network profile<br>• Add/Delete/Provision device<br>**Note** For add/delete/provision a device, you also need the DEVICE_MANAGEMENT permission from platform.<br>• Add SDA fabrics and site domains<br>• View SDA fabrics and site domains<br>• Delete SDA fabrics and site domains<br>• Add Cisco DNA Center site hierarchy<br>• Delete Cisco DNA Center site hierarchy |

For more information on Cisco MSX out-of-box roles, see the Cisco MSX Administration 4.3 Documentation.

For a complete list of all the permissions available in Cisco MSX, see the Cisco Managed Services Accelerator (MSX) 4.3 Platform and Service Packs Permissions Addendum.

# About this Content

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

## Related Documentation

You can access Cisco MSX 4.3.0 content at Cisco MSX End User Documentation.

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

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

| Document | Description |
|---|---|
| Cisco Managed Services Accelerator (MSX) 4.3 Release Notes Documentation | This documentation provides information about the new features in Cisco MSX 4.3. |
| Cisco Managed Services Accelerator (MSX) 4.3 Administration Documentation | This documentation covers the post-install configuration information that is required to set up Cisco MSX. |
| Cisco Managed Services Accelerator (MSX) 4.3 Platform and Service Pack Permissions Addendum | This addendum covers all the permissions that are required to operate Cisco MSX and the service packs. |
| Cisco Managed Services Accelerator (MSX) 4.3 SD-WAN Service Pack Documentation | This documentation includes details that are related to deploying, managing, configuring the Cisco MSX SD-WAN service pack, and troubleshooting service errors. |
| Cisco Managed Services Accelerator (MSX) 4.3 SD-WAN Out-of-the-Box Applications Addendum | This document is an addendum to the *Cisco MSX SD-WAN Service Pack* content. It has details about the out-of-the-box applications of Cisco MSX 4.3 and the comparison of applications in older releases with applications in Cisco MSX 4.3 based on possible application mapping. |
| Cisco Managed Services Accelerator (MSX) 4.3 Enterprise Access Service Pack Documentation | This documentation includes details that are related to deploying, managing, configuring the Cisco MSX Enterprise Access service pack, and troubleshooting service errors. |
| Cisco Managed Services Accelerator (MSX) 4.3 Managed Device Service Pack Documentation | This documentation includes details related to subscribing the Cisco MSX Managed Device service pack, configuring the service, and troubleshooting service errors. |
| Cisco Managed Services Accelerator (MSX) 4.3 Solution Overview Documentation | This documentation provides a comprehensive explanation of the design of the Cisco MSX solution that enables service providers to offer flexible and extensible services to their business customers. |

| Document | Description |
|---|---|
| Open Source Used in Cisco MSX and Service Packs Documentation | This documentation contains licenses and notices for Open Source software that is used in this product. |

# Bias-free Doc Disclaimer

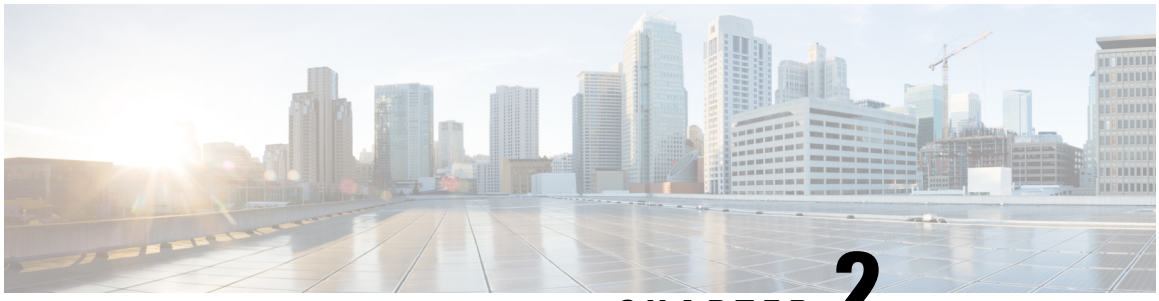
**Note** The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, 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

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.

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 standards documentation, or language that is used by a referenced third-party product.



CHAPTER 2

# Setting up Cisco MSX Enterprise Access Services

This chapter explains how to set up Cisco MSX Enterprise Access from Cisco MSX. This chapter has the following topics:



## Prerequisites

You need to generate a Cisco DNA Center certificate and upload that certificate into Cisco DNA Center. For more information, see Manage Certificates.

## Subscribing to Cisco MSX Enterprise Access Service

After you add a tenant, you can subscribe to Cisco MSX Enterprise Access service.

Before you subscribe, ensure the following:

- Cisco DNA Center is reachable
- IP network connectivity to the Enterprise is working
- Credentials of Cisco DNA Center management account are valid

**Step 1** Log in to the Cisco MSX portal using your credentials. Use super administrator credentials if you are ordering for your tenant.

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

**Step 3** From the left pane, under **Tenant Workspace**, click **Offer Catalog**.

The **Offer Catalog** window appears with the available services.

**Step 4** Click **Enterprise Access**.

**Step 5** Click **Subscribe** and then click **OK**.

### What to do next

You have now created a subscription for a tenant. The next step is to add a Controller (Cisco DNA Center) to the Cisco MSX platform.

# Attaching Controllers to Cisco MSX

After you create a subscription, you can attach one or more Controllers (Cisco DNA Centers) to the Cisco MSX platform. You should have the following information ready before you attach a Controller:

- Name of the Controller. The Controller name can be anything of your choice. The name can be up to 255 alphanumeric characters in length, including hyphens (-) and underscore (_) characters.
- Host name or IP address
- Username and Password
- Cisco DNA Center port. The default port is 443.

**Note** You can attach a Controller to the Cisco MSX platform even if the Controller is not reachable, but you cannot perform most of the tasks until the connection is established.

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

The **Services** page displays all the services the tenant is subscribed to.

**Step 3** Choose **Enterprise Access**.

**Step 4** If you are adding Controller for the first time, click **Continue Setup**. If you have already added a Controller, click the + (**Add New Controller**) icon to add another Controller.

The **Add New Controller** dialog box is displayed.

**Step 5** Click **Attach Controller**.

A wizard is displayed with the instructions to attach a Controller.

**Step 6** Enter the Controller name, IP address, Username, Password, and Cisco DNA Center port.

**Step 7** (Optional) Enter the physical location of the Controller.

**Step 8** Click **Next**.

Controller is now attached to the Cisco MSX platform.

**Step 9** Click **View Controller** to view the Controller you added.

**Note** You can continue to add Controllers, if you choose to.

If you are not able to attach a Controller, check the following:

- Management credentials of the Controller
- Hostname or IP address of the Controller
- Your network connectivity
- Validity of your certificates

**Note** While on-boarding, if you are not able to connect to the Controller, you can do a force connect that will attach the Controller to Cisco MSX. You can troubleshoot the connectivity issues later.

# Deploying Cisco DNA Center Appliances

You can deploy a Cisco DNA Center appliance in your network in one of the following modes:

- Standalone: This option is preferred for initial or test deployments and in smaller network environments. You cannot change a Standalone option to Cluster in the future.
- Three Node Cluster: In this mode, all the services and data are shared among the hosts. This is the preferred option for large deployments. If you choose Cluster mode for your initial deployment, be sure to finish configuring the primary node before configuring the secondary nodes.

Configuring Cisco DNA Center appliance in Cisco MSX involves the following tasks:

- Configuring the Appliance Interfaces
- Configuring the Proxy and NTP Servers
- Configuring the Controller Credentials
- Setting up Virtual IP addresses and Subnets

## Prerequisites

- The installation supports only second-generation appliances. The first-generation appliances are not supported.

- Appliances must have ISO images built in. Re-imaging is not supported, but after the setup, you can upgrade DNA Center to the newest version.
- Only IPv4 addresses are supported.
- Designate the Enterprise interface on your appliance to use the IP address, subnet mask, and default gateway that a DHCP server assigns to it.
- Confirm that the IP address assigned by the DHCP server is reachable by the machine from which you will complete the wizard.
- Appliances must be racked, connected, and powered on.

Before beginning the installation, you must ensure that your network has sufficient IP addresses available to assign to each of the appliance ports that you plan on using. Depending on whether you are installing the appliance as a single-node cluster or as a primary or secondary node in a three-node cluster, you will need the following appliance port (NIC) addresses:

- **Enterprise Port Address (Required)**: One IP address with a subnet mask.
- **Cluster Port Address (Required)**: One IP address with a subnet mask.
- **Management Port Address (Optional)**: One IP address with a subnet mask.
- **Internet Port Address (Optional)**: One IP address with a subnet mask. This is an optional port, used only when you cannot connect to the cloud using the Enterprise port. You do not need an IP address for the Internet port unless you must use it for this purpose.

