



Device Compliance

Adding Standard Configuration	2
Adding Standard Configuration Category	3
Creating a ServiceNow Account	6
Adding a Device to Compliance Monitoring	7
Removing a Device from Compliance Monitoring	8
Configuring the Compliance for Devices	8
Remediating Non-compliant Values on a Device	9
Updating Monitored Devices with Standard Configuration	11
Viewing Device Vulnerabilities	12
Viewing Monitored Devices	12
Converting Device Configuration to Device Template	13

Revised: September 17, 2021,

Adding Standard Configuration

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

Standard Configuration involves two parts. The first part is defining the Standard Configuration by creating a set of categories, which is described in [Adding Standard Configuration Category, on page 3](#). After you create the Standard Configuration categories, the second part is providing any dynamic values required, which is described below.

To add or edit standard configuration values:

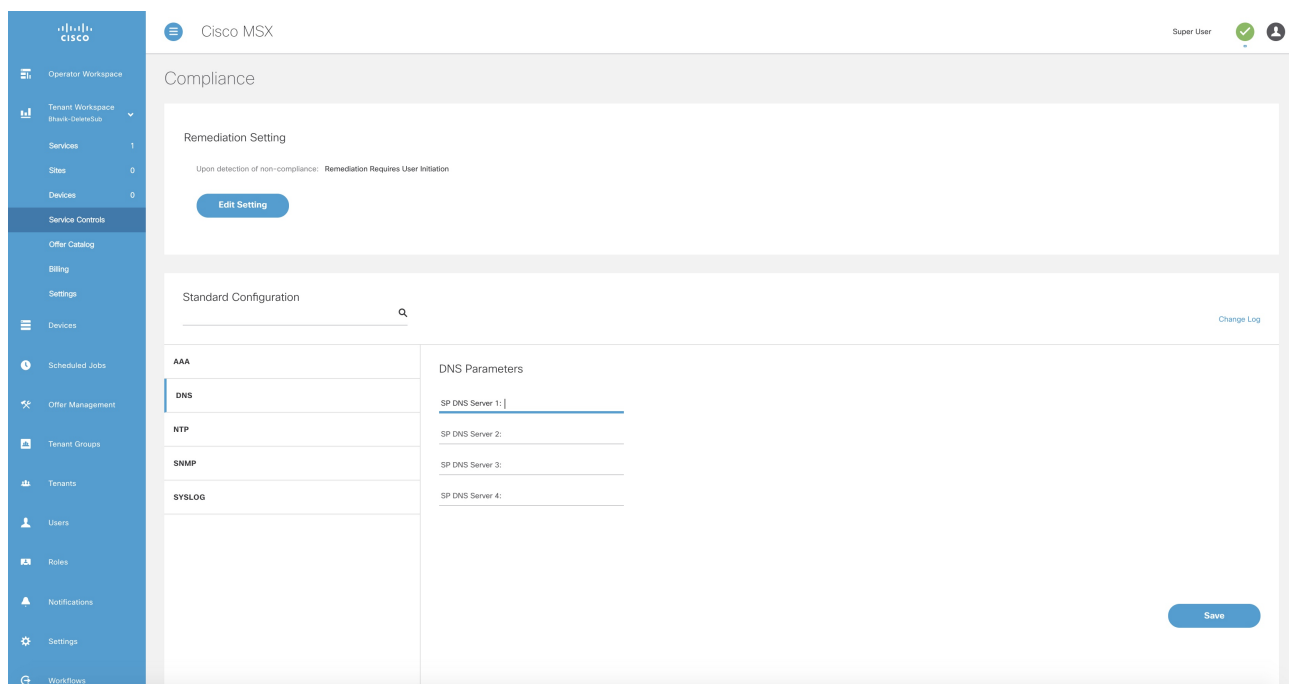
Procedure

Step 1 Log in to the Cisco MSX portal.

Step 2 From the left pane, choose **Tenant Workspace > Service Controls > Compliance**.

The **Compliance** window is displayed.

Figure 1: Compliance Settings



Step 3 In the **Standard Configuration** section, click a category you want to add or edit values.

The category parameters are displayed.

Step 4 Add or edit the parameter values.

