Getting Started with Cisco Managed Services Accelerator

Cisco Managed Services Accelerator (MSX) is an open software platform that enables service providers to create and manage services across physical and virtual network elements. The MSX solution utilizes network function virtualization and enables service providers to provide their customers a flexible selection of services that are easily customized through a self-service portal. It reduces the costs for service creation, customer acquisition, service fulfillment, time to repair, and maintenance. With Cisco MSX solution, you can automate end-to-end provisioning for different use cases and service topologies. Each release of the MSX provides out-of-box capabilities to orchestrate particular use cases, also called service packs (such as, SD-WAN, vBranch, and Managed Devices). The MSX service packs are a suite of prepackaged software capabilities that fully automate the end-to-end service creation including ordering, service chaining, orchestration, service assurance, user self care, real time performance reporting, and user-defined policy changes. With these fully validated service level packages, end customers can quickly turn on, control, and ensure cloud-based managed services offered by the service provider. For detailed information about MSX solution, see Cisco Managed Services Accelerator (MSX) Solution Overview Guide.

For information on MSX platform or service pack installation, see the latest version of Cisco MSX Installation Guide on cisco.com.

This chapter contains the following topics:

- Logging In and Out of the MSX Portal, on page 1
- Configuring Integrations for Outbound APIs, on page 2
- Enabling Multiple Subscriptions for a Tenant, on page 2
- Enabling Notification for Events, on page 3
- Defining Terms and Conditions for a Service, on page 6
- Configuring an Announcement, on page 6
- Registering a Device on MSX, on page 7

Logging In and Out of the MSX Portal

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

https://<server-ip>/vms 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 ensures the security of the connection between your client and the Cisco MSX web server.

Your user account privileges determine what you can see and do in the user interface. For information on Cisco MSX users and the actions they can perform, see Managing User Roles.

To log out, in the left pane of the MSX Portal, click **Logout**.

### Configuring Integrations for Outbound APIs

Using this procedure, you can enter the configuration details for the Business Support Set (BSS), Representational State Transfer (REST), and outbound API calls.

**Procedure**

**Step 1** From the left pane of the MSX Portal, click **Settings**.

**Step 2** In the **Integrations** tab, you can enable or disable the following attributes:

- Support - Read knowledge articles and raise support tickets via the Cloud Services Portal.
- Manage Users - Add and remove portal users via the Cloud Services Portal.
- User and Tenant View (under **Identity**) - Disabling these attributes does not let you create, modify, or delete Users and Tenants respectively. You can only view the users and tenants. You can also enable the **Show Profile** option.

**Step 3** Click the **REST Configuration** tab to set the authentication mode details for the Integrations system.

**Step 4** Select **Basic** or **OAuth 2** based on your requirement.

  - If you have selected **Basic**, enter the user ID and password of the Integrations system.
  - If you have selected **OAuth 2**, enter the client ID, password, Token request URL, HTTP Method, Token Validation header, Token header format and other necessary details.

**Step 5** Click **Save** to save the authentication details.

**Step 6** In the **Outbound API** tab, under **API Context**, enter the base context URL for the outbound API calls in the **Base Context** attribute.

  a) Under **APIs** area, you can modify the **Allowed Values**, **Pricing Options**, **Accessible Services**, **Service Cancellation**, **Notification URL** of APIs. Click **Update** to save changes.

**Step 7** You can validate use case API operations in the **UseCase API** area.

### Enabling Multiple Subscriptions for a Tenant

Multiple ordering of a service allows service providers to customize the same service to meet different needs of a subscriber. For example, multiple WAN networks can be instantiated separately for security reasons to provide an air gap in the network by configuring a red network and a green network using WAN network.
As a user with an administrator role, you can enable this feature at the service definition time. Upon installing service packs, the necessary configuration needs to be done at the service pack level to enable this feature on MSX Portal. To configure this feature, enable the multipleInstance metadata using the POST request in the Consume Service API. For more information on this API, refer the Swagger documentation that can be accessed from MSX portal > Account Settings > Swagger > SIF SDK > Consume Service API. By default, only a single instance of a service can be ordered. After this feature is enabled, tenants can order more than one instance of a service.

```json
{
  "id": "f3e326cc-6545-11e7-6547-be2e65b06b65",
  "name": "vbranch",
  "label": "cisco.consume.service.vbranch.name",
  "activeFlag": true,
  "version": 1,
  "displayOrder": 1,
  "description": "cisco.consume.service.vbranch.description",
  "image": "/services/vbranch/images/icons/image_vbranch_service.svg",
  "multipleInstanceAllowed": true,
  "configuration": {
    "device": "false",
    "parts": "2",
    "showOffers": "true"
  }
}
```

*Note*  
Multiple Service instance is supported for both Create and Update Subscription.

