



Cisco Managed Services Accelerator (MSX) 4.2 SD-WAN Service Pack User Guide

First Published: 2022-01-31

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	About this Document	1
	Audience	1
	What's New in Cisco MSX 4.2.0 for SD-WAN Services	2
	Related Documentation	3
	Bias-free Doc Disclaimer	4
	Full Cisco Trademarks with Software License	4

CHAPTER 2	Overview of Cisco MSX	7
	Cisco SD-WAN Service	7
	Cisco Meraki SD-WAN Service	8

CHAPTER 3	Getting Started with Cisco MSX SD-WAN Services	11
	Logging In to the MSX Portal	11
	Configuring Single Sign-On Between MSX and Cisco SD-WAN	12
	Configuring Integrations	14
	Managing SD-WAN Notifications	14
	Defining Terms and Conditions	16
	Configuring Password Policies	16
	Setting Up Cisco SD-WAN Specific Configurations in MSX	17
	Configuring Cisco SD-WAN Orchestrator Settings	17
	Configuring Serial Number Format for an ENCS Device	17
	Configuring Subnet Pools	18
	Setting Up Meraki SD-WAN-Specific Configurations in MSX	18
	Generating API Access Key for Meraki	18
	Adding MSX IP Address to the Meraki Allowed List	19
	Managing Meraki Traffic Class Access for Tenants	19

CHAPTER 4	Managing Roles in Cisco MSX	21
	Managing User Roles	22
	SD-WAN-Specific Permissions	22
	Adding a User Role	24
	Modifying an Existing Role	25
	Managing Tenants, Tenant Groups, and Users	25
	Managing Tenants	25
	Managing Tenant Groups	26
	Managing Users	26

CHAPTER 5	Managing Cisco SD-WAN vEdge Cloud TDE Templates	29
	Uploading a vEdge Cloud Template	30
	Deleting a vEdge Cloud Template	31
	Managing vEdge Cloud Template Access for Tenants	31

CHAPTER 6	Deploying Cisco SD-WAN Services on MSX	33
	Deployment Workflow for Cisco SD-WAN	33
	Setting Up Control Plane for Cisco SD-WAN	34
	Prerequisites for Setting Up Control Plane	34
	Creating Control Plane on OpenStack	36
	Creating Cisco SD-WAN Control Plane on AWS	39
	Postdeployment Tasks for SD-WAN Control Plane	42
	Logging in to the Cisco SD-WAN Control Plane	43
	Creating a New User on the Control Plane	44
	Updating Smart Account Details	44
	Generating PKI Certificates on the Control Plane	44
	Synchronizing Smart Accounts from the Control Plane	45
	Managing SSL Certificates	46
	Change SD-WAN Controllers Password	46
	Importing and Exporting Cisco SD-WAN Device Template	46
	Importing Device Templates from a Tenant Cisco SD-WAN System to the MSX Library	48
	Exporting Device Templates from the MSX Library to a Tenant Cisco SD-WAN System	49
	Attaching Control Plane	50

Deploying a Device for Cisco SD-WAN	51
Adding a vEdge Cloud Device	51
Setting Up Initial Configuration on the ENCS CPE (First-Time Use Only)	55
Adding a vEdge SP Cloud Device	56
Adding a Physical Device	59
Assigning a Device to a Site	61
Importing Multiple Site Data from Cisco SD-WAN into MSX	62
Check the Status of Various SD-WAN Components	65
Provisioning a Device	67
Configuring Traffic Policies	67
Configuring Path Preference Settings	68
Configuring Application Relevance Settings	70
Deactivate a Traffic Policy	72
Maintaining Cisco SD-WAN Deployments	72
Editing an SD-WAN Control Plane	72
Editing a Provisioned Device	73
Upgrading Control and Data Plane	74
Uploading Software Images	74
Upgrading vEdge Devices	74
Activating New Software Image on vEdge Devices	75
Deleting a Device	75
Deleting a Device	76
Detaching an SD-WAN Control Plane	77
Unsubscribing the SD-WAN Service	77
<hr/>	
CHAPTER 7	
Deploying Cisco Meraki SD-WAN Services on MSX	79
Deployment Workflow for Meraki SD-WAN	79
Setting Up SD-WAN Control and Management Plane for Meraki	79
Adding a New Device for Meraki	80
Postdeployment Tasks for Meraki SD-WAN	82
Deploying an Additional Controller Type	82
Maintaining Cisco Meraki SD-WAN Deployments	82
Configuring Application Relevance Settings for Meraki SD-WAN	82
Deleting the Meraki Site	85

Detaching the Control Plane for Meraki 85

CHAPTER 8

Monitoring Cisco SD-WAN and Meraki SD-WAN Services in MSX 87

Monitoring SD-WAN Service Status on the Cisco MSX GUI 87

Understanding Cisco SD-WAN Service Statuses 89

Monitoring Cisco SD-WAN Device Status 90

Understanding Cisco SDWAN Synchronization 91

Understanding Cisco SD-WAN Device Statuses 91

Device Statuses for Physical Device 93

Device Statuses for vEdge SP Cloud 96

Device Statuses for vEdge Cloud 98

Site Statuses for Meraki SD-WAN Devices 101

Monitoring SD-WAN Control Plane Status 101

Monitoring Tunnel Health 103

Monitoring SD-WAN Reporting Metrics Using Third-Party Network Monitoring Applications 106

Monitoring the Traffic Policy 106

Monitoring the Traffic Paths 106

Monitoring the Application Queue 107

Viewing Event Logs 107

CHAPTER

Appendixes 109

APPENDIX A Troubleshooting Cisco SD-WAN Issues 111

Troubleshooting Cisco SD-WAN Reachability Issues 111

Troubleshooting Cisco SD-WAN vEdge-Cloud Deployment Errors 111

Troubleshooting Cisco SD-WAN vEdge Reachability Errors 113

Troubleshooting ENCS Reachability Issues 114

Changing MSX Trace Logging Level During Runtime 115

Troubleshooting Control Plane 117

Troubleshooting Control Plane on OpenStack 117

Change Control Plane Password or Vault Failures 120

Fixing Control Plane Device Status State 120

Data Plane Troubleshooting 122

Data Plane Deployment Status: NSO Device Status 122

Data Plane Deployment Status (MSX Portal)	122
Reachability Status: vManage Device State	123
Data Plane Reachability Status (MSX Portal)	123
PnP Server Troubleshooting Commands	124
List of Devices in Contact with the PnP Server	124
CPE in Contact with the PnP Server (Without a Service)	124
CPE in Contact with the PnP Server (With a Service)	124
CPE in Contact with the PnP Server (Detailed)	124
View CPE Details	125
IPsec Tunnel Cannot be Established	126
APPENDIX B Troubleshooting Cisco Meraki SD-WAN Issues	129
Handling Meraki Rate Limiting Issue on MSX	129
Checking Meraki Beat	130
Checking Device Status	130
Checking Device Connections	134
APPENDIX C Applications Available with Cisco MSX SD-WAN	137
APPENDIX D Out-of-the-Box Cisco SD-WAN Device Templates Available Within MSX	139
APPENDIX E Sample Payloads for Creating Cisco SD-WAN Control Plane on Openstack	149
Adding VIM Payload in Provider Network	149
Adding VIM Payload in Tenant Network	150
Adding Control Plane Payload with Enterprise Certificate in Provider Network	151
Adding Control Plane Payload with Symantec Certificate in Provider Network	152
Adding Control Plane Payload with Enterprise Certificate in Tenant Network	153
Adding Control Plane Payload with Symantec Certificate on Tenant Network	154



CHAPTER 1

About this Document

This chapter provides information about the intended audience of the Cisco MSX SD-WAN Service Pack, what's new in the current release, and the related documentation.

- [Audience, on page 1](#)
- [What's New in Cisco MSX 4.2.0 for SD-WAN Services, on page 2](#)
- [Related Documentation, on page 3](#)
- [Bias-free Doc Disclaimer, on page 4](#)
- [Full Cisco Trademarks with Software License, on page 4](#)

Audience

This guide is designed for service provider operators and tenants who deploy, manage, configure Cisco MSX SD-WAN service pack, and troubleshoot various SD-WAN service issues.