Step 5 Click **Save**.

The parameter values are saved to the Standard Configuration.

Adding Standard Configuration Category

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

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

To add a new category to Standard Configuration:



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

- Standard Configuration Manage
 - Device Templates Manage
-

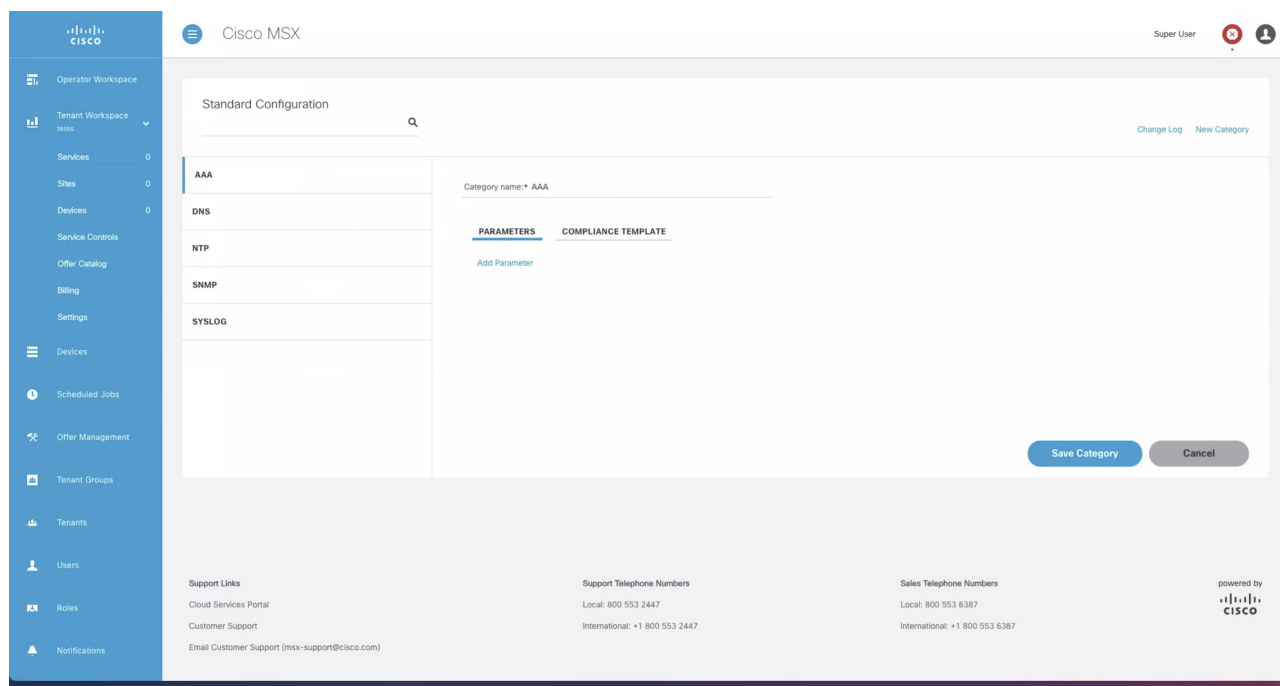
Procedure

Step 1 Log in to the Cisco MSX portal.

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

The **Standard Configuration** window is displayed.

Figure 2: Standard Configuration Settings



- Step 3** Click **New Category**.
- Step 4** In the **Category Name** field, enter a category name.
- Step 5** To create a template, click **COMPLIANCE TEMPLATE** tab.
- Step 6** From the **NED ID** drop-down list, choose a NED ID. The NED represents the device type you want the device template configuration to apply. You can specify multiple NEDs, each with their own specific device template or just a single NED and template.
- Step 7** Enter the configuration in the textbox provided.
- Step 8** Click **Generate Parameters** to generate parameters from the configuration you entered in the template textbox. Parameters that are not already included in the Parameters tab only will be generated.
- Step 9** You can add more than one template to a category. To add another template, click the plus (+) icon. Similarly, to delete a template, click the minus (-) icon.
- Note** To see the template that you already added, scroll down to the bottom of the screen.
- Step 10** To add parameters, click **PARAMETERS** tab and then click **Add Parameter**.
The fields to enter parameter details are displayed.
- Step 11** Enter the **Parameter Name**, **Parameter Description**, and **Parameter Label** in the fields displayed.
- Step 12** From the **Parameter Type** drop-down list, choose a parameter type.
- Step 13** Click the **Optional** radio button if the parameter is optional. Click the **Required** radio button if the parameter is mandatory. Click the **Read Only** radio button if the parameter is a read-only parameter. If you click **Read Only**, then enter the default value of the parameter. This value will be displayed as a read-only value when users access the standard configuration.
- Step 14** You can add more than one parameter to a category. To add another parameter, click the plus (+) icon. Similarly, to delete a parameter, click the minus (-) icon.