# Setting up Controllers in Cisco MSX

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

The **Services** page displays all the services the tenant is subscribed to.

**Step 3** Choose **Enterprise Access**.

**Step 4** Click the + (**Add New Controller**) icon.

The **Add New Controller** dialog box is displayed.

**Step 5** Click **Setup New Controller**.

The **New Controller** dialog box is displayed.

A wizard is displayed with the instructions to add a new Controller.

**Step 6** In the **Controller Name** field, enter a name for your Cisco DNA Center controller.

**Step 7** Choose an operating mode from the options **Standalone** and **3-Node Cluster**.

**Note** You cannot change a Standalone option to Cluster in the future.

**Step 8** Click **Configure Primary Node.**

A wizard is displayed with the instructions to set up a Controller.

**Step 9** Read the prerequisites instructions.

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

The **Configure Appliance Interfaces** dialog box is displayed.

**Step 11** In the **Enterprise Network Interface** section, choose one of the following network interface controller (NIC) bonding modes for the Enterprise interface:

- **Active-Backup**: This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.
- **LACP**: This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.

**Step 12** Enter the following information for the mode you selected:

- **Host IP Address**: IP address for the Enterprise port. This is required.

  **Note** This is the IP address assigned by the DHCP server indicated in pre-requisites.

- **Subnet Mask**: The netmask for the port's IP address. This is required.
- **Default Gateway IP Address**: Default gateway IP address to use for the port.

  **Note** You can configure only one gateway. For instance, if you provide the gateway on the Management interface, you cannot provide one for the Enterprise or Internet interface.

- **DNS**: IP address of the preferred Domain Name System (DNS) server. To enter additional DNS servers, separate each entry by a comma.

**Step 13** Click **Add Static Route** to configure a static route. Enter the route's network IP address, subnet mask, and Gateway IP address. To add additional static routes, click **+**.

**Step 14** In the **Intracluster Interface** section, choose one of the following network interface controller (NIC) bonding modes for the Intracluster interface:

- **Active-Backup**: This mode provides fault tolerance by aggregating two Ethernet interfaces into a single logical channel. When the interface that's currently active goes down, the other interface takes its place and becomes active.
- **LACP**: This mode aggregates two Ethernet interfaces that share the same speed and duplex settings into a single logical channel. This provides load balancing and higher bandwidth.

**Step 15** Enter the following information for the mode you selected:

- **Host IP Address**: IP address for the Cluster port. This is required.
- **Subnet Mask**: The netmask for the port's IP address. This is required.

**Step 16** (Optional) In the **Management Network Interface** section, click the **Configure Management Interface** checkbox to configure a dedicated Management interface. Enter the following information for the interface:

- **Host IP Address**: IP address for the Management port. This is required.
- **Subnet Mask**: The netmask for the port's IP address. This is required.

- **Default Gateway IP Address**: Default gateway IP address to use for the port.

**Step 17** (Optional) In the **Internet Access Interface** section, click the **Configure Internet Access Interface** checkbox to configure a port to link the appliance to the Internet when you cannot do so through the Enterprise port. Enter the following information for the interface:

- **Host IP Address**: IP address for the Internet Access port. This is required.
- **Subnet Mask**: The netmask for the port's IP address. This is required.
- **Default Gateway IP Address**: Default gateway IP address to use for the port.

**Step 18** Click **Next**.

The **Proxy and NTP Servers** dialog box is displayed.

**Step 19** In the **Proxy Server** section, click **Network uses a proxy server to access the internet** checkbox if your network uses a proxy server to access the internet. Enter the following information for the proxy server:

- **Proxy Server**: The URL or host name of an HTTPS network proxy used to access the Internet.
- **Port**: The port your appliance used to access the network proxy.
- **Username**: The user name used to access the network proxy. If no proxy login is required, leave this field blank.
- **Password**: The password used to access the network proxy. If no proxy login is required, leave this field blank.

**Step 20** In the **NTP Servers** section, enter at least one NTP server address or hostname. Minimum three NTP server addresses are recommended. To enter more NTP server addresses or hostnames, click the **+ (Add NTP Server)** icon.

**Step 21** Click **Next**.

The **Controller Credentials** dialog box is displayed.

**Step 22** Enter the following information for the Maglev account. The Maglev account is used to administer Cisco DNA Center using its command-line interface. The admin account is used to administer Cisco DNA Center through its graphical user interface.

- Linux Console Username: maglev
  - **Password**: The password used to access the maglev account.
- GUI Web Access Username: admin
  - **Password**: The password used to access the admin account.

**Step 23** Click **Next**.

The **Virtual IP Addresses and Subnets** dialog box is displayed.

**Step 24** In the **Cluster Virtual IP Addresses** section, enter the Virtual IP addresses that will be used for traffic between the cluster and the interfaces that you have configured on your primary node:

- **Enterprise**: IP address to access from Enterprise Network. IP should be within the range 124.1.1.1/24.
- **Intracluster**: IP address to access from Intracluster. IP should be within the range 124.12.12.4/24.
- (Optional)**FQDN**: Fully qualified domain name (FQDN) for your cluster.

- (Optional)**For Management Access**: IP address to access from Management network interface. This is optional only if you are not configuring a Management interface in Step 16, on page 11. If you have already added a Management interface, then a Virtual IP address is required.
- (Optional)**For Internet Access** : IP address to access from Internet access interface. This is optional only if you are not configuring an Internet interface in Step 17, on page 12. If you have already added an Internet interface, then a Virtual IP address is required.

**Note** Virtual IP addresses are required only for 3 Node cluster installations. For a standalone installation, you don't need to provide this information.

**Step 25** In the **Container and Cluster Subnets** section, enter the Container and Cluster subnets. Cisco DNA Center requires a dedicated, nonrouted IP subnet to manage internal and cluster services. The minimum subnet size is 21 bits and it must be in the link-local or private address space (169.254.0.0/16, 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 10.64.0.0/10):

- **Container Subnet**: A dedicated, nonrouted IP subnet that Cisco DNA Center uses to manage internal services.
- **Cluster Subnet**: A dedicated, non-routed IP subnet that Cisco DNA Center uses to manage internal cluster services.

**Note** For Container and Cluster subnets, currently, Cisco MSX uses default values that are recommended in the Cisco DNA Center Installation Guide.

**Step 26** Click **Next**.

The **Review Primary Node Details** dialog box is displayed.

**Step 27** Review the details you entered.

**Step 28** Click **Next**.

The **Starting Primary Node Configuration** dialog box is displayed. The configuration of your primary node begins. The configuration process takes up to 4 hours. Once the configuration is complete, you can configure your secondary nodes.

**Note** After a standalone install is successful, a control plane will be auto attached to Cisco MSX. For a 3 node cluster, after the primary node installation is successful, a control plane will be auto attached to Cisco MSX.

**Step 29** Click **View Progress** to view the progress of the installation.

The progress screen continuously updates during the process, indicating the tasks that are currently being completed and their progress, as well as any errors that have occurred.

You can perform the following tasks from the progress screen:

- **Delete Cluster**: If an installation fails, you can either delete the cluster or edit the configuration values and retry the failed installation. You can only delete a whole cluster. For more information, see Deleting a Cluster Node , on page 15 and Retrying a Failed Installation , on page 15.
- **Continue Setup**: After the primary node was successfully installed, you can continue installing the secondary node. To install a secondary node, click **Continue Setup**. For more information, see Configuring the Secondary Node , on page 14.

**Note** After the installation, if the synchronization fails, it is because the fabric package is not installed. To install the fabric package on Cisco DNA center, see the Cisco DNA Center documentation at *Plan the Deployment*.

**Note** After you successfully complete the installation, you can add network hierarchy. For more information, see *Designing Network Hierarchy*.

# Configuring the Secondary Node

After you complete deploying the appliance as the primary node, you can continue the installation with secondary and third nodes.

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

The **Services** page displays all the services the tenant is subscribed to.

**Step 3** Choose **Enterprise Access**.

**Step 4** Click the **Setup is in progress for controllers link**.

The **Controller Setup Monitor** dialog box is displayed. All the controllers are listed in the dialog box.