What's New in Cisco MSX 4.2.0 for SD-WAN Services

Table 1: What's New in Cisco MSX 4.2.0 for Cisco SD-WAN and Meraki SD-WAN Services

Feature	Description
<p>Access SD-WAN Service Panel and SD-WAN Options in the New MSX GUI</p>	<p>Using the new MSX GUI, a tenant can:</p> <ul style="list-style-type: none"> • Attach or create an Cisco SD-WAN control plane. For more information, see Creating Cisco SD-WAN Control Plane on AWS and Attaching Control Plane. • Edit, detach, or delete the Cisco SD-WAN control plane. For more information, see Detaching an SD-WAN Control Plane and Editing an SD-WAN Control Plane. • Assign one or more devices to a site. For more information, see Assigning a Device to a Site. • Monitor and view the status of the Cisco SD-WAN control plane. For more information, see Monitoring SD-WAN Control Plane Status. • Unsubscribe from the Cisco SD-WAN service. For more information, see Unsubscribing the SD-WAN Service. • Setup and view traffic policies. For more information, see Configuring Traffic Policies. • Perform bulk import of device templates. For more information, see Importing Multiple Site Data from Cisco SD-WAN into MSX. <p>From the new MSX GUI, a tenant can now access legacy GUI to:</p> <ul style="list-style-type: none"> • Add device. • Manage Meraki service.
<p>Support for Cisco SD-WAN Release 20.6.2.2</p>	<p>Cisco MSX 4.2.0 supports Cisco SD-WAN Release 20.6.2.2. For more information, see Cisco SD-WAN and MSX Version Compatibility Matrix.</p>
<p>Add Support Details in the Device Information Section</p>	<p>When you add a site in Cisco SD-WAN, you must now enter support details instead of contact details in the Device Information section. For more information, see Deploying a Site or Device for Cisco SD-WAN.</p>

Related Documentation

You can access Cisco MSX 4.2.0 content at https://www.cisco.com/c/en/us/td/docs/net_mgmt/msx/end_user_doc/4_2/Cisco_MSX_End_User_Documentation.html.

The documents listed here are available for additional reference. To access API documentation on the Swagger GUI, log in to the 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) 4.2 Release Notes Documentation	This documentation provides information about the new features in Cisco Managed Services Accelerator (MSX) 4.2.
Cisco Managed Services Accelerator (MSX) 4.2 Administration Documentation	This documentation covers the post-install configuration information that is required to set up MSX.
Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum	This addendum covers all the permissions that are required to operate MSX and the service packs.
Cisco Managed Services Accelerator (MSX) 4.2 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) 4.2 SD-WAN and Meraki 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 MSX 4.2 and the comparison of applications in older releases with applications in MSX 4.2 based on possible application mapping.
Cisco Managed Services Accelerator (MSX) 4.2 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) 4.2 Solution Overview Documentation	This documentation provides a comprehensive explanation of the design of the MSX solution that enables service providers to offer flexible and extensible services to their business customers.
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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)



CHAPTER 2

Overview of Cisco MSX

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 Cisco MSX SD-Branch, Cisco MSX Cloud UTD, and Cisco MSX Managed Device).

For detailed information about Cisco MSX solution, see the [Cisco Managed Services Accelerator \(MSX\) 4.2 Solution Overview Documentation](#).

The Cisco SD-WAN and Meraki SD-WAN service packs are a suite of prepackaged software capabilities that fully automate the end-to-end SD-WAN service creation. With these fully validated service level packages, end customers can quickly turn on, control, and assure cloud-based WAN services that are offered by the service provider.

This section contains the following topics:

- [Cisco SD-WAN Service, on page 7](#)
- [Cisco Meraki SD-WAN Service, on page 8](#)

Cisco SD-WAN Service

Cisco MSX enables service providers to deploy and manage SD-WAN services for their customers. The deployment of an SD-WAN service in the context of a managed service requires deployment per customer and includes the SD-WAN management control plane (vManage, vBond and vSmart), and the corresponding data plane (vEdge and cEdge).

The Cisco SD-WAN service pack consists of:

- vManage— Cisco’s GUI based centralized management and provisioning platform for Day 0, Day 1 and Day n+ for the entire Cisco SD-WAN infrastructure. You can login to the Cisco vManage dashboard to centrally manage the WAN. Cisco vManage provides the ability to manage all aspects of the WAN from provisioning, monitoring, and upgrading routers to application visibility and troubleshooting the WAN.
- vBond—The vBond facilitates the initial bring-up by performing initial authentication and authorization of all elements into the network. vBond provides the information on how each of the components connects to other components. It plays an important role in enabling devices that sit behind the NAT to communicate with the network.
- vSmart Controller—The vSmart controllers establish the secure SSL connections to all other components in the network, and run an Overlay Management Protocol (OMP) to exchange routing, security, and

policy information. The centralized policy engine in vSmart provides policy constructs to manipulate routing information, access control, segmentation, extranets, and service chaining.

- vEdge and cEdge (IOS XE) Routers—These routers (physical and cloud) establishes secure connectivity to all of the control components and also establishes IPSec sessions with other routers in the WAN network. These routers can be used as a Virtual Network Function (VNF) deployment at the branch. NFV Infrastructure Software (NFVIS) platform on Cisco Enterprise Network Compute System (ENCS) facilitates the deployment and operation of VNFs and hardware components.

Some of the advantages of the Cisco MSX SD-WAN service pack are:

- User interface portal for ordering service (Control Plane and Data Plane Connectivity) and network visualization.
- Lifecycle management of services.
- Site and device activation.
- Site level monitoring and tunnel health reporting.
- Traffic policy management.

The table below lists supported versions of Cisco SD-WAN on Cisco MSX :

Table 2: Cisco SD-WAN and MSX Version Compatibility Matrix

Cisco MSX Release	Cisco SD-WAN Release
4.2	20.6.2.2, 20.6.2.1, 20.6.2, 20.6.1
4.1	20.5.1, 20.4.1
4.0	20.5.1, 20.4.1
3.10	20.4.1, 20.3.2
3.9.0	20.1.1, 19.3.0

Cisco Meraki SD-WAN Service

All Cisco Meraki security appliances comes with SD-WAN capabilities that allow administrators to dynamically adjust to changing WAN conditions without the need for manual intervention. By providing granular control over how certain traffic types respond to changes in WAN availability and performance, SD-WAN can ensure optimal performance for critical applications and help to avoid disruptions of highly performance-sensitive traffic, such as VoIP

Using Meraki SD-WAN on MSX, service providers can add or remove networks (equivalent to adding sites in Cisco SD-WAN) and display uplink information about a device.

Some of the advantages of using Cisco Meraki SD-WAN on MSX are:

- User interface portal for ordering Meraki SD-WAN service for tenant.
- Ability to attach to a Meraki organization established for the Tenant.

- Lifecycle management of services.
- Control Plane and Data Plane Connectivity and network visualization.
- Site and device activation by selecting and applying configurations on Meraki networks.
- Site level monitoring with uplink interface details.
- Traffic policy management

The following are the Meraki wireless and combined device types currently supported on Cisco MSX:

- SD-WAN appliance devices:
 - MX64, MX65, MX67, and MX68 required for a small branch setup.
 - MX84 and MX100 required for a medium branch setup.
 - MX250 and MX450 required for a large branch/campus setup.
- vMX device types for virtual devices.
- MR device types for wireless
- MS series of access switches



CHAPTER 3

Getting Started with Cisco MSX SD-WAN Services

This chapter provides information about how to get started with SD-WAN services (Cisco SD-WAN and Meraki SD-WAN) in Cisco MSX.

This chapter contains the following topics:

- [Logging In to the MSX Portal, on page 11](#)
- [Configuring Single Sign-On Between MSX and Cisco SD-WAN, on page 12](#)
- [Configuring Integrations, on page 14](#)
- [Managing SD-WAN Notifications, on page 14](#)
- [Defining Terms and Conditions , on page 16](#)
- [Configuring Password Policies , on page 16](#)
- [Setting Up Cisco SD-WAN Specific Configurations in MSX, on page 17](#)
- [Setting Up Meraki SD-WAN-Specific Configurations in MSX, on page 18](#)

Logging In to the MSX Portal

You can access the SD-WAN service pack on the MSX Portal, only after installing the MSX platform along with the required service pack.

To log into the MSX portal, enter the following URL in your web browser address field:

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

In this URL:

< server-ip> is the IP address or fully qualified domain name (FQDN) name of the MSX server:

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.

What you can see and do in the user interface is determined by your user account privileges. For information on Cisco MSX users and the actions they can perform, see [Managing Roles in Cisco MSX](#).

Log in to the MSX portal and ensure all Microservices and Service UI information in the Settings main menu > Component Versions displays the latest MSX version.

Configuring Single Sign-On Between MSX and Cisco SD-WAN

Use the procedure below to configure the SSO between MSX and Cisco SD-WAN. Only a user with an administrator role can configure the SSO.

-
- Step 1** Upload the MSX metadata to the SD-WAN control plane.
- Download the MSX metadata from the following link: <https://msx-fqdn/idm/metadata>.
 - Upload the metadata file to the SD-WAN control plane by choosing Settings > Identity Provider Settings. For information on logging in to the Control Plane, see [Logging in to the Cisco SD-WAN Control Plane](#).
 - Click Edit and then select Enable Identity Provider option.
 - Copy the contents of the metadata file to the Upload Identity Provider Metadata field.
 - Click Save.
- Step 2** Download the Cisco SD-WAN SAML metadata file:
- From the Cisco SD-WAN control plane, choose Administration> Settings >Identify Provider Settings .
 - Navigate to [Click here to download the SAML metadata](#) and save the contents in a file, for example, `vmanage_metadata.xml`.
- Step 3** Save the Cisco SD-WAN metadata file in the following location Kubernetes location:
- ```
/data/vms/heapdumps/usermanagementservice/vmanage_metadata.xml
```
- Note** MSX usermanagement service map the Kubernetes location to the following file:
- ```
/data/conf/vmanage_metadata.xml
```
- Step 4** Configure the SSO client (Cisco SD-WAN control plane) details in the MSX portal.
- Log in to the Cisco MSX portal.
 - In the main menu, choose Settings > SSO Configuration.
 - Expand the Add SSO Client window and click Add . In the Add SSO Client window, specify the following details:
 - Associate Tenants: Specify the tenant for whom the SSO client is configured. If no tenants are specified, MSX assumes that the SSO client configuration is for all the tenants.