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

Step 15 Click **Save Category**.

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

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

Deleting Standard Configuration Category

You can delete a category from the Standard Configuration.

To delete a category:

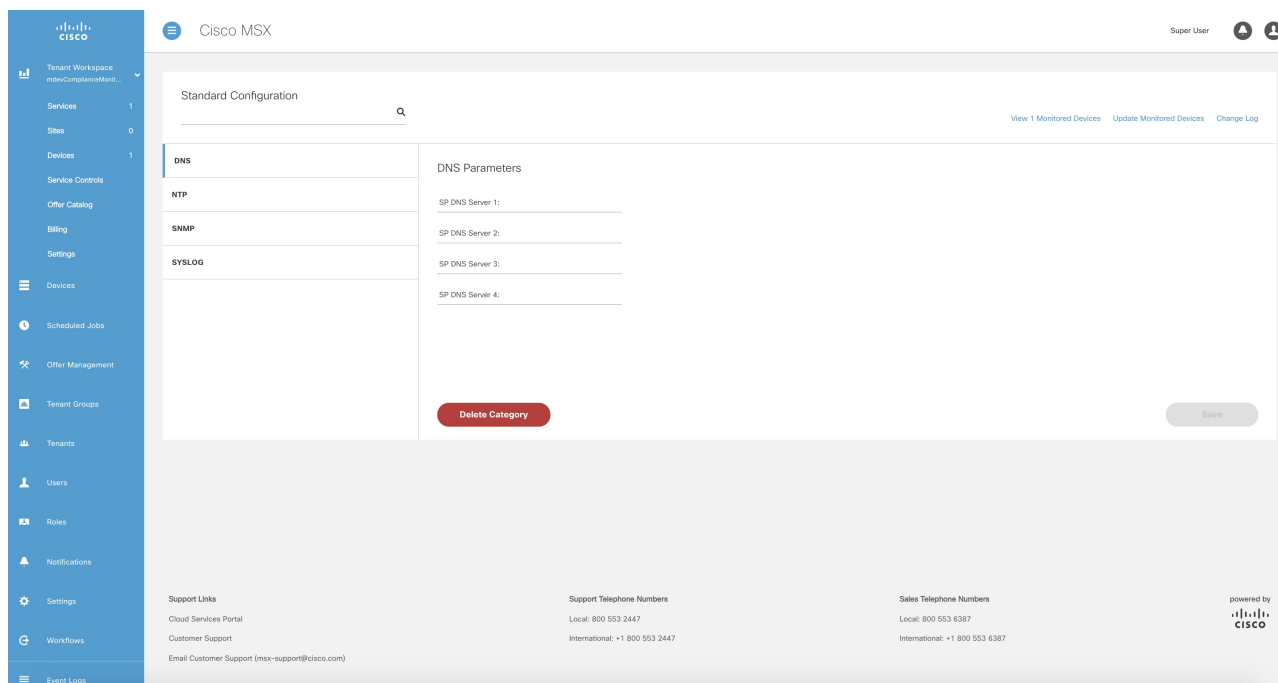
Procedure

Step 1 Log in to the Cisco MSX portal.

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

The **Standard Configuration** window is displayed.

Figure 3: Standard Configuration Settings



Step 3 Click a category from the left pane.

The category information is displayed.

Step 4 Click **Delete Category**.

A message 'Standard Configuration Category Deleted' is displayed.