**Step 5** Click the name of a controller.

The **Controller Setup** window is displayed.

**Step 6** Click **Continue Setup**.

A wizard is displayed with the instructions to configure the second or third node based on the current step you are in.

**Step 7** Read the prerequisites instructions.

**Step 8** Click **Next**.

The **Configure Appliance Interfaces** dialog box is displayed.

**Step 9** Enter the IP address for the Enterprise, Management, Intracluster, and Internet interfaces. Interfaces cannot use the same IP address used in primary. The interfaces will be configured in the same subnet as the primary node.

**Note** The Internet and Management interfaces will be shown only if you have selected Internet and Management when you installed the primary node.

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

The **Controller Credentials** dialog box is displayed.

**Step 11** Enter the password for the Cisco DNA Center user accounts. If you want to use the password from Primary, click the **Use Password from Primary** checkbox.

The 'maglev' username is the default for command line interface (CLI). The username is the same on all the appliances in a cluster. You cannot change the username.

**Step 12** Click **Next**.

The **Review Node Details** dialog box is displayed.

**Step 13** Review the node details before you submit the configuration. You can also see the configuration from primary node. Click **From Primary Node** link to see the primary node configuration. Click **Network Interfaces** link to see the IP

addresses that you have provided for the installation. You can edit these values by clicking **Edit Network Interfaces** link.

**Step 14** Click **Next**.

The node configuration begins and the process may take up to one hour.

**Step 15** Click **Close**.

The **Controller Setup** window displays the status of the installation.

## Retrying a Failed Installation

If an installation fails, you can resubmit it after editing the configuration values. To retry an installation:

**Step 1** Go to the **Controller Setup** page.

**Step 2** Click **Edit Setup**.

The wizard is displayed with the previously entered values.

**Step 3** Make the required changes and submit again.

## Deleting a Cluster Node

You can delete a cluster as a whole. You can delete a cluster when the current installation fails or succeed. For instance, if the current step is configuring the secondary node, and the first node installation was successful, when you delete a node, it will delete the whole cluster.

**Note** Deleting a cluster node will not remove the setup from the Cisco DNA center. It will only delete from the Cisco MSX side. You have to manually remove it from the Cisco DNA center.

**Note** When you delete a cluster, it will also remove the auto-attached control plane from Cisco MSX.

**Step 1** Go to the **Controller Setup** page.

**Step 2** Click **Cancel Setup**.

The **Cancel Setup** confirmation dialog box is displayed for you to confirm the deletion.

**Step 3** Click **Cancel Setup**.

## Activating Cluster

After all the nodes are successfully installed, you can activate a cluster. The activation option will be shown on the Controller page only after all the nodes are successfully installed.

**Step 1** Go to the **Controller Setup** page.

**Step 2** Click **Activate Cluster**.

The **Activate Cluster** confirmation dialog box is displayed for you to confirm the activation.

**Step 3** Click **Activate**.

**Note** The activation is an asynchronous process and it may take up to two and half hours to complete. During this time, the primary node will be in maintenance mode and will undergo multiple re-starts.

## Email Notification

You get an email notification when the following events happen:

- Node (Standalone or Cluster) is initiated
- Node (Standalone or Cluster) fails
- Node (Standalone or Cluster) is installed successfully
- Cluster activation is initiated
- Cluster activation fails
- Cluster is activated successfully

Separate emails will be sent for Primary, Secondary, and Tertiary nodes.

## Installation of TLS Certificate

To make sure that the communication between Cisco MSX and external domains is over a trusted network, Cisco MSX requires a TLS certificate for a newly installed controller. After you complete the installation, you don't need to attach a valid TLS certificate immediately. A self-signed certificate is used for a short duration until you install a valid TLS certificate.

The self-signed certificate comes with a grace period (14 days) and you have to install a valid TLS certificate before it expires. If you don't install a valid TLS certificate after the grace period, communication between Cisco MSX and Cisco DNA Center stops. The 14 day grace period is the default value. Using Consul, you can change the grace period to any amount of days you want.

**Note** The grace period is available only for new installation, not for attaching an existing controller.

For more information on applying certificate, see Cisco DNA Center Security Best Practices Guide.

# Monitoring Controller Setup

You can monitor the progress of the controller setup from the monitoring page. To monitor the progress:

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

The **Services** page displays all the services the tenant is subscribed to.

**Step 3** Choose **Enterprise Access**.

**Step 4** Click the **ellipsis (…)** and choose **Controller Setup Monitor**.

The **Controller Setup Monitor** dialog box is displayed. The list of controllers and the status of their setup are listed in the dialog box.

**Step 5** From the list, click a controller name.

The **Controller Setup** page is displayed.

# Adding Cisco.com Credentials

After you complete the installation, you need to add the credentials for Cisco.com, Smart Accounts, IPAM, and Proxy Settings. This procedure explains adding the Cisco.com credentials. The rest of the procedures are performed through APIs. For more information on configuring Smart Accounts, IPAM, and Proxy Settings, see the Swagger documentation.

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

The **Services** page displays all the services the tenant is subscribed to.

**Step 3** Choose **Enterprise Access**.

**Step 4** Click the pencil icon displayed at the top right corner of the screen and choose **Cisco.com Credentials** from the menu.

The **Add Cisco.com Credentials** dialog box is displayed. If credentials are already added, it will display the details. Otherwise you can add new credentials.

**Step 5** Enter the Username and Password.

**Step 6** Click **Add**.

# Troubleshooting

Cisco DNA Center may show the following error when you try to access some of the APIs:

```
{
 "404 Not Found": [{
  "error": "BAPI not found with technicalName<ID> and restMethod GET"
```

```
 }]
}
```

To fix this issue, you can disable (set enable to false) and enable API Access using Cisco MSX Swagger API below:

**/sda/api/v1/controlplanes/{controlPlaneId}/apiaccess**

Payload is:

```
{
  "enable": true
}
```

# Editing a Controller

To edit the Controller information:

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

**Step 3** Click **Enterprise Access**.

**Step 4** From the list, choose the Controller you want to edit.

**Step 5** Click the **Edit** icon displayed at the top right corner of the screen.

The Controller information is displayed.

**Step 6** Make the changes as required. Click **Save Changes**.

**Note** Edit the password only if you wish to change the password saved by Cisco DNA center.

**Step 7** Click **OK**.

# Deleting a Controller

To delete a Controller from Cisco MSX:

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

**Step 3** Click **Enterprise Access**.

**Step 4** Choose a Controller from the list.

**Step 5** Click the cross icon displayed at the top right corner of the screen.

You are prompted before deleting a Controller.

**Step 6** Click **Remove Controller**.

# Synchronising Cisco DNA Center Inventory

Cisco MSX retrieves the inventory information periodically from Cisco DNA Center. If a device exists in Cisco DNA Center and not in Cisco MSX, then the device will be added to Cisco MSX. If a device exists in Cisco MSX and not in Cisco DNA Center, then the device will be deleted from Cisco MSX. The synchronization happens within the time you configured. Sometimes, if you do not want to wait for the configured period for the inventory to refresh, you can force a refresh.

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

**Step 3** Click **Enterprise Access**.

**Step 4** Choose a Controller from the list.

**Step 5** Click the **Sync with Cisco DNA Center** icon displayed at the top right corner of the screen.

A message 'Successfully initiated Cisco DNA Center sync' is displayed.

**Step 6** Click **Okay**.

**Note** When Cisco MSX completes a refresh, the result of the refresh appears in the event log. To view the event logs, from the left pane, click **Event Logs**.

**Note** You can also refresh the inventory from the page that shows all the Cisco DNA Center and sites. Go to the inventory page, click the **Ellipsis (...)** that is located on the far right of the row and choose **Synchronize with Cisco DNA Center**.

# Viewing Enterprise Network Health

Enterprise Network Health shows the overall health status of the Enterprise Network. The Health Status displays the following information:

- Overall Cisco DNA Center status based on reachability
  - Green: Cisco DNA Center is reachable
  - Red: Cisco DNA Center is not reachable
  - Gray: Cisco DNA Center is reachable but has no health data
- Overall Health Summary
  - Percentage of healthy network devices
  - Percentage of healthy wireless clients
  - Percentage of healthy wired clients
- Network Snapshot
  - Number of images

- Network profiles
- Cisco DNA Center licensed devices (Switches, Routers, and Access Points)

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

**Step 3** Click **Enterprise Access**.

The summary of the Enterprise Network health appears on the screen. The black line shows the overall aggregate network health of the Enterprise for the last 24 hours. The gray line shows the overall aggregate network health of the Enterprise prior to the last 24 hours.