Note Superuser, Tenant Administrator, and Service Provider operator can access the control plane without configuring SSO.
 - Grant Types: From the drop-down, choose the option 'urn:ietf:params:oauth:grant-type:saml2-bearer'.
 - Metadata Source : “file:/data/conf/vmanage_metadata.xml” . Specify the Cisco SD-WAN metadata file location (from step 3) in the Metadata Source field. The metadata source field takes an url or a file path.

Note Metadata field is displayed only if you have specified a SAML service provider client ID in the Client ID field.
 - Authorities : From the drop-down, choose the option 'ROLE_USER'.

- Use Session Timeout: Select the option 'No'.
- Access Token Validity Seconds: Enter the time in seconds for when the token is valid. Enter this value as '1'.
- Max Tokens Per User: From the drop-down, choose the number of tokens allowed per user.
- Refresh Token Validity Seconds : Enter the time in seconds.
- Client ID: Specify the SAML service provider's client ID (Cisco SD-WAN control plane IP address in this case).
- Client Secret: Specify a string that can be used to guess the password.

Note This string can be used later for MSX access token.
- Scopes: From the drop-down, choose 'read'.
- Auto Approve Scopes: From the drop-down, choose 'read'.

d. Click Save.

A new SSO client configuration is added and displayed in the SSO Clients table.

A green success banner indicates that the above settings are correct. If a red banner is displayed, verify the SAML metadata file location in the Kubernetes location and all the values.

Step 5 Create user roles in the MSX portal. These roles should map to the SD-WAN control plane user roles (Basic, Netadmin, and Operator).

Step 6 (Optional) Disable the SAML security settings.

Perform this step if the SSO configuration is not successful and is not working as expected.

By default, the following SAML security parameters in MSX are set.

- `security.auth.saml.want-authn-request-signed`
- `security.auth.saml.encrypt-assertion`

For SAML service provider integration with MSX, if the above security parameters are set to True, the auth request from the service provider must be signed, and the assertion sent back by MSX is encrypted.

To turn off this default setting, do the following:

a. Log in to the Inception VM and access the Kubernetes location:

```
ssh -i id_rsa centos@_INCEPTION_FLOATING_IP_ADDRESS_ -t ssh _kubernetes-master-1_IP_ADDRESS
```

b. Run the following curl commands:

- `curl --request PUT -g -k -v -H "X-Consul-Token: {consul_acl_master_token}" --data 'false' https://consul.service.consul:8500/v1/kv/userconfiguration/defaultapplication/security.auth.saml.want-authn-request-signed`
- `curl --request PUT -g -k -v -H "X-Consul-Token: {consul_acl_master_token}" --data 'false' https://consul.service.consul:8500/v1/kv/userconfiguration/defaultapplication/security.auth.saml.encrypt-assertion`

Note Replace `<consul_acl_master_token>` with your consul acl token value from the passwords.yml file.

c. Save the consul entries by restarting the usermanagement microservices from the Kubernetes location using the following commands:

- `kubectl -n vms delete -f /etc/kube-manifests/usermanagementservice-3.9.0-dep.yml`
- `kubectl -n vms create -f /etc/kube-manifests/usermanagementservice-3.9.0-dep.yml`

Configuring Integrations

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

To configure BSS integrations, do the following:

-
- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left hand pane, click Settings.
- Step 3** Click the BSS Integrations tile. The BSS Integration page is displayed.
- Step 4** Click the Global tab and configure the following fields:
- Read only User View: Check this option to allow your users to only view the details.
 - Show Profile: Check this option to enable the show profile option for your tenants.
 - Read only Tenant View: Check this option to allow your tenants to only view the details.
- Step 5** Click the REST Configuration tab to set the authentication mode details for the integrations system.
- Select the Basic or OAuth2 radio button, based on your requirement.
 - If you select the Basic radio button, enter the User ID and Password of the integrations system.
 - If you select the OAuth2 radio button, enter the details such as the Token Request URL, Client ID, Client Secret, HTTP Method, Token Validation Header, Token Header Format, and so on.
 - Click Save to save the authentication details.
- Step 6** Click the Outbound API tab and specify the APIs used for business integrations. Click on the edit button to modify the Allowed Values, Pricing Options, Accessible Services, Service Cancellation, and Notification URL for the APIs.
- Step 7** Click Update to save the changes.
-

Managing SD-WAN Notifications

Before You Begin

You can configure integrations for enabling support for BSS, REST, and outbound API calls. For more information, see [Configuring Integrations](#).

Perform this procedure to enable notifications:

- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left hand pane, choose Settings > Service Configurations > SD-WAN > Notifications.
The Provider and End Users tab displays the events that are related to service provider and end users. Using the Category drop-down list, you can further categorize events as End Users, Services, and Devices.
- Step 3** To edit the notification settings, click the Edit icon adjacent to the Category column.
For an event, you can edit the template name, the communication mode, and enable or disable notifications for a specific event.
- Step 4** Click Save.
The following table lists the Cisco MSX notifications and the corresponding recipients for events:

Table 3: Notifications and Recipients

Notifications	Recipients
SD-WAN control plane status changed	REST clients
SD-WAN control plane operation notifies user	End users
SD-WAN control plane operation notifies tenant	Tenants
SD-WAN control plane operation notifies provider	Provider
SD-WAN site deletion notifies user	End users
SD-WAN site deletion notifies tenant	Tenants
SD-WAN site deletion notifies provider	Provider
SD-WAN site creation notifies user	End users
SD-WAN site creation notifies tenant	Tenants
SD-WAN site creation notifies provider	Provider
SD-WAN site status changed	REST clients

The following are examples of control plane and data plane notifications:

- Control Plane Message
 - Dear customer, the requested changes on your SD-WAN service have been applied.
 - <Control plane URL>
 - <Control plane Org>
 - <User ID>
 - <User name>

- Best regards, Managed Services Accelerator powered by Cisco
 - Data Plane Message
 - Dear customer, the requested changes on your service have been applied.
 - <Site ID>
 - <Site Name>
 - <Chassis Number>
 - <User id>
 - <User name>
 - <Tenant id>
 - <Tenant name>
 - <Tenant email>
 - Best regards, Managed Services Accelerator powered by Cisco
-

Defining Terms and Conditions

Cisco MSX allows you to define and maintain the terms of a service for acceptance by a consumer while purchasing a service.

- Step 1** Log in to the Cisco MSX portal using your credentials.
- Step 2** From the left hand pane, choose Settings > Service Configurations > SD-WAN > Terms & Conditions.
- Step 3** Enter the details. This information will be displayed while a consumer is placing an order for a service. The terms and conditions are specifically defined specific to an offer in a service.
- The Offers drop-down list displays the service pack offer selected in step 2.
- Step 4** Click Save.
-

Configuring Password Policies

In MSX, as an administrator user, you can define various settings for the password policies, such as password strength, password minimum/maximum length, password history, and password aging.

By default, there are two default policies available on MSX. An Administrator user can modify these existing policies or create new policies. The default policies that are created at the deployment time are:

- ppolicy_default - Applicable for a consumer user

- `ppolicy_strong` - Applicable for administrator accounts

For more information on the password policies and to modify the default password policies, see [Cisco Managed Services Accelerator \(MSX\) 4.2 Administration Documentation](#).

Setting Up Cisco SD-WAN Specific Configurations in MSX

Configure the following for Cisco SD-WAN setup:

- [Disabling MSX-Managed Proxy](#)
- [Configuring Cisco SD-WAN Orchestrator Settings](#)
- [Configuring Serial Number Format for an ENCS Device](#)
- [Configuring Subnet Pools](#)

Configuring Cisco SD-WAN Orchestrator Settings

Before creating a control plane for a tenant, you must first provide the SD-WAN Orchestration settings in the MSX Portal.

To configure orchestrator settings for Cisco SD-WAN:

Before you begin

Request for the SD-WAN Orchestration stack URL from your Cisco account representative using your Service Provider's Smart Account details.