Creating a ServiceNow Account

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

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

To create a ServiceNow account:



Note You need the following permission to update ServiceNow settings:

- Incidents Manage

Procedure

Step 1 Log in to the Cisco MSX portal.

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

The **ServiceNow** window is displayed.

Figure 4: ServiceNow Settings

The screenshot displays the 'ServiceNow Settings' page in the Cisco MSX interface. The page title is 'ServiceNow Settings' under 'Service Controls'. Below the title, there is a sub-header 'ServiceNow Settings' and a brief instruction: 'Add ServiceNow Integration to create incident tickets for compliance drift and remediation actions. Please supply the following ServiceNow account information'. The form contains the following fields:

- Domain* Domain
- Client Id* Client Id
- Client Secret* Client Secret
- User Name* User Name
- Password* Password
- Caller Caller
- Proxy: https://proxy.someservice.com/

At the bottom of the form, there are two buttons: 'Clear Credentials' and 'Save'. The footer of the page includes 'Support Links' (Cloud Services Portal, Customer Support, Email Customer Support), 'Support Telephone Numbers' (Local: 800 553 2447, International: +1 800 553 2447), and 'Sales Telephone Numbers' (Local: 800 553 6387, International: +1 800 553 6387). The page is powered by Cisco.

Step 3 In the **Domain** field, enter a domain name.

Step 4 In the **Client Id** field, enter a client id.

- Step 5** In the **Client Secret** field, enter a client secret.
- Step 6** In the **User Name** field, enter your user name.
- Step 7** In the **Password** field, enter your password.
- Step 8** In the **Caller** field, enter the caller name. The Caller is the person contacting the Service Desk to get an incident registered. We recommend creating a ServiceNow user called 'MSX' (in ServiceNow) and providing 'MSX' as the Caller in the ServiceNow settings.
- Step 9** (Optional) In the **Proxy** field, enter a proxy URL.
- Step 10** Click **Save**.

A message 'ServiceNow Configuration Saved Successfully' is displayed.

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

Adding a Device to Compliance Monitoring

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

To add a device to compliance monitoring:

Procedure

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

Removing a Device from Compliance Monitoring

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

To remove a device from compliance monitoring:

Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.
The **Devices** tile is displayed with the list of devices.
- Step 3** Choose a device or devices from the list.
- Step 4** If you choose a single device, click the **ellipsis (...)** that is located far right on the same row and then choose **Remove from Compliance Monitoring**. If you choose multiple devices, click the **ellipsis (...)** that is located far right above all devices, and then choose **Remove from Compliance Monitoring**.
The **Remove Device from Compliance Monitoring** dialog box is displayed. The dialog box provides information about how many devices will be removed from monitoring.
- Step 5** Click **Remove from Monitoring**.
A confirmation message is displayed.
- Step 6** Click **Close**.
-