**Step 4** Choose a Controller from the list.

The status of the Controller and the health of the Enterprise is displayed.

# Deleting Cisco MSX Enterprise Access Subscription

To delete a Cisco MSX Enterprise Access subscription:

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

**Step 3** Click **Enterprise Access**.

**Step 4** Click the delete icon.

You are prompted before deleting the subscription.

**Step 5** Click **Delete Subscription**.

# Launching Cisco DNA Center from Cisco MSX

To launch Cisco DNA Center from Cisco MSX:

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

**Step 3** Click **Enterprise Access**.

The list of Controllers attached to a tenant is displayed.

**Step 4** Choose a Controller from the list.

The summary of the network health is displayed.

**Step 5** Go to the appropriate section and click the launch icon. For instance, to view the healthy Cisco DNA Center devices, click the **Visit Cisco DNA Center Healthy Devices** icon. The Cisco DNA Center opens up in a separate window.

# Generating Fusion Router Configuration

In Cisco MSX Enterprise Access solution, the devices are managed and configured by a Cisco DNA Center. However, components that perform the role of fusion routers are not managed by the Cisco DNA Center and have to be manually configured. Cisco MSX allows you to generate the configuration, for Virtual routing and forwarding (VRF) leaking across Enterprise Access Fabric domains, and host connectivity to different external servers (Dynamic Host configuration Protocol or DHCP and others).

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

**Step 2** From the left pane, click **Operator Workspace** and then click the tenant name in the Dashboard page.

**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 'Connect Virtual Networks' icon displayed at the top right corner of the screen.

A wizard appears with the instructions to generate the router configuration.

**Note** A fabric can have a maximum of one external border router. So, if you have two in your fabric, you will get an error message.

**Step 6** Choose a Fabric from the list and click **Next**.

**Step 7** Choose two Virtual Networks from the list and click **Next**.

**Note** You must have a minimum of two Virtual Networks that have segments. If you have less than two, the system will show a warning message. You can go to the fabric border in Cisco DNA Center and either add more Virtual Networks or segment in your existing Virtual Networks.

**Step 8** Choose a Segment from the list and click **Next**.

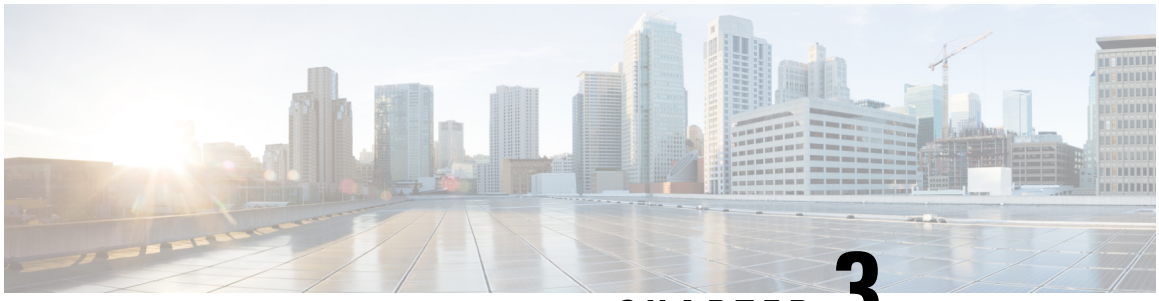
**Step 9** Choose a Segment from the list and click **Next**. This is the segment from the other network.

A confirmation window is displayed with the networks you chose.

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

System generates the Fusion Router Configuration.

**Step 11** Click **Copy to Clipboard** to copy the configuration to clipboard.



CHAPTER 3

# Designing Network Hierarchy

This chapter has the following sections:



## Overview

Using the Cisco MSX Enterprise Access, you can organize the enterprise network sites as a parent child hierarchy to be able to capture the network organization as closely as possible as it will be deployed.

The network hierarchy is predetermined:

- **Areas** do not have a physical address, such as the United States. You can think of areas as a grouping. Areas can contain buildings and subareas. For example, an area called United States can contain a subarea that is called California, and the subarea California can contain a subarea called San Jose.
- **Buildings** have a physical address and contain floors and floor plans. When you create a building, you must specify a physical address. Buildings cannot contain areas. By creating buildings, you can apply settings to a specific area.
- **Floors** are within buildings and consist of cubicles, walled offices, wiring closets, and so on. You can add floors only to buildings.

## Adding an Area

Before you add an area to a network hierarchy, 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.

**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 the controller where you want to create a network hierarchy.

**Step 5** Click the **View Actions(…)** icon, and then click **Add Area**.

The **Add Area** window is displayed.

**Note** In this procedure, you are creating an area under a controller. You can create an area under another area also.

**Step 6** Enter a name for the area. The Controller name is automatically populated, and it is editable.

**Step 7** Select a parent area from the drop-down list. By default, **Global** is the parent area.

**Step 8** Click **Add**.

A message displays 'Successfully Created Area'.

**Step 9** Click **OK**.

**Note** There is another workflow using which you can add an area, site, or floor. Go to the **Controller Overview** page, click the **Add actions** icon that is displayed at the top right corner of the screen, and then select the appropriate options from the menu.

# Editing an Area

This procedure shows how to edit an area.

**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 the Controller and click the collapse icon >.

The list of area is displayed.

**Step 5** Click the **View Actions(…)** icon, and then click **Edit Area**.

The **Edit Area** window appears.

**Step 6** Make the changes as required. Click **Save Changes**.

A message displays 'Site Successfully Updated'.

**Step 7** Click **OK**.

# Deleting an Area

This procedure shows how to delete an area.

**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 the Controller and click the collapse icon >.

The list of area is displayed.

**Step 5** Click the **View Actions(…)** icon, and then click **Delete Area**.

The **Delete Area** window appears.

**Note** You cannot delete a site (Area/Building) if it has a child. Delete the child first and then delete the site.

**Step 6** Click **Delete**.

A message displays 'Area Successfully Deleted'.

**Step 7** Click **OK**.

# Adding a Building

Buildings have a physical address and contain floors and floor plans. When you create a building, you must specify a physical address.

**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 the controller where you want to create a network hierarchy.

**Step 5** Click the **View Actions(…)** icon, and then click **Add Site**.

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

**Step 6** Enter a name for the building.

**Step 7** In the **Street Address** text field, enter an address. If you are connected to the Internet, as you enter the address, the system narrows down the known addresses to the one you enter. When you see that the correct address appears in the window, select it.

**Step 8** Click **Next**.

**Step 9** You can change the Controller name, which is automatically populated. The Parent Area is automatically populated, and you can change it.

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

A message displays 'Successfully Created Site'.

**Step 11** Click **Close**.

# Editing a Building

This procedure shows how to edit the building information.

**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 the Controller and click the collapse icon >.

The list of area is displayed.

**Step 5** Click the collapse icon > till you see the building you want to edit.

**Step 6** Click the **View Actions(…)** icon, and then click **Edit Site**.

The **Edit Site** window appears.

**Step 7** Make the changes as required. Click **Save Changes**.

A message displays 'Site Successfully Updated'.

**Step 8** Click **OK**.

# Deleting a Building

This procedure shows how to delete a building.

**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 the Controller and click the collapse icon >.

The list of area is displayed.

**Step 5** Click the collapse icon > till you see the building you want to delete.

**Step 6** Click the **View Actions(…)** icon, and then click **Delete Site**.

You are prompted before deleting a building.

**Step 7** Click **Delete**.

A message displays 'Building Successfully Deleted'.

**Note** You cannot delete a building if:

- It has floors (child sites)
- A device attached to it
- It is used in fabric as site domain

**Step 8** Click **OK**.

# Adding Floors to a Building

After you add a building, you can create floors in that building.

**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 the Controller and click the collapse icon >.

The list of area is displayed.

**Step 5** Click the collapse icon > till you see the building where you want to add the floors.

**Step 6** Click the **View Actions(…)** icon, and then click **Add Floor**.

The **Floor Information** window is displayed.