-
- Step 1** Log in to the MSX Portal .
- Step 2** From the main menu, click Settings > Service Configurations > SD-WAN > Settings > Cisco SD-WAN Orchestration Settings tile, to access the orchestrator settings for Cisco SD-WAN.
- Step 3** Specify the details of the SD-WAN orchestration stack, such as orchestrator URL, username, password, contact email, and status tag.
- The Status Tag field accepts two values—Proof-of-concept (POC), and production. So, you can add the status tag with one of these values. This status tag applies the relevant label within the vOrchestrator.
- Note** By default, the vOrch tagged as POC expires in 90 days. So, you can extend this timeline from the vOrchestrator.
- The Contact Email field notifies the user about progress in the SD-WAN processes. Only three email domains are accepted in this field: gmail.com, cisco.com, and external.cisco.com
- Step 4** Click Save.
-

Configuring Serial Number Format for an ENCS Device

Cisco SD-WAN coordinates with the SD-Branch service pack to deploy virtual vEdge on ENCS. To configure the ENCS device serial number format for the vEdge cloud deployments, do the following:

-
- Step 1** Log in to the Cisco MSX portal using your credentials.
- Step 2** From the left hand pane, choose Settings > Service Configurations > SD-Branch > Settings > SD-Branch Settings.
- Step 3** Choose device serial number format. Specify device serial number format to be used during the Add Site flow:
- Cisco: Applies Cisco format for device serial number
 - Custom: Preloads Cisco's regex. You can edit this regex or replace with a new one
 - None: Applies no specific format
- Step 4** Specify the Site Contact Information and Terms and Conditions for the service.
- Step 5** Click Submit.
-

Configuring Subnet Pools

Use the following procedure for the vEdge Cloud to configure subnet pool for IPsec Tunnel for secure communication between MSX and NFVIS.

-
- Step 1** Log in to the Cisco MSX portal using your credentials.
- Step 2** From the left hand pane, choose Settings > Service Configurations > SD-Branch > Settings > SD-Branch > Settings > Subnet Pools.
- Step 3** Specify the following for the IPsec tunnel:
- Specify the time for which the IP Subnet Allocation is reserved.
 - Add IP subnet pool for ENCS NFVIS internal management to allow users to assign IP for the ENCS from this pool.
- Step 4** Click Submit.
-

Setting Up Meraki SD-WAN-Specific Configurations in MSX

Use this section to configure initial settings in the MSX Portal after installing the Meraki SD-WAN.

Generating API Access Key for Meraki

After you get access to Meraki, use the following procedure to get API access key for Meraki.

Before you begin

- Enable Meraki Service: Meraki service is not available in Cisco MSX by default. To enable Meraki in Cisco MSX, contact your Cisco account representative.
- Obtain the Meraki Organization ID: When the Meraki organization is setup for the Tenant, the ID for organization is shared.

- Step 1** Log in to Meraki Dashboard with your user name and password .
- Step 2** Choose User > My Profile.
- Step 3** Click Generate New API Access Key button to generate a new key.

- Note**
- Only two access keys are permitted.
 - If you do not see the Generate New API Access button, it means you already have an API access key. Revoke the existing key and then generate a new key. Before you revoke an existing key, get the consent of the user who had generated the previous key.

Figure 1: Revoking API Access Key

API access

API keys

Key	Created at	Last used	
*****1be4	Sep 27 2019 14:30 UTC	Never	Revoke
*****dea0	Sep 18 2019 22:15 UTC	Sep 28 2019 14:54 UTC	Revoke

Adding MSX IP Address to the Meraki Allowed List

To ensure seamless connectivity between Meraki and MSX, ensure MSX IP address are added to the allowed list in Meraki. Do the following

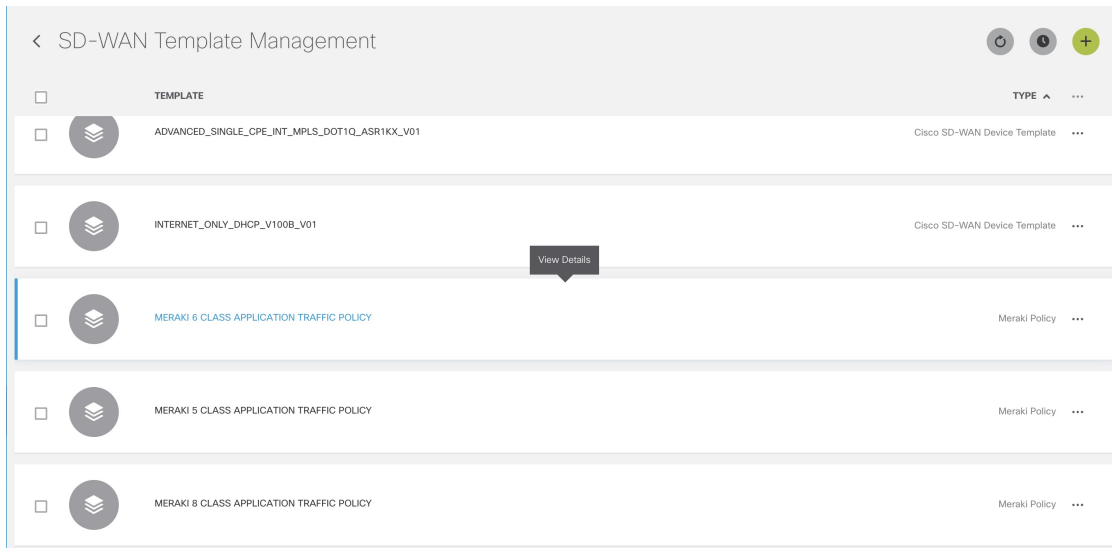
- Step 1** Log in to the Cisco Meraki Dashboard.
- Step 2** Go to the Organization Settings.
- Step 3** In the Login IP ranges section:
- Enable the option to add IP addresses to the allowed list.
 - Enter the address ranges.

Managing Meraki Traffic Class Access for Tenants

Use this procedure to assign Meraki application relevancy templates to tenant users. While defining traffic policies for Meraki SD-WAN, the tenant users will see only the templates that they were given access to.

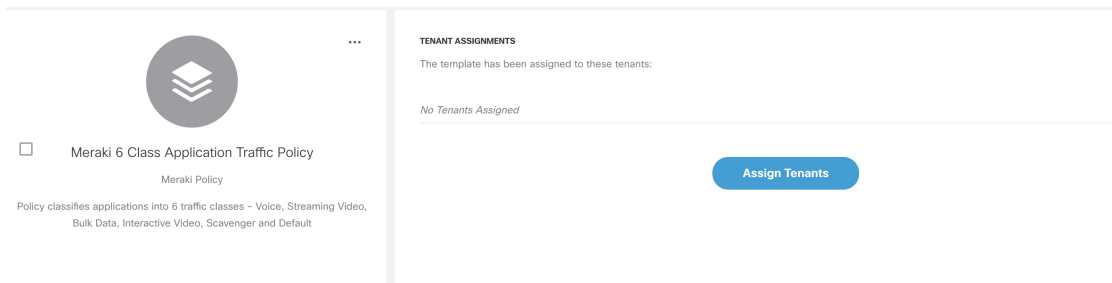
- Step 1** Log in to the Cisco MSX Portal using your credentials.
- Step 2** From the left hand pane, choose Settings > Template Management.
- Step 3** Select the SD-WAN tile to see the list of available templates on the Template Management screen. The SD-WAN Template Management screen lists templates that are currently available in the MSX library.

Figure 2:



Step 4 Select one or more Meraki Policy based template type and click (...) > Assign Tenants option to display the wizard. You can also expand the template, and click Assign Tenants option to display the wizard.

Figure 3: Assign Tenants Option After Expanding the Template



Step 5 Choose one or more tenants from the drop-down list and click > to start the export process.

Step 6 Click Confirm Assignment to save and apply the changes.

Step 7 Click View Template Activity option to track the progress in the Template Activity screen.



CHAPTER 4

Managing Roles in Cisco MSX

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

In MSX, you need to create a new role (such as an SD-WAN Operator) and assign the permissions required to order, operate, and view service pack-related services. MSX provides five out-of-box roles. For more information on MSX out-of-box roles, see [Cisco Managed Services Accelerator \(MSX\) 4.2 Administration Documentation](#).

To create the SD-WAN role and assign it to users:

Table 4: Procedure for Creating SD-WAN Service Pack-Specific User Roles

	Procedure	References
1	Log in to the Cisco MSX portal (Admin/Super user)	
2	Create the tenants.	For more information on creating a new tenant, see Managing Tenants .
3	<p>Create a new role if you want to perform specific tasks on SD-WAN.</p> <p>Note By default, MSX provides five out-of-the-box (OOB) roles that have permissions applied. In these OOB roles, Service Operator role has permissions required to create and manage SD-WAN service. To see the default permissions applied on a service provider operator role:</p> <p>In the main menu of the MSX Portal, click Roles and select Service Provider Operator. Expand the various categories to see the default permissions applied on this role.</p>	For more information on basic permissions that are required to perform the documented tasks for the MSX platform and the service packs, see Cisco Managed Services Accelerator (MSX) 4.2 Platform and Service Pack Permissions Addendum . For more information on creating a new user role, see Managing User Roles .

	Procedure	References
4	Create users (such as SD-WAN User), and assign the role that is defined in Step 3 to the user, and select all the tenants that the user needs to access.	For more information on creating a new user, see Managing Users .

- [Managing User Roles, on page 22](#)
- [Managing Tenants, Tenant Groups, and Users, on page 25](#)

Managing User Roles

Your user account privileges determine, what you can see and do in the MSX user interface. In MSX, the permissions are managed using Role-Based Access Control (RBAC). RBAC restricts or authorizes system access for users based on their user roles. A role defines the privileges of a user in the system. Since users are not directly assigned with privileges, management of individual user privileges is simply a matter of assigning the appropriate roles.