---

### Enabling Notification for Events

You can either enable notifications for various events through email or REST API. Cisco MSX provides support to trigger notifications when certain events occur:

- Ensure you have configured Integrations, REST configuration details, and Outbound API details for sending REST notifications, if you want to use REST API rather than email notifications. For more information, see the section, Configuring Integrations for Outbound APIs.

- Both REST and Email communication modes are supported for all of the following list of events. However, only Email notification is supported (and not REST) for the event **End User Password Reset Link**.

- Email notifications are sent only when you have configured email client.

---

**Table 1: List of Events**

<table>
<thead>
<tr>
<th>Recipients</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumer, operator, or administrator</td>
<td>Password is reset.</td>
</tr>
</tbody>
</table>
### Enabling Notification for Events

<table>
<thead>
<tr>
<th>Recipients</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote user</td>
<td>• Remote user created or deleted.</td>
</tr>
<tr>
<td></td>
<td>• User ID is activated or deactivated/suspended.</td>
</tr>
<tr>
<td></td>
<td>• Password reset.</td>
</tr>
<tr>
<td>Service Provider</td>
<td>• Update Site</td>
</tr>
<tr>
<td>End User</td>
<td>• Delete Site</td>
</tr>
<tr>
<td></td>
<td>• Add Site</td>
</tr>
<tr>
<td></td>
<td>• Tenant Added.</td>
</tr>
<tr>
<td></td>
<td>• Tenant Updated.</td>
</tr>
<tr>
<td></td>
<td>• Tenant Deleted.</td>
</tr>
<tr>
<td></td>
<td>• Approval Pending for Requester.</td>
</tr>
<tr>
<td></td>
<td>• Approval Pending for Approver.</td>
</tr>
<tr>
<td></td>
<td>• Service Approved or Rejected.</td>
</tr>
<tr>
<td></td>
<td>• Device Added.</td>
</tr>
<tr>
<td></td>
<td>• Device Deleted.</td>
</tr>
<tr>
<td></td>
<td>• Device Only Purchase.</td>
</tr>
<tr>
<td></td>
<td>• Device Updated.</td>
</tr>
<tr>
<td></td>
<td>• Device Registered.</td>
</tr>
<tr>
<td></td>
<td>• End User Added.</td>
</tr>
<tr>
<td></td>
<td>• End User Deleted.</td>
</tr>
<tr>
<td></td>
<td>• End User Password Reset Link (supports only Email notification).</td>
</tr>
</tbody>
</table>

---

**Getting Started with Cisco Managed Services Accelerator**
### Recipients
- Service Provider
- End User

### Events
- End User Password Success Confirmation.
- End User Updated.
- Confirmation for Service Order.
- Service Order Failure.
- Service Activation Success Confirmation.
- Service Activation Failure.
- Service Deprovisioned.
- Service Deprovisioning Failure.
- Service Unsubscribed.
- Service Updated
- Service Update Failure.
- Configuration of Tenant VCE Required (indicating that the Cisco VCE is added to the Cloud VPN service).
- SSL VPN User Added.
- SSL VPN User Add Failure.
- SSL VPN User Deleted.
- SSL VPN User Password Reset Link (supports only Email notification).
- SSL VPN Password Reset Success.
- SSL VPN Password Reset Failure.
- SSL VPN User Status Changed.
- Enable Bandwidth Prioritization.

To enable notification for events:

**Procedure**

**Step 1**
From the left pane of the MSX Portal, click **Notifications**.
Events related to Provider and End Users are displayed when you click the **Provider** and **End Users** tab respectively.

**Step 2**
Using the **Category** drop-down, you can further categorize events.

**Step 3**
For an event, you can edit the **Template** name, **Communication Mode** by clicking the Edit icon (located next to the Communication Mode value). You can also enable or disable the notification for a specific event.
Defining Terms and Conditions for a Service

Cisco MSX allows you to define and maintain the terms for a service.

Procedure

Step 1  From the left pane of the MSX Portal, click **Configurations** and select the service pack.
Step 2  Click **Terms & Conditions**.
Step 3  Select one of the service packs offers from the "Offers" drop-down list.
Step 4  Select the desired format for the font.
Step 5  Enter details required for acceptance by a consumer while purchasing a service. This information is displayed while the consumer is placing an order for the service. The terms and conditions are defined specific to an offer in a service.
Step 6  Click **Save**.