**Step 7** Enter a name for the floor. The floor name has a 21-character limit. The floor name must start with a letter or a hyphen (-) and the string following the first character can include one or more of the following:

- Upper or lowercase letters or both
- Numbers
- Underscores (_)
- Hyphens (-)

- Periods (.)
- Spaces ( )

**Step 8** The Controller name is automatically populated, and it is editable.

**Step 9** Define the type of floor by choosing the Radio Frequency (RF) model from the **Type (RF Model)** drop-down list: **Indoor High Ceiling**, **Outdoor Open Space**, **Drywall Office Only**, and **Cubes And Walled Offices**. This defines if the floor is an open space or a drywall office, and so on. Based on the RF model selected, the wireless signal strength and the distribution of heatmap is calculated.

**Step 10** Enter the **Width**, **Length**, and **Height** of the floor.

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

A message displays 'Successfully Created Floor'.

**Step 12** Click **Close**.

# Editing a Floor

This procedure shows how to edit the floor information.

**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 the Controller and click the collapse icon >.

The list of area is displayed.

**Step 5** Click the collapse icon > till you see the floor you want to edit.

**Step 6** Click the **View Actions(…)** icon, and then click **Edit Floor**.

The **Edit Floor** window is displayed.

**Step 7** Make the changes as required. Click **Save Changes**.

A message displays 'Floor Successfully Updated'.

**Step 8** Click **Close**.

# Deleting a Floor

This procedure shows how to delete a floor.

**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 the Controller and click the collapse icon >.

The list of area is displayed.

**Step 5** Click the collapse icon > till you see the floor you want to delete.

**Step 6** Click the **View Actions(…)** icon, and then click **Delete Floor**.

You are prompted before deleting a floor.

**Note** You cannot delete a floor if:

- There is a device attached to it in Cisco DNA Center
- It is used in fabric as site domain

**Step 7** Click **Delete**.

A message displays 'Floor Successfully Deleted'.

**Step 8** Click **OK**.

# Viewing Network Hierarchy

You can view the details of a network hierarchy on the Tenant Workspace. Cisco MSX displays the following details for a site:

- All the buildings on the Tenant Sites
- Building address
- Network hierarchy on which a building belongs
- Network devices deployed on a building
- Floors in a building
- All devices associated with a building

## Viewing Buildings

This procedure shows how to view building information.

**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 **Sites**.

All the sites attached to a tenant are displayed. To view the buildings on the map, zoom in. When you zoom in, you can see the overall health status of a building.

**Step 4** Click on a site to view the building details.

The page displays all the devices that are attached to a building. From this page, you can apply a template and delete a device. Click the **Ellipsis (…)** to see the menu options. For more information on applying a template and deleting a device, see Provisioning a Device

# Viewing Devices

This procedure shows how to view device information.

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

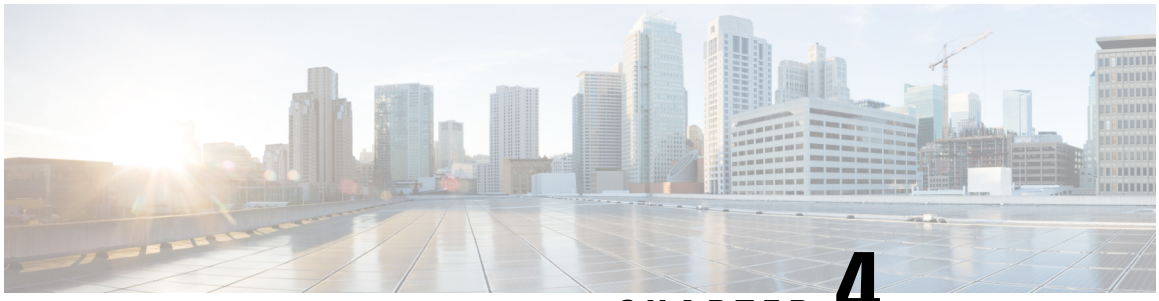
**Step 2** From the left pane, click **Tenant Workspace** and then choose a tenant from the drop-down list.

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

All the devices attached to a tenant are displayed. From this page, you can apply a template and delete a device. Click the **Ellipsis (…)** to see the menu options. For more information on applying a template and deleting a device, see Provisioning a Deviceand Deleting a Device respectively.

**Step 4** From the list, click on a device to view the device summary.

**Step 5** Click **Device Details** to see the device details.



CHAPTER 4

# Managing Devices and Templates

This chapter has the following sections:



# 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.

**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 2: 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.<br>**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 3: 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:<br>• **Authentication and Privacy**; Provides both authentication and encryption.<br>• **Authentication and No Privacy**: Provides authentication, but does not provide encryption.<br>• **No Authentication and No Privacy**: Does not provide authentication or encryption. |

| Field | Description |
|---|---|
| **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:<br>• **SHA**: Authentication based on HMAC-SHA.<br>• **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:<br>• **AES128**: CBC mode AES for encryption.<br>• **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.<br>**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 4: CLI Credentials*

| Field | Description |
|---|---|
| **Protocol** | Network protocol that enables Cisco DNA Center to communicate with remote devices. Valid values are **SSH2** or **Telnet**.<br>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. |
| **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.

**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 5: 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 6: 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:<br>• **Authentication and Privacy**: Provides both authentication and encryption.<br>• **Authentication and No Privacy**: Provides authentication, but does not provide encryption.<br>• **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:<br>• **SHA**: Authentication based on HMAC-SHA.<br>• **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:<br>• **AES128**: CBC mode AES for encryption.<br>• **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. |

**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 7: 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.<br>For security reasons, enter the password again as confirmation. |
| **Enable Password** | Password used to move to a higher privilege level in the CLI.<br>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.

**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.

**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.

**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 8: 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.

**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.

**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**.

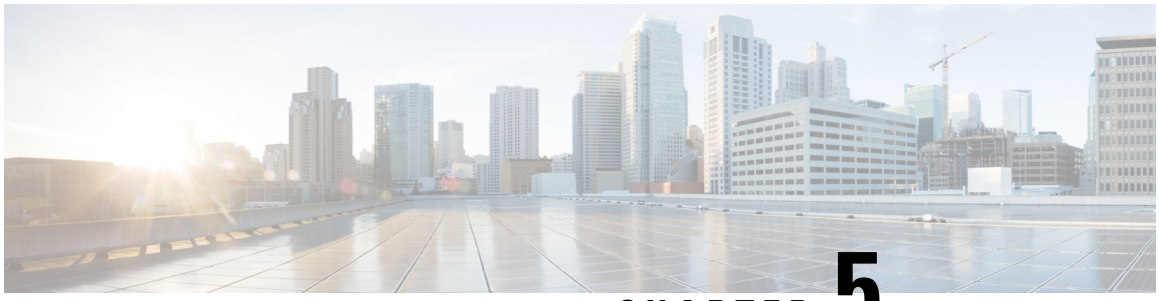
You are prompted before you delete the template.

**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**.



CHAPTER 5

# Managing Fabrics

This chapter has the following sections:



## Managing Fabrics

A fabric is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.

The Cisco MSX allows you to add devices to a fabric network. These devices can be configured to act as control plane, border or edge devices within the fabric network.

## Creating a Fabric Domain

**Before you begin**

- Pre-provision the underlay infrastructure as defined in the Cisco DNAC SD-Access LAN Automation Deployment Guide.
- Create policy definitions that reflect your organization's business intent for a particular aspect of the network, such as network access. See, Cisco DNA Center Users Guide, Release 2.2.2.

**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 **Service Controls**.

The list of service controls attached to a tenant is displayed.

**Step 4** Click **Fabric Management**.

The **Fabric Management** window is displayed.

**Step 5** Click **Add Fabric (+)** icon.

The **Add Fabric** window is displayed.

**Step 6** Enter a name and description for the fabric.

**Step 7** Click **Next**.

**Step 8** Choose a controller from the drop-down list.

**Step 9** Choose a site from the drop-down list.

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

A message displays 'Successfully Created Fabric'.

**Step 11** Click **Close**.

# Viewing Fabric Details

You can view the following fabric details in the Fabric Management page:

- Controller name
- Number of site domains
- Devices in a fabric
- Authentication template
- Virtual networks
- Port assignment: You have to go to Cisco DNA Center to view the port assignment information.
- Wireless SSID
- Devices at the site domain
- Last Sync Time

**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 **Service Controls**.

The list of service controls attached to a tenant is displayed.

**Step 4** Click **Fabric Management**.

The **Fabric Management** window is displayed with the list of fabrics.

**Step 5** Choose a fabric from the list by clicking on it. You can also click on **View Actions(…)** icon and click **View Details**.

The **Fabric Management** window displays the fabric details. You can modify the fabric details in Cisco DNA Center. Click **Modify on Cisco DNA Center** to launch the Cisco DNA Center.