Configuring the Compliance for Devices

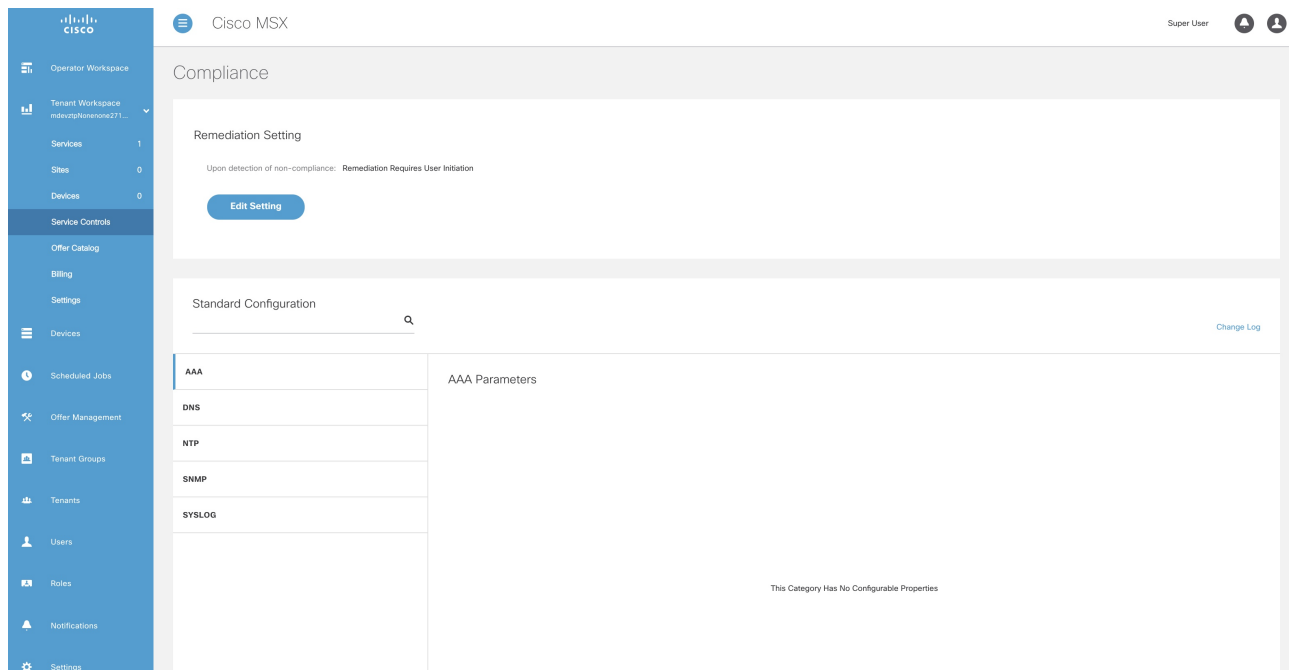
You can edit the compliance remediation settings of devices. You can either choose automatic remediation or user initiated remediation.

To edit compliance settings:

Procedure

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

Figure 5: Compliance Settings



- Step 3** Click **Edit Setting** to change the compliance settings.
The **Remediation Settings** window is displayed.
- Step 4** Click the **Remediation Requires User Initiation** radio button if user initiation is required for remediation. If you choose this option, the values will not be reverted to standard values until you initiate it from your side.
- Click **Save Settings**.
A message 'Compliance Settings were Saved Successfully' is displayed.
- Step 5** Click the **Non-compliance Values Reverted When Detected** radio button if you want automatic remediation. If you choose this option, devices are automatically reverted to standard configuration values when non-compliant values are detected. You will be notified of the changes.
- Click **Save Settings**.
The **Confirm Automatic Remediation Setting** dialog box is displayed.
 - Click **Confirm**.
A message 'Compliance Settings were Saved Successfully' is displayed.

Remediating Non-compliant Values on a Device

Deviations on a device from the Standard Configuration can be remediated in two ways. The first option is to revert the changes on the device to the Standard Configuration values. The second option is to accept the non-complaint values on the device. This action

will track the exception for this device and not warn again if the device is checked again for deviation drift. Changing the Standard Configuration value will negate any exceptions stored for a device against the changed Standard Configuration value.

To remediate non-compliance values:

Procedure

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, choose **Tenant Workspace > Devices**.
The **Devices** tile is displayed with the list of devices.
- Step 3** From the list, click a device.
The device summary is displayed.
- Step 4** Click **Device Details**.
The device metric page lists the device information.
- Step 5** From the **Compliance** section, click **Remediate**.
The **Remediate Non-Compliant Values** window is displayed. From the remediation options, you can either choose **Revert to Standard Configuration Values** or **Accept Devices Values**.
- Step 6** Click **Revert to Standard Configuration Values** if you want to revert the values to standard configuration.
- Click **Next**.
The **Scheduling Options** window is displayed. You can remediate now or schedule the remediation for a later date.
 - Click **Remediate Now** to remediate the values immediately. Click **Next**.
Review the remediation details and click **Next**. The remediation process initiates and a message 'Remediation Initiated' is displayed.
 - Click **Schedule Remediation** to schedule the remediation for a later date.
 - If you click **Schedule Remediation**, you can either schedule a new job or add to an existing job.
 - To schedule a new job, click the **New Schedule Job** radio button.
In the **Schedule Job Name** field, enter a name for the schedule job.
In the **Date and Time** field, choose a date and time.
 - To add to an existing job, click the **Add to Existing Scheduled Job** radio button.
From the **Schedule Job** drop-down list, choose an existing schedule job.
 - Click **Next**.
The **Review Remediation** window is displayed.
 - Review the remediation details and click **Next**.
The remediation process initiates and a message 'Remediation Initiated' is displayed.
 - Click **Done**.
- Step 7** Click **Accept Devices Values** if you want to accept the values as compliant despite their differences with the standard configurations.

a) Click **Next**.