A user is granted access to desired system resources only if the assigned role grants the access privileges. For example, a user with the Service Extension permissions can import service extension templates, define service extension parameters, define default parameter values, and so on. For more information on assigning roles to a user with appropriate permissions, see [Managing Users](#).

SD-WAN-Specific Permissions

The table below lists the Cisco SD-WAN and SD-Branch category of permissions:

Table 5: Cisco SD-WAN and SD-Branch Category of Permissions

SD-WAN Service	SD-WAN Data Plane	<p>Allows users with manage permissions to add, edit, or delete sites (data plane).</p> <p>View permission allows you to view sites (Data Plane) and the status of the sites.</p>
	SD-WAN Maintenance	<p>Allows users with manage permission to debug and access SD-WAN GET APIs. Using these APIs, users can query SD-WAN databases, or query Cisco SD-WAN to check on status of various components.</p>
	SD-WAN Control Plane	<p>Allows users with manage permissions to create, attach, delete, detach Control Plane.</p> <p>View permission allows users to view a control plane that is already created or attached and see the status of the Control Plane components.</p>
	SD-WAN Orchestrator Settings	<p>Allows users with manage permission to configure orchestrator settings to spin up a new Control Plane. For more information, see Configuring Cisco SD-WAN Orchestrator Settings.</p>
	SD-WAN Traffic Policy	<p>Allows users with manage permission to add and modify Application Relevance policy or Path Preference policy to the Cisco SD-WAN fabric. For more information on how to configure these traffic policies for Cisco SD-WAN, see Configuring Traffic Policies.</p> <p>This permission along with Service Configuration Application manage permission is also required to configure application relevance for various applications across MSX managed sites that have MX device models (Meraki SD-WAN appliance).</p>

	SD-WAN Bulk Site	Allows users to download the template to their local machine and to view or manage the template.
Cisco MSX SD-Branch Operations	Template Data Operations	Allows users with manage permissions to manage predefined data for Cisco MSX SD-Branch service templates.
	Template Operations	Allows users with manage permissions to add, edit, or delete Cisco MSX SD-Branch service templates and edit tenant access to SD-Branch service templates
	SD-Branch Settings Operations	Allows users with manage permissions to manage Cisco MSX SD-Branch settings.
	SD-Branch Sites Operations	Allows users with manage permissions to add, edit, or delete Cisco MSX SD-Branch sites.

Along with the preceding permissions, SD-WAN services also need permissions from the MSX platform side. For more information on minimum permissions (platform) that are required to perform a task in SD-WAN and on the complete list of MSX permissions, see [Cisco Managed Services Accelerator \(MSX\) 4.2 Platform and Service Pack Permissions Addendum](#).

Adding a User Role

To add a user role:

-
- Step 1** Log in to the Cisco MSX Portal.
 - Step 2** In the main menu, click Roles. The Manage Roles screen appears.
 - Step 3** Click the Add Role button.
 - Step 4** Enter the role name, display name, and description.
 - Step 5** To assign the permission for the roles, click Category and select the corresponding check boxes for the permissions that you want to grant to the role. For permissions related to SD-WAN, see [SD-WAN Specific Permissions](#).

The types of permission you can grant are::

Table 6: Assigning User Roles

Permission Type	Description
View	Provides read-only access to the function.
Manage	Provides access to read and manage tasks associate with the function.

Step 6 Click Save.

Modifying an Existing Role

To modify an existing role:

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click Roles to view the list of roles. The Manage Roles screen appears.

Step 3 Select the role that you want to modify and click the Edit icon.

Step 4 To assign or revoke the permission for the roles, click Category and select or clear the corresponding check box for the permissions. The types of permission you can grant are:

Table 7: Permission Types

Permission Type	Description
View	Provides only read-only access to the function.
Manage	Provides access to read and manage tasks associate with the function.

Step 5 Click Save.

Managing Tenants, Tenant Groups, and Users

The multitenant architecture of MSX provides the ability to segment the data stored by a tenant. When tenants are defined, data is partitioned by a tenant, thus providing data security and privacy for each tenant. This multitenant approach allows cloud or managed service providers to consolidate many smaller customer configurations on a set of infrastructure servers.

Consider the following points while configuring tenants:

- Tenant administrators are linked to their data by a tenant object.
- Tenant objects should be consistent and unique across all clusters.
- A tenant administrator cannot view or modify the data of another tenant.

Managing Tenants

To manage tenants:

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click Tenants to view the list of existing tenants (customers) with their details on the Manage Tenants page.

- To add a new tenant, click Add Tenant and enter the customer name and description, email address, website URL, and contact number.
 - Click Save. The new customer details are listed on the Manage Tenants page.
 - To update the tenant details, select the tenant on the list and click the Edit icon.
 - To delete a tenant, select the tenant from the list and click the Delete icon.
-

Managing Tenant Groups

After you create tenants, you can configure the tenant groups, which are a collection of tenants that are grouped for the purpose of assigning a common list of functions such as, service extensions parameter values and so on.

To manage tenant groups:

- Step 1** Log in to the Cisco MSX Portal.
 - Step 2** In the main menu, click Tenant Groups to view the list of tenant groups with their details in the Manage Tenant Groups window.
 - Step 3** Click Add Tenant Group.
 - Step 4** Enter the tenant group name and description.
 - Step 5** Select the tenants that you want to add to the tenant group.
 - Note** A tenant can be associated with only one tenant group. The Tenant drop-down lists only those tenants which are not associated with any tenant group.
 - Step 6** Click Save.
-

Managing Users

You can add new user details, assign appropriate role to the user, and associate the new user to the tenant.

To manage users:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, click Users to view the list of users with their details in the Manage Users window.
- Step 3** Click Add User and enter the username and ID, email address, and contact number.
- Step 4** To assign a role, you can choose from the available options.
 - Note** For more information on categories and permissions for the Cisco MSX SD-WAN service pack, see [Cisco Managed Services Accelerator \(MSX\) 4.2 Platform and Service Pack Permissions Addendum](#)
- Step 5** Select a tenant from the Associate Tenants drop-down list.

Step 6 Click Save. The new user details are displayed in the Manage User window username.



CHAPTER 5

Managing Cisco SD-WAN vEdge Cloud TDE Templates

Cisco SD-WAN coordinates with SD-Branch service pack to deploy virtual vEdge on ENCS. To simplify the deployment of the virtual branch that gets hosted on the ENCS unit, operators can use existing vEdge cloud TDE templates in MSX and collect inputs from users associated with the parameters used in the branch.

Along with the vEdge cloud templates, ensure you have the desired version of the vEdge image available within MSX or on a webserver to deploy devices on ENCS.

Generate vEdge TAR image for new Cisco SD-WAN versions or custom root certificates. The process of generating vEdge TAR image for deploying vEdge Cloud on ENCS device is available in the [Cisco MSX DevNet Portal](#) documentation.

By default, the following onboarding types will use the following template and image for both new install or upgrade:

1. Open Network Policy:
 - Internal value: ("standard")
 - TDE Template file name: DualIP-vedge19.1.0-msx3.6.tar.gz (image)
 - NFVIS < 3.11
2. 2 Public IP Addresses:
 - Internal value: ("standard-secure")
 - TDE Template file name: DualIP-vedge19.1.0-msx3.6.tar.gz (image)
 - NFVIS 3.11, 3.10.2+
3. Single Public IP:
 - Internal value: ("single_ip_secure")
 - TDE Template file name: SingleIP-vedge19.1.0-msx3.6.tar.gz (image)
 - NFVIS 3.11, 3.10.2+

For more information on these onboarding types, see Step 15 in [Adding a vEdge Cloud Device](#).

The topics below describe how to manage vEdge cloud templates in MSX.

- [Uploading a vEdge Cloud Template, on page 30](#)
- [Deleting a vEdge Cloud Template, on page 31](#)
- [Managing vEdge Cloud Template Access for Tenants, on page 31](#)

Uploading a vEdge Cloud Template

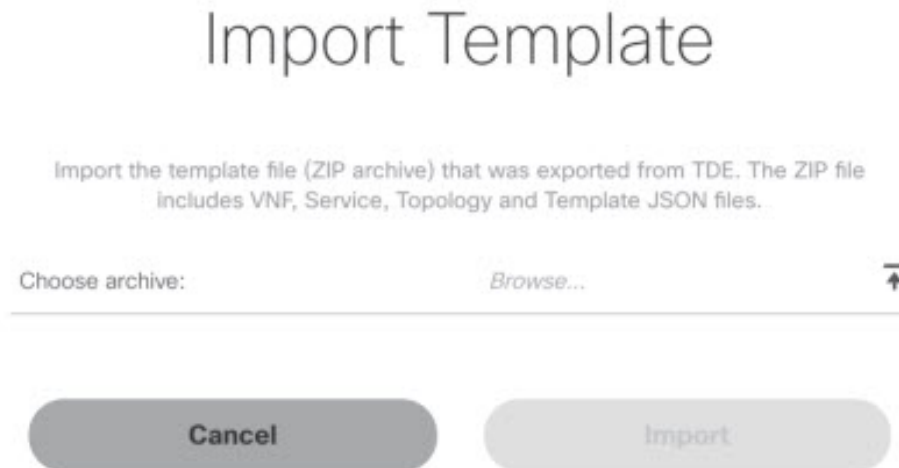
Before you begin

Download the vEdge templates from [DevNet Portal](#) and save it on your local.