You can configure the following details in Cisco DNA Center:

- Authentication template
- Port assignment
- Wireless SSID
- Segmenting your virtual network

  To configure the details, click the **launch** icon to launch the Cisco DNA Center.

# Deleting a Fabric

Before you delete a fabric, ensure that you have deleted the site domain. You can delete a fabric only if you have deleted the site domain.

**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 **Service Controls**.

The list of service controls attached to a tenant is displayed.

**Step 4** Click **Fabric Management**.

The **Fabric Management** window is displayed with the list of fabrics.

**Step 5** Choose a fabric from the list. Click the **View Actions(…)** icon and then click **Delete Fabric**.

A message displays 'Fabric Successfully Deleted'.

**Note** If the fabric contains a site domain, you cannot delete it. You will get a message 'Failed to Delete Fabric'. Delete the site domain first and then delete the fabric. For more information, see Deleting a Site Domain.

# Deleting a Site Domain

This procedure shows how to delete a site domain.

**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 **Service Controls**.

The list of service controls attached to a tenant is displayed.

**Step 4** Click **Fabric Management**.

The **Fabric Management** window is displayed with the list of fabrics.

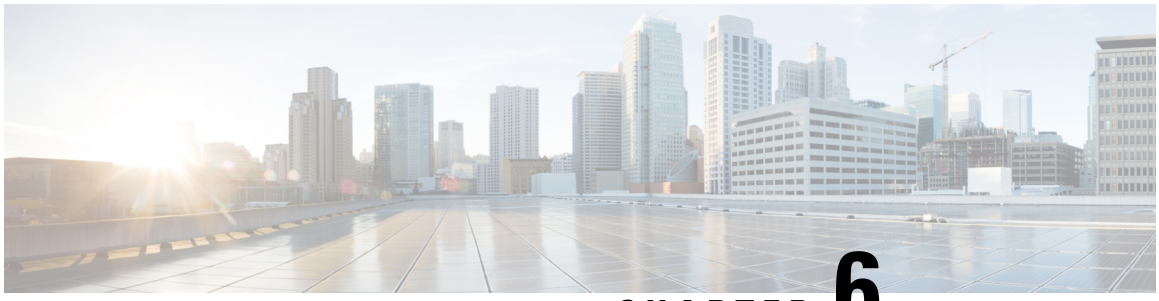
**Step 5** Choose a fabric from the list. Click the **View Actions(…)** icon and then click **Delete Site Domain**.

**Delete Site Domain** window is displayed.

**Step 6** From the **Site Domain** drop-down list, select a site domain.

**Step 7** Click **Delete**.

A message displays 'Site Domain Successfully Deleted'.



CHAPTER 6

# Managing Centralized Configuration Templates

This chapter has the following sections:



## Managing the Centralized Configuration Templates

Cisco MSX Enterprise Access service pack allows you to create and manage device CLI configuration templates. You can deploy these templates across tenants. The templates can contain parameterized variables applied to specific device family types. You can deploy these templates to one or more Cisco DNA Center at the same time. The feature allows you to:

- Create, edit, and delete templates
- Add notes and comments
- Associate one or more templates to one or more tenants
- Dissociate (only if not deployed) a template from a tenant
- Identify the applicability of the template for:
    - Device family, for example, routers, switches, wireless devices, and so on
    - Device series, for example, Cisco Catalyst 9800 Series Wireless Controllers
    - Device type, for example, Catalyst 9000-CL Wireless Controller
    - Operating system, for example, IOS-XE
    - Operating system version, for example, 10.0

# Creating a Configuration Template

To create a configuration template:

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

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

The **Template Management** window is displayed.

**Step 3** Select **Enterprise Access**.

The **Enterprise Access Template Management** window is displayed with the templates that are currently available in the Cisco MSX library.

**Note** Only templates for Enterprise Access will show up in this page.

**Step 4** Click the + icon (**Create Template**) displayed at the top-right corner of the page.

The **Create Template** wizard is displayed with instructions to create a template.

**Step 5** Click **Next**.

**Step 6** In the **Name** text box, enter a unique name for the template.

**Step 7** (Optional) In the **Description** text box, enter a description for the template.

**Step 8** (Optional) In the **Notes** text box, enter note.

**Step 9** Click **Next**.

**Step 10** In the **Template CLI** area, enter the CLI commands.

**Step 11** In the **Template Applicability** area, choose the device applicability for Family, Series, or Device Type from the listed devices. Click the > icon to collapse the list of devices. You can select one of more device applicabilities.

**Step 12** From the **Software Type** drop-down list, choose a software type.

**Step 13** (Optional) In the **Software Version** text box, enter the software version.

**Step 14** Click **Next**.

The template is created. It may take a while before the template is ready for assignment.

**Step 15** Click **Close**.

# Assigning a Configuration Template to a Tenant

You can assign a configuration template to one or more tenants in Cisco MSX. After you assign a template, you can see the template in the **Tenant Workspace** and deploy it on a domain controller and provision the device.

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

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

The **Template Management** window is displayed.

**Step 3** Click **Enterprise Access**.

The **Enterprise Access Template Management** window is displayed with the templates that are currently available in the Cisco MSX library.

**Step 4** From the list, choose a template and click the ellipsis (**…**), and click **Assign Tenants**.

A wizard is displayed with instructions to assign templates.

**Step 5** From the **Select tenants** drop-down list, choose a tenant.

**Step 6** Click **Next** to confirm the assignment.

The process of assigning template starts. It may take approximately one minute to assign a template.

**Step 7** (Optional) Click **View Template Activity** to view the progress of the assignment.

**Note** Not all assignments are successful.

**Step 8** (Optional) Click **Continue to Template Library** to view the template library.

# Unassigning a Configuration Template from a Tenant

You can unassign a template from a tenant. After you unassign a template, you cannot retrieve the list of templates associated with that tenant. To unassign a template:

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

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

The **Template Management** window is displayed.

**Step 3** Select **Enterprise Access**.

The **Enterprise Access Template Management** window is displayed with the templates that are currently available in the Cisco MSX library.

**Step 4** Click a template name. The page displays four tabs: **Applicability**, **Tenants**, **CLI**, and **Notes**.

**Step 5** Click **Tenants** tab.

The window displays the list of tenants assigned to a template.

**Step 6** Choose a tenant from the list and click **X** to unassign the template from the tenant.

You are prompted before you unassign the template.

**Step 7** Click **Unassign**.

# Deploying a Configuration Template in Cisco DNA Center

You can deploy one or more templates in Cisco DNA Center.

**Note** If you want to deploy the same template for a second time to the same controller, you have to undeploy it first and then deploy it again.

To deploy a configuration template:

**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 **Service Controls**.

The list of service controls attached to a tenant is displayed.

**Step 4** Click **Enterprise Access**.

**Step 5** Click **Template Management**.

The **Template Management** window is displayed with the templates that are assigned to the tenant.

**Step 6** From the list, choose a template and click the ellipsis (**…**), and then click **Deploy Template**. Alternatively, you can also click a template name, click the **Controllers** tab, and click **Deploy Template** to deploy a template.

The **Deploy to Controllers** window is displayed.

**Step 7** Click **Next**.

**Step 8** Choose one or more controllers from the list.

**Step 9** Click **Next**.

**Step 10** From the **Project** drop-down list, choose a project. If no projects are displayed in the drop-down list, then you can enter a new project name.

**Step 11** From the **Tags** drop-down list, choose a tag. If the tag you specified does not exist on the controllers, then you can enter new tags. After entering a tag name, click **Add new**. Note that you can add multiple tags.

**Note** You can create new projects and tags, and not select them. After you click **Add new** and enter a project name or tag, the new project and tag will be stored in Cisco MSX, and you can use them later when you deploy a template, as required. Also, note that if you unselect a newly created tag or project, it will not be saved. The saved tags and projects are saved on a per tenant basis.

**Step 12** Click **Next**.

The **Review** window is displayed with the details you selected.

**Step 13** Review the details and click **Next**.

A message displays 'Successfully Initiated Deployment'.

**Step 14** Click **Close**.

# Undeploying a Configuration Template from Cisco DNA Center

You can undeploy a configuration template from Cisco DNA Centre. To undeploy a configuration template:

**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 **Service Controls**.

The list of service controls attached to a tenant is displayed.

**Step 4** Click **Enterprise Access**.

**Step 5** Click **Template Management**.

The **Template Management** window is displayed with the templates that are assigned to the tenant.