The **Review Remediation** window is displayed.

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

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

c) Click **Done**.

Updating Monitored Devices with Standard Configuration

You can update all the monitored devices with standard configuration.

To push standard configuration to monitored devices:

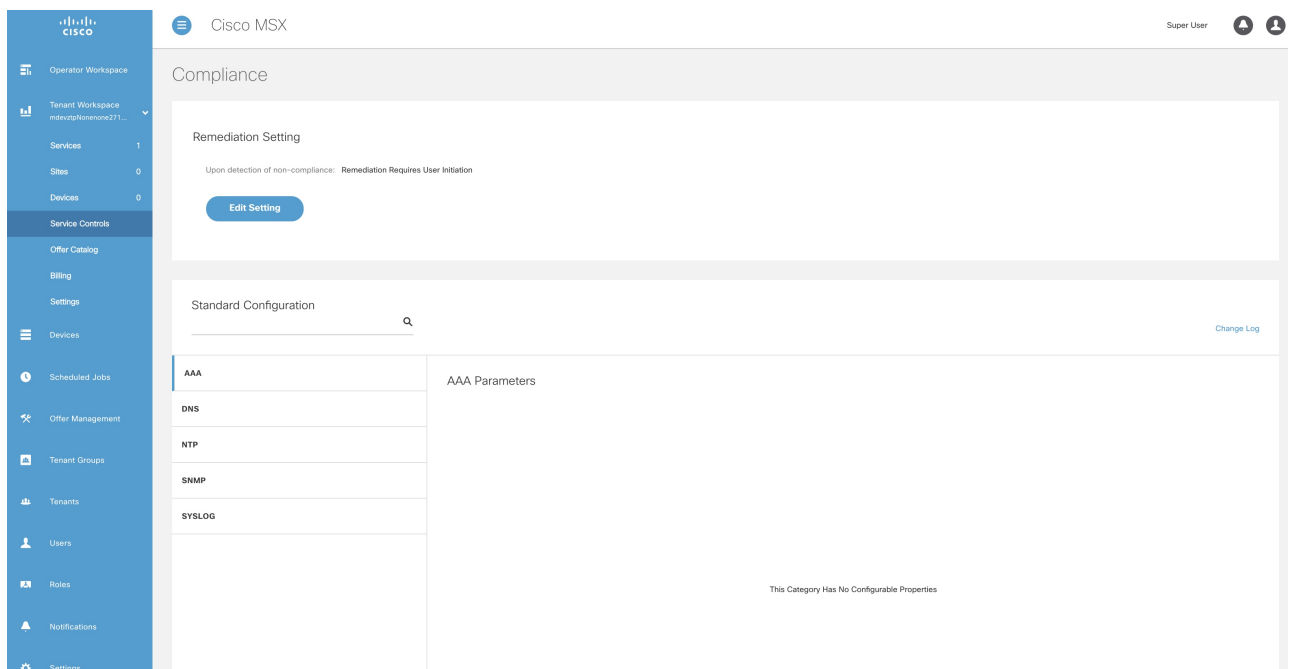
Procedure

Step 1 Log in to the Cisco MSX portal.

Step 2 From the left pane, choose **Tenant Workspace > Service Controls > Compliance**.

The **Compliance Settings** window is displayed.

Figure 6: Compliance Settings



Step 3 Click **Update Monitored Devices**.

The **Push Standard Config to Monitored Devices** window is displayed.

Step 4 Click **Update Devices**.

A message 'Standard Configuration Saved Successfully' is displayed.

Viewing Device Vulnerabilities

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

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

To view the device vulnerabilities:

Procedure

Step 1 Log in to the Cisco MSX portal.

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

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

Step 3 From the list, click a device.

The device summary is displayed.

Step 4 Click **Device Details**.

The device metric page lists the device information. Go to **Vulnerabilities** tile to see the device vulnerabilities.