To upload a template:

-
- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, choose Settings > Service Configuration.
- Step 3** Click SD-Branch and then click the Settings > Template Management. The Manage Template appears.
- Step 4** To add a new template:
- Select Import Template. The Import Template dialog box appears.

Figure 4: Import Template



- Click the Browse icon to upload the zip file that has VNF file, Service file, Topology file, or Template file. This zip file was downloaded from Cisco DevNet Portal and was saved in your local directory.
- Click Import.

Note The template name is defined in the template.json and topology.json file.

- Step 5** To modify an existing template:
- Select the template that you want to modify and select Import Template. The Import Template dialog box appears.

- b) Click the Browse icon to upload the zip file that has VNF file, Service file, Topology file, or Template file. This zip file was downloaded from Cisco DevNet Portal and was saved in your local directory.
 - c) Click Import.
-

Deleting a vEdge Cloud Template

To delete a template version:

- Step 1** Log in to the Cisco MSX Portal.
 - Step 2** In the main menu, choose Settings > Service Configuration.
 - Step 3** Click SD-Branch and then click the Settings > Template Management. The Manage Template appears and list the existing templates.
 - Step 4** Select the template version that you want to delete and click the Delete (X) icon. A confirmation dialog box appears.
Note You cannot delete a template version if the template version is associated with a site.
 - Step 5** Click Delete Template.
-

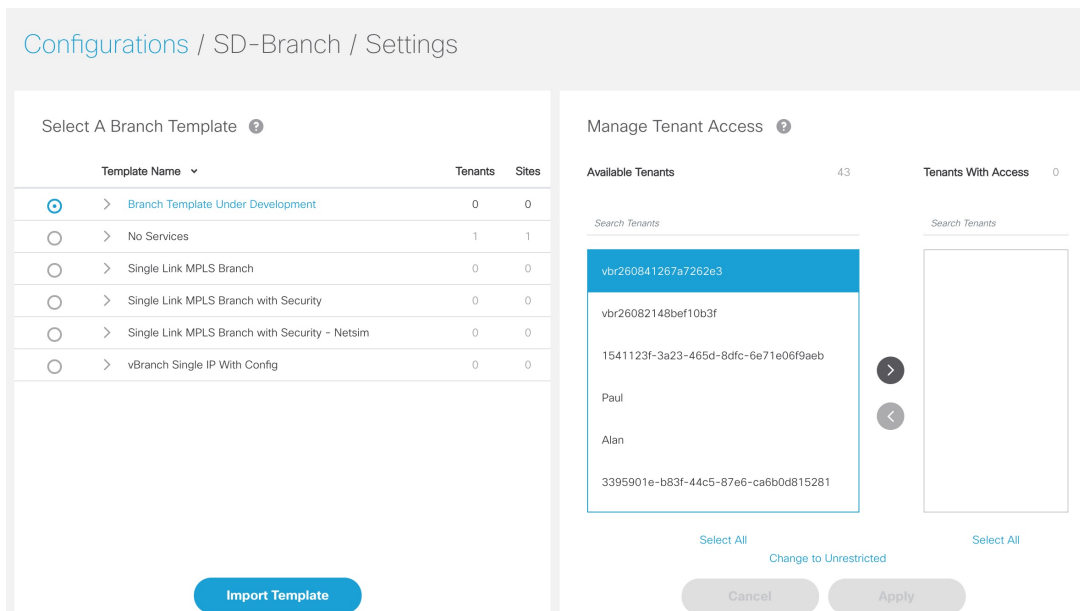
Managing vEdge Cloud Template Access for Tenants

After the cloud service (vEdge cloud) templates are created via TDE and uploaded into MSX, use this procedure to assign these templates to a tenant user. These templates will then be visible to a tenant user while adding a site.

To assign or modify template access for tenants:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, choose Settings > Service Configuration.
- Step 3** Click SD-Branch and then click the Settings > TemplateManagement. The Manage Template appears and list the existing templates.

Figure 5: SD-Branch Settings

**Step 4**

To assign the template to a tenant:

- Click the template that you want to assign to the tenant.
- Select the template version.
- To display the template version, click >.
- In the Available Tenants list, select one or more tenant users to assign the template to. To assign the template to all the tenants, click Select All.
- Click >. The tenant record(s) moves to the Tenant With Access list.
- Click Apply.

Step 5

To remove access to a template:

- Click the template that for which modify the access.
- In the Tenants with Access list, select the tenant to revoke the access. To revoke the access for all the existing and future customers, click Select All.
- Click <. The tenant records moves to the Available Tenant list.

Note For a tenant with active sites that use a template, the tenant user continues to appear in the Tenants with Access list, but is dimmed, if you remove access.

- Click Apply.



CHAPTER 6

Deploying Cisco SD-WAN Services on MSX

This chapter details the procedures for deploying Cisco SD-WAN services on Cisco Managed Services Accelerator (MSX).

- [Deployment Workflow for Cisco SD-WAN](#), on page 33
- [Setting Up Control Plane for Cisco SD-WAN](#), on page 34
- [Postdeployment Tasks for SD-WAN Control Plane](#), on page 42
- [Attaching Control Plane](#), on page 50
- [Deploying a Device for Cisco SD-WAN](#), on page 51
- [Provisioning a Device](#), on page 67
- [Configuring Traffic Policies](#), on page 67
- [Maintaining Cisco SD-WAN Deployments](#), on page 72

Deployment Workflow for Cisco SD-WAN

Using the workflow in the table below, you can deploy Cisco SD-WAN vEdge Cloud, or vEdge SP Cloud, or the Physical site.

Table 8: Workflow for Cisco SD-WAN vEdge Cloud, or vEdge SP Cloud, or Physical Sites

Task	See
1. Attach an existing control plane or create a new control plane.	Setting Up Control Plane for Cisco SD-WAN
2. Complete Control Plane post deployment tasks.	Postdeployment Tasks for SD-WAN Control Plane
3. Add a vEdge Cloud or vEdge SP Cloud or a Physical Site/Device.	<ul style="list-style-type: none">• For vEdge Cloud, see Adding a vEdge Cloud Device.• For vEdge SP Cloud, see Adding a vEdge SP Cloud Device.• For Physical site, see Adding a Physical Device.
4. (Optional) If you have details of multiple sites available, you can import these details into MSX.	Importing Multiple Site Data from Cisco SD-WAN into MSX

Task	See
5. Push the site details to the Control Plane such that the device is set up for day one configurations.	Provisioning a Device
6. Verify all the components of SD-WAN service are deployed.	Monitoring SD-WAN Control Plane Status
7. Configure Traffic Policies	Configuring Traffic Policies

Setting Up Control Plane for Cisco SD-WAN

The deployment of an SD-WAN service in the context of a managed service requires deployment per customer and includes the SD-WAN management control plane (vManage, vBond and vSmart), and the corresponding data plane (vEdge and cEdge).



Note This section describes the steps required to set up MSX control plane on both AWS and OpenStack.

The following are the topics covered in this section:

Prerequisites for Setting Up Control Plane

This section lists the common prerequisites as well as OpenStack and AWS-specific prerequisites for setting up Control Plane.

Control Plane Prerequisites for both AWS and OpenStack

The following are control plane prerequisites applicable for both AWS and OpenStack environment:

- Contact Cisco Account representative for:
 - Setting up a Smart Account if you are a Service Provider, or you can request for a smart account here: <https://software.cisco.com>.
 - Creating a Virtual Account for a new tenant (Service Provider end customer) and associating it to the service provider smart account. A Virtual Account is necessary for every new SD-WAN tenant.
 - Requesting for Cisco SD-WAN orchestration stack environment. This is required to spin up control plane components on AWS.
 - Ordering physical devices and virtual devices through Cisco Commerce Workspace (CCW).
 - Associating the purchased devices to the Virtual Account.

After devices are associated with your smart account, you can synchronize the device details on the Control Plane after setting the Control Plane. For more information, see [Synchronizing Smart Accounts from the Control Plane](#).

- Assign 'SD-WAN Control Plane' permission to the user who will create a Control Plane for the tenant. Along with the control plane permission, assign other SD-WAN permissions to the user managing

SD-WAN services. For more information on the SD-WAN-specific permissions and to associate these permissions to a role, see [Managing Roles in Cisco MSX](#).

- Create a new SD-WAN tenant for the Service Provider end customer on MSX, see [Managing Tenants](#) and [Managing Users](#).
- If you have an SD-WAN deployment with vManage connected, your external certificates must be copied and imported into the centralized MSX keystore. Contact your Cisco representative to add your external certificates to MSX.