Configuring an Announcement

Using this procedure, you can create an announcement text to display the alert messages such as planned maintenance alert and technical issues. These announcements are displayed for users upon login.

Procedure

Step 1  From the left pane of the MSX Portal, click **Settings > Announcements**.
Step 2  Enter the title and the message to be communicated.
Step 3  Choose an announcement style - **Danger**, **Warning**, **Info**, or **Success** from the **Visual Style** drop-down list, depending on the criticality or type of announcement to make.
Step 4  Optionally select the **Start Time** and **End Time** for the announcement.

If **Start Time** is not specified, the announcement is displayed immediately after it is saved. If an **End Time** is not specified, the announcement is displayed indefinitely after start time - You need to resolve the message for it to stop displaying.

Step 5  Choose either **Page Header Announcement** or **Ticker Announcement** to select the Announcement Type.
Step 6  Click **Save**. The newly added announcements are listed.

Once the issue is resolved, you can select the announcement that you want to delete from the list.
Registering a Device on MSX

When you place an order for an MSX service, the service comprises of devices for sites. These devices must be registered with the MSX portal. In Cisco MSX, the service orchestration is provided by Cisco Network Services Orchestrator (NSO). NSO automates the dynamic provisioning of physical, virtual, and software assets required to create the end-to-end service. NSO is a model-driven orchestrator which uses YANG for modeling the services, and can use various methods such as NETCONF, SSH, REST, and APIs to provision the devices. NSO runs as a Virtual Machine (VM) in the MSX solution.

When you place an order for an MSX service, the service comprises of devices for sites that need be registered with the MSX service interface. In the MSX solution, NSO also functions as the Plug-N-Play (PnP) server, which is utilized for zero-touch deployment (ZTD) of the CPE devices. When you place a request to register, the status changes to Provisioning, and after the device is successfully registered, the status of the device is updated as Provisioned. (There are several states which the device may cycle through in the process of provisioning, but the device will be in Up state when it comes into service.)

![Figure 1: CPE Connects to the PnP Server](image1)

The complete CPE onboarding in the PnP server is:

1. Onboard CPE to the PnP server (into CDB) with the specific identifier (UDI/Serial #) and service. Wait for the CPE to be enabled.

2. Router is connected, powered, and receives interface IP Address from the DHCP server. PnP Call Home Function using HTTPS (with Crypt/Cert) to PnP Server. Identify based on UDI (Serial #).

If steps 1 and 2 are reversed, the PNP server waits until CPE UDI is associated with a service in order to apply the correct Day0 config.

3. The PnP server delivers service specific Day0 configuration including the management hub keys to form FlexVPN Tunnel (IKEv2).
4. The FlexVPN management tunnel is formed for subsequent configuration activities.

5. The PnP server sends Day1 configuration to the device(s) over the FlexVPN management tunnel.

6. Using Day1 configuration and keys from the PnP server, create IPSec Tunnel(s) between the CPE and DMVPN Hub

7. The CPE sends alarms and Netflow data to MSX over FlexVPN management tunnel.

In the MSX solution, NSO also functions as the Plug-N-Play (PnP) server, which is utilized for zero-touch deployment (ZTD) of the CPE devices.

---

**Note**

Before you register a device, you must ensure that the branch and hub site settings and tenant service settings are configured. For more information, see the Service Pack user guides.

---

You can register a device as follows:

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Cisco MSX Portal using admin credentials.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the left pane of the Service Interface, click <strong>Devices</strong> to view the list of devices you have purchased in the Register Device window. The devices with the status such as Unregistered, Provisioned, Provisioning, Up, and Down are displayed.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the device you want to register.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the right pane, enter the serial number of the device in the Enter Device Serial Number (SN) field.</td>
</tr>
</tbody>
</table>

**Note**

A Serial Number is associated to the Customer Premises Equipment (CPE) before the device is shipped. When you specify the serial number, you tell the application to register the device with the service.

| Step 5   | Click **Register**. You can refresh the Register Devices window to view the registration status of the device. The device status is "Provisioning" indicating the registration is in progress and the status turns to "Provisioned" indicating registration is complete. |

**Note**

- You can modify the name and location of the device. Also, slide the time frame bar to view the Device Traffic accordingly.
- You can delete a device by selecting a device and clicking Delete. Deleting a device will remove it from the list. The device can be connected again to the same or another service but it will not retain any properties which have been previously defined.