Viewing Monitored Devices

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

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

To view all the devices under compliance monitoring:

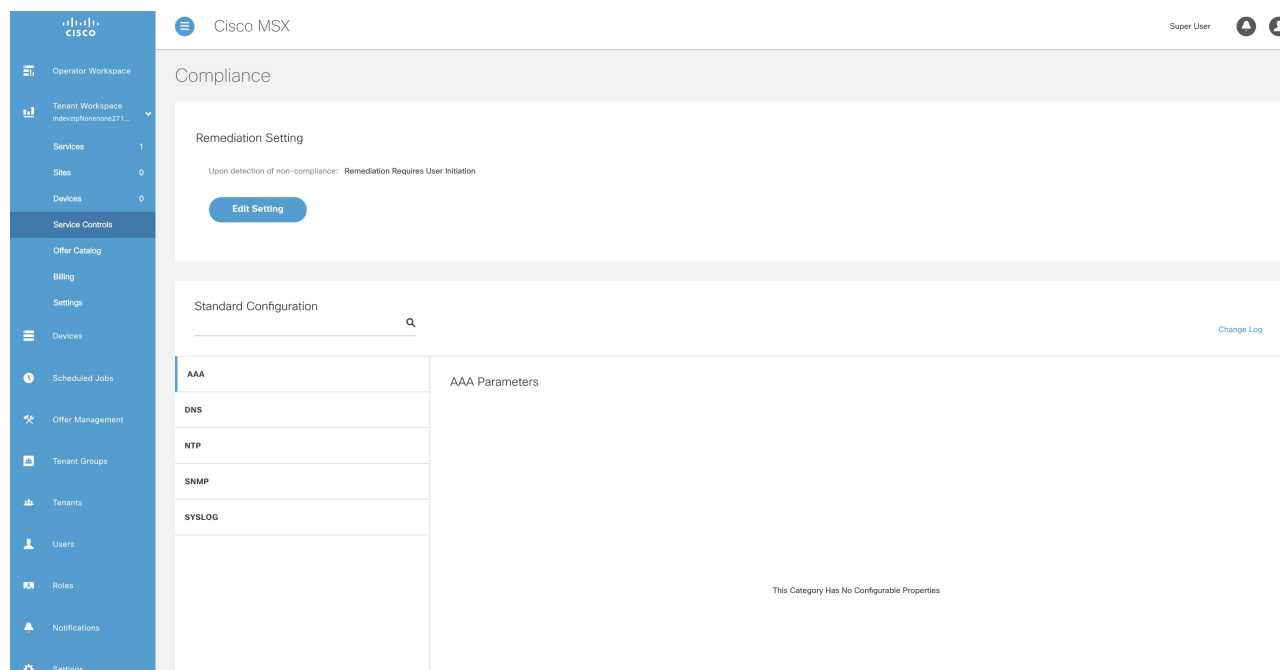
Procedure

Step 1 Log in to the Cisco MSX portal.

Step 2 From the left pane, choose **Tenant Workspace > Service Controls > Compliance**.

The **Compliance Settings** window is displayed.

Figure 7: Compliance Settings



Step 3 Click **View Monitored Devices**.

The list of devices under compliance monitor is displayed.

Step 4 To filter the devices based on compliance criteria, choose a filtering option from the **Compliance** drop-down list.

Converting Device Configuration to Device Template

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

To convert device configuration to device template:

Procedure

Step 1 Log in to the Cisco MSX portal.

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

The **Templates** window is displayed.

Step 3 In the **Select A Configurational Template** section, click the **ellipsis (...)** and choose **CLI to Template** from the menu.

The **Convert Device Configuration to Template** window is displayed.



Convert to Template

In this dialog you can convert a native device format into an XML device template and will have the option to copy or download that file after conversion is complete


NED ID: cisco-ios-cli-6.37 ▼

Native Device Format

```
ip domain name cisco.com
ip name server 8.8.8.8
```

Device Template  

```
<config>
<ip xmlns="urn:ios">
  <domain>
    <name>cisco.com</name>
  </domain>
</ip>
</config>
```



Close

Figure 8: Convert to Template

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



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

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

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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