**Step 6** Click a template name. The page displays four tabs: **Controllers**, **Applicability**, **CLI**, and **Notes**.

**Step 7** Click **Controllers**.

The controllers that are assigned to the template are listed.

**Step 8** Choose a controller from the list, click the ellipsis (**…**), and then click **Undeploy**.

You are prompted before you remove the template.

**Step 9** Click **Undeploy**.

A message displays 'Undeployment Initiated'.

**Step 10** Click **Okay**.

# Viewing Configuration Templates

After you create a configuration template, you can view the details of the template in the **Enterprise Access Template Management** page. To view the details:

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

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

The **Template Management** window is displayed.

**Step 3** Select **Enterprise Access**.

The **Enterprise Access Template Management** window is displayed with the templates that are currently available in the Cisco MSX library.

**Step 4** Click a template name. The page displays four tabs: **Applicability**, **Tenants**, **CLI**, and **Notes**. Click a tab to view the details:

- **Applicability**: Displays the applicability of the templates. It lists all the applicable devices supported by a template and the operating system.

- **Tenants**: Displays tenants assigned to a template. From this tab, you can assign a tenant to a template. Click the + icon (**Add Tenant).** For more information, see Assigning/Unassigning Template to a Tenant.
- **CLI**: The CLI configuration applied to a template.
- **Notes**: Any note that was entered.

**Step 5** Click **Close** to close the display of template details.

# Viewing Configuration Templates for a Specific Tenant

To view the configuration templates assigned to a tenant:

**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 **Service Controls**.

The list of service controls attached to a tenant is displayed.

**Step 4** Click **Enterprise Access**.

**Step 5** Click **Template Management**.

The **Template Management** window is displayed with the templates assigned to the tenant.

**Step 6** Click a template name. The page displays four tabs: **Controllers**, **Applicability**, **CLI**, and **Notes**. Click a tab to view the details:

- **Controllers**: Lists all the controllers attached to a template. If no controllers are listed, you can create controllers from here and deploy a template. To deploy a template, click **Deploy Template**. For more information, see Deploying/Undeploying a Template in Cisco DNAC.
- **Applicability**: Displays the applicability of the templates. It lists all the applicable devices supported by a template and the operating system.
- **CLI**: The CLI configuration applied to a template.
- **Notes**: Any note that was entered.

**Step 7** Click **Close** to close the display of template details.

# Viewing Deployment History

Template history lists the history of all the activities performed on a template. To view the template history:

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

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

The **Template Management** window is displayed.

**Step 3** Select **Enterprise Access**.

The **Enterprise Access Template Management** window is displayed with the templates that are currently available in the Cisco MSX library.

**Step 4** Click the clock icon (**History**) displayed at the top-right corner of the page.

The template history is displayed.

**Note** The template history shows the events related to creation, deletion, assignment, and unassignment of templates.

## Viewing the Template History of a Tenant

To view the template history of a tenant:

**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 **Service Controls**.

The list of service controls attached to the tenant is displayed.

**Step 4** Click **Enterprise Access**.

**Step 5** Click **Template Management**.

The **Template Management** window is displayed with the templates that are assigned to the tenant.

**Step 6** Click the clock icon (**History**) displayed at the top-right corner of the page.

The template history is displayed.

**Note** The template history shows only the deployment actions.

# Deleting a Configuration Template

You can delete a configuration template from the Template Library. Before you delete a template, ensure that it is not assigned to a tenant. If it is assigned to a tenant, you can't delete it. To delete a configuration template:

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

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

The **Template Management** window is displayed.

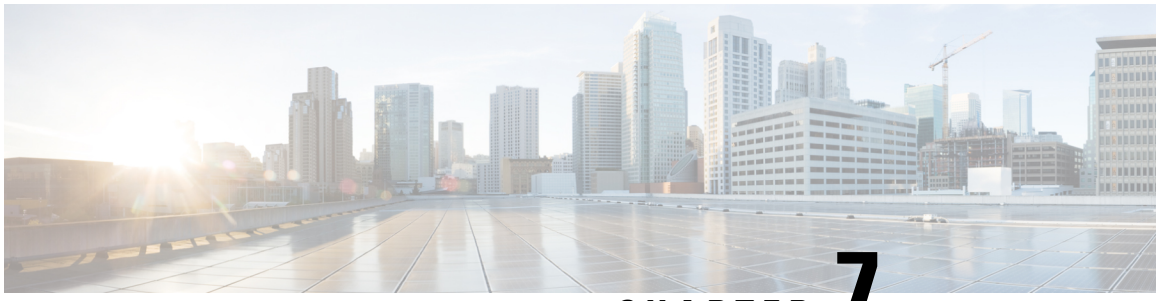
**Step 3** Select **Enterprise Access**.

The **Enterprise Access Template Management** window is displayed with the templates that are currently available in the Cisco MSX library.

**Step 4** From the list, choose a template and click the ellipsis (**…**), and then click **Delete Template**.

You are prompted before you delete a template.

**Step 5** Click **Delete**.



CHAPTER 7

# Provisioning Wireless Devices in Cisco MSX

This chapter describes how to create a WLAN service and provision the devices using Enterprise Access Service Pack.

This chapter has the following sections:



## Overview

Cisco MSX allows you to deploy a Wireless Local Area Network (WLAN) service on an existing switched access network (Non-Fabric). Using this feature, you can:

- Create a new WLAN
- Update an existing WLAN
- View the details of a WLAN
- Delete a configured WLAN
- Deploy WLANs to Controllers
- Undeploy WLAN
- Provision a WLC

# Creating a New Wireless LAN

You can configure WLANs with different SSIDs or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access.

**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 **Service Controls**.

The list of service controls is displayed.

**Step 4** Click **WLAN Management**.

The **WLAN Management** window is displayed with the list of wireless networks.

**Step 5** Click the + icon (**Create Wireless Network**) displayed at the top-right corner of the page.

A wizard is displayed with the instructions to create a new enterprise wireless network.

**Step 6** In the **Name (SSID)** field, enter a unique name for the wireless network or the SSID that you are creating. The name can contain up to 32 alphanumeric characters. All special characters are allowed except < and >.

**Step 7** From the **Starter Configuration** drop-down list, choose a wireless configuration. You can choose **Basic**, **Open**, **Secure Data**, or **Secure Voice and Data**. For more information about the settings, see the Table 9: Network Wireless Settings:

A description of the selected starter configuration is displayed at the bottom of the window.

***Table 9: Network Wireless Settings***

| Network Wireless Settings | Open | Basic | Secure Data | Secure Voice and Data |
|---|---|---|---|---|
| Type Of Enterprise Network | Voice and Data | Voice and Data | Data | Voice and Data |
| Wireless Option | 2.4 GHz only | Dual band operation (2.4GHz and 5GHz) | Dual band operation (2.4GHz and 5GHz) | Dual band operation (2.4GHz and 5GHz) |
| Fast Lane | False | False | True | True |
| Level of Security | Open | WPA2 Personal - Ask Password | WPA2 Enterprise and WPA3 | WPA2 Enterprise and WPA3 |
| **SSID State** | | | | |
| Admin Status | True | True | True | True |
| Broadcast SSID | True | True | True | True |
| **Fast Transition (802.11r)** | | | | |
| Over the DS | NA | NA | True | False |
| Mac Filtering | No | No | No | No |

**Step 8** Click **Next**.

The **General Settings** window is displayed with the starter configuration. You can use the displayed values as it is or you can change the values based on your requirements.

a) From the **Wireless Frequency** drop-down list, choose a frequency for the wireless network.
b) From the **Wireless Type** drop-down list, choose the type of enterprise network: **Voice and Data** or **Data**. The selection type defines the quality of service that is provisioned on the wireless network.

   If you select **Voice and Data**, the quality of service is optimized to access either voice or data traffic.

   If you select **Data** option, the quality of service is optimized for wireless data traffic only.

c) Check the **Admin** checkbox to enable admin status.
d) Check the **Broadcast SSID** checkbox to broadcast the SSID. If you uncheck this, Cisco MSX hides the SSID from clients attempting to connect to this SSID, thereby reducing unnecessary load on the wireless infrastructure.
e) Under **Wireless Security Mode**, click the radio button to choose a security option. The security options are:

   - **Open**: Provides no security. It allows any device to connect to the wireless network without any authentication.