Control Plane Prerequisites Applicable Only For AWS

The following are control plane prerequisites for AWS:

- Provide the SD-WAN orchestration settings to integrate MSX with Cisco SD-WAN orchestration stack. For more information, see [Configuring Cisco SD-WAN Orchestrator Settings](#).
- Add Cisco MSX and Tenants IP Subnets in the MSX Allowed List: For Cisco MSX to create SD-WAN Control Planes, it needs to be able to communicate with the Cisco SD-WAN Orchestration stack which is protected by secure IP. Do the following to add these IP to the allowed list in MSX:
 1. Determine the source IP addresses of an Cisco MSX deployment:
 - If Cisco MSX is installed on AWS: These are the NAT GW IP addresses. Go to VPC > NAT Gateway dashboard on your AWS console. There should be three IP addresses, one for each public subnet.
 - If Cisco MSX is installed on-prem: This will be proxy IP, if no proxy, then use the Cisco MSX public IP.
 2. Contact Cisco TAC, submit your tenant users IP subnet and request to add these to the allowed list on SD-WAN Orchestration Stack for HTTPS/443 port.



Note If you use Cisco MSX to access the control plane, you do not have to add tenant's IPs to the allowed list as MSX connects to the control plane using an MSX-managed proxy. This functionality is not enabled by default and can be configured using an API. For more information, see [Disabling MSX-Managed Proxy](#).

Control Plane Prerequisites Applicable Only For OpenStack

The following are control plane prerequisites for OpenStack:

- You can customize Cisco MSX to create control plane in OpenStack environment. Leverage and deploy an ansible API playbook. This will install the additional OpenStack Orchestration (OSorch) micro-services in the Cisco MSX.
 1. Create flavors, these are hardware specifications such as vCPU, Root Disk, RAM, and so on. Provide the hardware details that are required for creating control plane on OpenStack.



Note OS orchestration creates 100G (vManage) volume as part of the deployment

2. Download the qcow images from the SD-WAN [Cisco website \(CCO\)](#) and upload it into OpenStack cloud.

- To install the OS orchestrator from the deployer system, execute the following command:

```
export ANSIBLE_VAULT_PASSWORD_FILE=/tmp/ansible-vault-password
cd /msx-4.1.0/ansible/
ansible-playbook -i inventory/inventory deploy-osorch.yml
```

Creating Control Plane on OpenStack

You need to specify the following attributes while creating SD-WAN control plane on OpenStack.

Table 9: Attributes Used in Creating SD-WAN Control Plane in OpenStack

Key Options of OS orchestrator	Explanation
Provider Network	<ul style="list-style-type: none"> • Create a control plane using the existing network on OpenStack cloud. • The control plane is established using the existing subnets that are already provisioned on the Openstack cloud, it has dedicated subnets setup for different customers.
Tenant Network	<ul style="list-style-type: none"> • Create a newly dedicated network for the customer. • Deploy the required VPN0, VPN512, and floating IPs on the OpenStack to create an SD-WAN control plane on OpenStack. <p>Note</p> <ul style="list-style-type: none"> • Ensure floating IP addresses are available for assignment to Viptela VMs. Each control plane requires six floating IP addresses (two per instance). • Additionally two more floating IPs are created for Openstack routers as part of Tenant network flow.

Key Options of OS orchestrator	Explanation
Multi-Tenant	<ul style="list-style-type: none"> • Create an SD-WAN control plane on a dedicated tenant project space. This option is used both in provider and tenant network. • OS orchestrator supports creating instances on multi-tenant or project space on the OpenStack cloud. <p>Note Change the "projectName" and "projectID" values in the add vim payload to reflect the Tenant/Project space that is to be configured.</p>
Enterprise Certificate Authentication (CA)	<ul style="list-style-type: none"> • Cisco MSX automatically creates CA, then generates Certificate Signing Request (CSR). • Use this certificate to sign in. This is a part of deployment activity. • Thus, creates fully configured control plane instances that are ready for vEdge site deployment. <p>Note To select this option, include 'createCA: true' in the create control plane payload.</p>
Default Symantec/Cisco CA	<ul style="list-style-type: none"> • Log in to vManage to generates CSR, and sign in using the CSR certificate for deploying the control plane. • Once you deploy the control plane instances state are moved 'Up'. <p>Note</p> <ul style="list-style-type: none"> • To select this option include 'createCA: false' in the create control plane payload. • For the OpenStack network, use symantec as the default enterprise Root-Certificate Authentication (CA) to activate Viptela controller during the day0 configuration process.

- To create a control plane on OpenStack environment, use curl command from Kubernetes-master mode.
- The OS orchestrator requires authorization token, and to get the token use the following curl command:

```
curl -k https://<MSX fqdn>/idm/api/v1/login -XPOST -d '{"username": "username", "password": "<password>" }' -H 'content-type: application/json'
```

- Enter authorization token as the value of the authorization parameter, as shown in the sample:
This is an sample curl command for creating and deleting VIM:

```
curl -H "Authorization: Bearer <token>" http://osorch.service.consul:8080/osorch/v1/vims -X POST -H "Content-Type: application/json" -d '<payload>'
curl -H "Authorization: Bearer <token>" http://osorch.service.consul:8080/osorch/v1/vims -X DELETE -H "Content-Type: application/json" -d '<payload>'
```



Note You can enter the valid values in <token> and <payload>.

- This table below various APIs used in managing SD-WAN control plane on OpenStack.

Table 10: Tasks involved in Creating SD-WAN Control Plane

Request Type	API	Description
Create VIM	POST /osorch/v1/vims	<ul style="list-style-type: none"> • You can choose either the Provider network or Tenant network based on the OpenStack cloud requirement. • Make API call using curl command. Ensure that you copy the ID that is obtained as response, as the ID is needed to create the CP payload.
Delete VIM	DELETE /osorch/v1/vims/{vimID} Use the given API in the DELETE job and monitor the progress using the jobs API: GET /osorch/v1/vims"	<ul style="list-style-type: none"> • Receives request to delete VIM, initiates the cleanup activity, and finally deletes the VIM. <p>Note To delete VIM, enter the vimID. The vimID is returned as a response for creating the VIM.</p>
Create CP	POST /osorch/v1/cps	<ul style="list-style-type: none"> • Receives request to prepare OpenStack cloud for creating a control plane. • Deploys CP instances and configures them to create the control plane on OpenStack.
Delete CP	DELETE /osorch/v1/cps/{cpID} Use the following API in DELETE job and monitor the progress using the jobs API: GET /osorch/v1/cps	<ul style="list-style-type: none"> • Receives request to delete the control plane, this initiates the OpenStack cleanup activity. Finally deletes the control plane. <p>Note To delete CP, enter the cpID. The cpID is returned from the create CP response.</p>
Get the Create/Delete job status	GET/osorch/v1/jobs/{jobID} <p>Note The jobID is the response from this API or "GET /osorch/v1/cps" to check the job status.</p>	<ul style="list-style-type: none"> • This API is used to check the create/delete transaction status.

Request Type	API	Description
Get all Templates	GET /osorch/v1/templates	<ul style="list-style-type: none"> Displays all the available templates in OS orchestration and allows you to edit the content of the templates. Make the API call using the curl command.
Get Content of a Template	GET /osorch/v1/templates/{templateName}	<ul style="list-style-type: none"> Displays the content of a specific template. You can edit the content of the specific template.
Change the Template	POST /osorch/v1/template	<ul style="list-style-type: none"> You can change the values of several template parameters using this API.

For information about the sample JSON files of the payloads that are involved in creating the control plane, see [Sample Payloads for Creating Cisco SD-WAN Control Plane on Openstack](#).



Note After the process is complete, an email is sent to the user whose email address was provided during the control plane creation process. The email includes the link to the vManage URL and the organization name. Attach the control plane to SD-WAN Tenant on Cisco MSX using the vManage URL. For more information, see [Attaching Control Plane](#).

The control plane instance is blank and has a default admin user. Controllers in the Control Plane appears in the alarm state as the controllers are not enrolled with a certificate authority and also does not have secure control connections between the controllers. To fix the alarm state, complete all the post-deployment tasks. For more information, see [Postdeployment Tasks for SD-WAN Control Plane](#).

Creating Cisco SD-WAN Control Plane on AWS

To create an SD-WAN control plane service on AWS:

Before you begin

You must configure the SD-WAN Orchestrator (vOrch) settings for your SD-WAN setup before you create an SD-WAN control plane service on AWS. For more information, see [Configuring Cisco SD-WAN Orchestrator Settings](#).

-
- Step 1** Log in to the Cisco MSX Portal.
 - Step 2** From the left pane, click Tenant Workspace > Services.
 - Step 3** From the SD-WAN service panel, click Setup to add a control plane.
 - Step 4** Click Get Started to launch the Add Control Plane wizard.
 - Step 5** Click the Create New Control Plane radio button to create a new control plane for the tenant.

Step 6 In the Control Plane Information section:

Figure 6: Control Plane Information Fields While Creating Control Plane on AWS

- Enter the Virtual Account Name: The service provider creates a Virtual Account (VA) to manage the licenses and assets of the tenant.
- Select a Cisco SD-WAN Software version from the list of versions available. For more information, see [Cisco SD-WAN and MSX Version Compatibility Matrix](#).
- Enter your email address, to receive an information about the creation process and an approved Certificate Signing Request (CSR) message.