     **Note** If you select **Open**, you cannot select the encryption methods **WPA**, **WPA2**, and **WPA3**.

   - **Personal**: Personal uses pre-shared keys (PSK) and is designed for home use. This doesn't require an authentication server.

     **Note** If you select **Personal**, you have to provide a pre-shared key.

   - **Enterprise**: Enterprise uses IEEE 802.1X, which offers enterprise-grade authentication. Enterprise is designed for use in organizations. This requires a RADIUS authentication server.

     **Note** If you select **Enterprise**, you do not provide a pre-shared key. You have to select at least one encryption method.

   - **WPA**: Provides a minimal level of security using Temporal Key Integrity Protocol (TKIP) encryption method.
   - **WPA2**: Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server.
   - **WPA3**: WPA3 is the latest version of WPA, which is a suite of protocols and technologies that provide authentication and encryption for Wi-Fi networks. WPA3-Enterprise provides higher-grade security protocols for sensitive data networks.

f) Under **Management Frame Protection**, click one of the radio buttons: **Disabled**, **Required**, or **Optional**.

   Management Frame Protection (MFP) increases the security of management frames. It provides security for the otherwise unprotected and unencrypted 802.11 management messages that are passed between access points and clients. MFP provides both infrastructure and client support.

   If you click the **Required** radio button, then the clients are allowed to associate only if the MFP is negotiated (that is, if WPA2 is configured on the wireless controller and the client supports CCXv5 MFP and is also configured for WPA2).

g) Set **Fast Transition** to **Enable**, **Adaptive**, or **Disable** mode.

   Fast transition allows wireless clients to quickly roam from one AP to another AP. Fast transition ensures less disrupted connectivity when a wireless client roams from one AP to another AP.

**Step 9** Click **Next**.

**Step 10** Review the wireless configuration.

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

**Step 12** Click **Close**.

### What to do next

You have created a wireless network. The next step is deploying the network to a wireless controller. For more information, see Deploying WLAN to Controllers.

# Viewing WLAN

**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 **Service Controls**.

The list of service controls is displayed.

**Step 4** Click **WLAN Management**.

The **WLAN Management** window is displayed with the list of wireless networks.

**Step 5** From the list, click a wireless network.

The wireless network information is displayed in two tabs: **Wireless Settings** and **Deployments**. Click **Wireless Settings** to see the wireless settings information. Click **Deployments** to see the status of the wireless deployment on controllers.

**Note** If a WLAN deployment fails, you can see the reason of the failure by clicking the **Deployment Failed** link under the status column in the **Deployments** tab.

# Editing WLAN

**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 **Service Controls**.

The list of service controls is displayed.

**Step 4** Click **WLAN Management**.

The **WLAN Management** window is displayed with the list of wireless networks.

**Step 5** Choose a wireless network and click the **ellipsis (...)** that is located on the far right of the row and choose **Edit WLAN**.

The **Edit Wireless Network** wizard is displayed.

**Step 6** In the General Settings, make changes wherever required. You cannot change the SSID Name. For field descriptions, see Creating a New Wireless LAN, on page 56.

**Step 7** Click **Next**.

**Step 8** Review the wireless configuration.

**Step 9** Click **Next**.

A message 'Wireless Network Saved' is displayed.

**Step 10** Click **Close**.

# Deploying WLAN to Controllers

**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 **Service Controls**.

The list of service controls is displayed.

**Step 4** Click **WLAN Management**.

The **WLAN Management** window is displayed with the list of wireless networks.

**Step 5** From the list, click a wireless network.

The wireless network information is displayed in two tabs: **Wireless Settings** and **Deployments**.

**Step 6** Click the **Deployments** tab.

**Step 7** Click **Deploy WLAN**.

The Deployment wizard is displayed.

**Step 8** Click **Next**.

The list of controllers is displayed.

**Note** The edited WLAN can be re-deployed using the same deployment wizard if the user needs to change WLAN on the controller.

**Step 9** Choose the controllers from the list. The wireless network will be deployed to the controllers you choose.

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

**Step 11** Review your selection. If you want to change the controllers, you can go back.

**Step 12** Click **Next**.

The deployment process starts and a message 'Successfully Initiated Deployment' is displayed.

**Step 13** Click **Close**.

# Undeploying WLAN

**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 **Service Controls**.

The list of service controls is displayed.

**Step 4** Click **WLAN Management**.

The **WLAN Management** window is displayed with the list of wireless networks.

**Step 5** From the list, click a wireless network.

The wireless network information is displayed.

**Step 6** Click the **Deployments** tab.

The list of controllers is listed. These are the controllers where the wireless network is already deployed.

**Step 7** To undeploy a wireless network from a controller, click the **ellipsis (...)** and choose **Undeploy**.

You will be prompted with a message 'Undeploy Wireless Network'.

**Step 8** Click **Undeploy**.

The undeployment process starts and a message 'Undeployment Initiated' is displayed.

**Step 9** Click **Okay**.

# Deleting WLAN

**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 **Service Controls**.

The list of service controls is displayed.

**Step 4** Click **WLAN Management**.

The **WLAN Management** window is displayed with the list of wireless networks.

**Step 5** Choose a wireless network and click the **ellipsis (...)** that is located on the far right of the row and choose **Delete WLAN**.

You will be prompted with a message 'Delete WLAN'.

**Step 6** Click **Delete WLAN**.

A message 'Successfully deleted' is displayed.

# Provisioning WLC

**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** From the list, choose the device you want to provision, click the **Ellipsis (…)** and choose **Provision Device**.

A wizard is displayed with the instructions to provision WLC.

In the **Provision Wireless LAN Controller** window, you have to assign the device to a site and choose one or more access point locations.

**Note** The wizard also supports re-provisioning. If the device is already provisioned and if you are re-provisioning it, the **Site** is pre-selected and you cannot change it.

**Step 5** From the **WLC Device Location** drop-down list, choose a device location.

**Step 6** From the **Managed Access Point Locations** section, choose a location of the access point.

The selected access point locations are displayed at the bottom of the window.

**Step 7** Click **Next**.

The **Managed AP Site Network Profiles** window is displayed with the AP locations and the associated wireless profile. Each managed AP site must be associated with a wireless profile, which can include one or more SSIDs. The profile also includes one or more templates.

**Step 8** If a site is not associated with a wireless profile, you can create a new wireless profile and attach to it. Click a site name.

The row expands and shows the **Network Profile** drop-down list. You can either choose an existing profile or create a new profile.

**Creating a New Profile**:

a) To create a new profile, click **Create New** from the drop-down list.
b) In the **Name** field, enter the profile name.
c) From the **SSID** drop-down list, choose a SSID. You can add more than one SSID for a profile. To add additional SSIDs, click the + icon. Similarly, you can delete an existing SSID by clicking the - icon.
d) Click the radio button to select the type of interface: **Existing Interface** or **New Interface**.

   If you select **Existing Interface**, you can select the interface from the drop-down list. If you select **New Interface**, you can create a new interface and it will be part of the drop-down list. For a new interface, you have to enter the **Interface name** and **VLAN ID**.

e) Check the **Flex Connect Local Switching** check box to enable local switching for the WLAN. When you enable local switching, any FlexConnect access point that advertises this WLAN is able to locally switch data packets.

If you have enabled **Flex Connect Local Switching** for an SSID, then all APs on that particular floor where the network profile is mapped will switch to FlexConnect mode.

f) From the **Templates** drop-down list, choose a template. You can add more than one template. To add additional templates, click the + icon. Similarly, you can delete an existing template by clicking the - icon.

g) Click **Save Network Profile** to save the network profile.

A message 'Network profile successfully saved to controller' is displayed. If you want to update the profile information, you can edit it. To edit the profile, click **Edit Network Profile**.

**Step 9** Click **Next**.

**Step 10** (Optional) Enter the **IP address**, **Gateway**, and **Subnet mask** for each interface. All IP and Gateway addresses must be unique.

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

The **Provide Template Variables** window is displayed.

**Step 12** If you want, you can either add or edit template variables.

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

**Step 14** Review the configuration before you provision your wireless LAN controller.

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

Provisioning the WLC starts and a message 'Started Provisioning Successfully' is displayed. The status of the provisioning will be shown in the device page.

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

# Viewing the Status of Provisioning

You can view the status of WLAN provisioning in the device details page. The device details page lists information like Status of the Device, Applied Template Variables, Managed AP Locations, Wireless Network, and so on.

**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** From the list, click a device that is already provisioned.

The **Device Details** page is displayed with device status and provisioning information.