Step 7 In the Control Plane Instances section:

- Enter the network size.
- Select the Primary AWS Region, which will be used as the primary region for all the SD-WAN Control Plane instances.
- Select the Secondary AWS Region, where a backup of the control plane is created for large-sized networks.
- If the secondary region is not selected, the instances are created in the primary region itself, and vManage backup process is not possible.

Step 8 In the Recommended Instances section:

Figure 7: Recommended Number of Instances

Review Recommended Instances

The control plane always consists of three parts: vManage, vSmart and vBond. Each may require several instances depending on how large the controlled network is. Below are the recommended instances. Click each tab to review the suggestions and make adjustments if needed.

vManage vBond vSmart

Instance Size: **c5.4xlarge** [Edit Instances](#)

vManage Volume Size: **500 GB**

Region: **US West (N. California)**

NAME	AVAILABILITY ZONE	BACKUP REGION
vManage-sarada_create-1	us-west-1a	US West (Oregon)

Back Submit

- a. The SD-WAN Control Plane has three parts: vManage, vSmart, and vBond.

Based on the desired size of the network, the Cisco MSX calculates and suggests the number of instances, and instance sizes. Cisco MSX automatically populates the instance name based on the Tenant name.

- If you find the recommended number of instances to be acceptable, click Submit. Cisco MSX starts to provision the Control Plane.
 - To edit the recommended number of instances, click Edit Instances in the vManage, vSmart, and vBond sections. You can also edit the Instance Names, Regions, and Availability Zones.
 - The Region and Backup Region are populated automatically based on your selection of Primary AWS region and Secondary AWS region.
 - The Availability Zones (AZ) are different for different instances and are populated automatically.
- b. The vManage instances are deployed in the Region and backup is stored in the Backup Region. Usually, backup happens once in a day and the backup information is retained for ten days.
- If there are multiple vManage instances, then the Region should be the same for all the vManage instances. For example, the Region can be either us-east-1 or us-west-2 (retain the same Region for all the instances).
 - For all the vManage instances, the Backup Region should be any region other than what was specified in Region. For example, if the Region is us-east-1, then the Backup Region can be us-west-2.
- Backup is possible only in the vManage and is specified in the vManage section. The backup information is stored in the Backup Region.
- c. The vSmart and vBond instances are evenly distributed across the Primary AWS region and the Secondary AWS region. For example, if there are six vSmart instances, then three vSmart instances are deployed in us-east-1 region and the other three vSmart instances are deployed in us-west-2 region.

Step 9 Click Submit to start the control plane creation process.

A notification on the control plane creation process appears at the top of the SD-WAN home page for a few seconds.

Even if there is an intermediate error in creating the Control Plane, the system continues to poll until the creation process is complete. The Control Plane creation process can take up to an hour or more. The progress is tracked in the Event Log. For information on accessing event logs, see [Viewing Event Logs](#).

After the process is complete, an email is sent to the user whose email address was provided during the control plane creation process. The email includes the link to the vManage URL and the organization name. Use this URL to login with default credentials.

Click View Details to view the status of the control plane and the instances in the SD-WAN service panel. You can also click on the ellipsis (...) and click Control Plane Details. For more information, see [Monitoring SD-WAN Control Plane Status](#).

What to do next

The control plane instance is blank and has a default admin user. Controllers in the Control Plane appear in the alarm state as the controllers are not enrolled with a certificate authority and also do not have secure control connections between the controllers. To fix the alarm state, complete all the post-deployment tasks. For more information, see [Postdeployment Tasks for SD-WAN Control Plane](#).

Postdeployment Tasks for SD-WAN Control Plane

This section details various tasks that must be performed after attaching or creating the Control Plane (vManage) on MSX for Cisco SD-WAN.

Table 11: Post Control Plane Deployment Tasks

Task	Description	Reference
1. Log in to the SD-WAN Control Plane	Log in to the Control Plane from MSX Portal or using the URL sent in an email after the control plane is created.	For more information, see Logging in to the Cisco SD-WAN Control Plane .
2. Create a new user on the Control Plane.	Create an additional user as soon as the Control Plane is set up.	For more information, see Creating a New User on the Control Plane .
3. Update Smart Account details on the Control Plane.	Update the smart account credentials including the certificate retrieval interval and validity period.	For more information, see Updating Smart Account Details .
4. Generate the PKI certificates.	Generate PKI certificates for all controllers on the Control Plane.	For more information, see Generating PKI Certificates on the Control Plane .
5. Synchronize your Smart Account (SA) to get the device details associated with your smart account on the control plane.	Synchronize your SA to upload the device list on your Control Plane.	For more information, see Synchronizing Smart Accounts from the Control Plane .
6. (Optional) Manage SSL certificates.	Generate and upload the SSL certificate after changing the domain name of the Control Plane.	For more information, see Managing SSL Certificates .

Task	Description	Reference
7. (Optional) Enable Single-Sign On for Cisco MSX	Enable Single-Sign On for Cisco MSX with SD-WAN Control Plane on both AWS and OpenStack.	For information on configuring SSO, see the Configuring Single Sign-On .
8. Add Device templates on the Control Plane.	<ul style="list-style-type: none"> Use out-of-the-box device templates available within MSX. <p>OR</p> <ul style="list-style-type: none"> Import the device templates that are already available within the particular tenant's Control Plane into MSX. 	For more information, see Importing and Exporting Cisco SD-WAN Device Template .
9. Add tenant source IP address to the Control Planes.	To allow MSX tenant users to access the control plane, add tenant users IP subnet to the allowed list on SD-WAN Orchestration Stack for HTTPS/443 port. To add the tenant subnet to the allowed list, contact Cisco TAC.	--

Logging in to the Cisco SD-WAN Control Plane

SD-WAN Control Plane web interface access is required for:

- Upgrading control and management components (vManage, vSmart, vBond)
- Upgrading data plane components (vEdges)

You can access SD-WAN Control Plane web interface in one of the following ways:

- Access Control Plane using the URL: The URL is sent through email that was provided during the control plane creation process. This email is sent after the Control Plane is created.

`https://<vManage server-ip>`

Where :

<vManage server-ip>: Is the IP address or fully qualified domain name (FQDN) name of the SD-WAN Control Plane server.

- Access Control Plane from the MSX Portal: If the SSO is enabled between MSX and SD-WAN Control Plane, you can directly access the Control Plane by clicking the View Control Plane Portal option on the MSX SD-WAN home page > Control Plane Status window.



Note Use the default admin user and the system-generated password to login to the Control Plane web interface. You can view this password by editing the control plane details. For more information, see [Editing an SD-WAN Control Plane](#).

Creating a New User on the Control Plane

A user, including admin, can be locked out from the Control Plane web interface after several failed attempts, so as a best practice, Cisco recommends creating an additional user as soon as the Control Plane is set up.

-
- Step 1** Log in to the SD-WAN Control Plane web interface as the admin user. For more information, see [Logging in to the Cisco SD-WAN Control Plane](#).
- Step 2** Create an additional user with netadmin user role privilege on the Control Plane. For more information on creating users on the control plane, see [Cisco SD-WAN Documentation](#).
- Note** Use quotes when creating passwords with special characters. For example: "Password!234".
- Step 3** Verify the newly created user can successfully login.
-

What to do next

To use the new username and password for accessing the Control Plane web interface, do the following:

- Change the passwords for SD-WAN controllers (vBond and vSmart) from the Control Plane console. For more information, see [Change SD-WAN Controllers Password](#).
- Optionally, edit the control plane details from the MSX Portal. For more information, see [Editing an SD-WAN Control Plane](#).

Updating Smart Account Details

Use this procedure to configure the smart account details such as smart account username, password, certificate validity period, and so on.

-
- Step 1** Log in to the SD-WAN Control Plane web interface. For more information, see [Logging in to the Cisco SD-WAN Control Plane](#).
- Step 2** In SD-WAN Control Plane console, choose Administration > Settings.
- Step 3** Under the Controller Certificate Authorization section, do the following:
- Select the certificate signing authority.
 - Set the validity period you want the certificate to be valid for.
 - Set the certificate retrieval interval.
- Step 4** Under the Smart Account Credentials section, edit the username and password.
- Step 5** Click Save.
-

Generating PKI Certificates on the Control Plane

Use this procedure to generate the certificates for all controllers on the Control Plane.

Before you begin

Configuring Smart Account details. For more information, see [Updating Smart Account Details](#).

-
- Step 1** Log in to Cisco SD-WAN Control Plane web interface. For more information, see [Logging in to the Cisco SD-WAN Control Plane](#).
- Step 2** In SD-WAN Control Plane web interface, choose Configuration > Certificates. The Configure | Certificates screen appears.
- Step 3** In the Controllers tab, the list of controllers will be shown with a Public IP and “No certificate installed” in the Certificate Serial column. Click on the ellipsis (...) and click Generate CSR.

Note First generate the CSRs for vManage, then vBonds, and finally the vSmarts.

After a few seconds, a confirmation message is displayed with the IP of the corresponding device. The operation status of the vManage is changed to 'vBond Updated' after the certificate signing is completed, and the Certificate Serial field is populated with a string.

- Step 4** Repeat the previous step for generating CSR for vBond and vSmart controllers.
- The signed certificates are securely pulled from the PnP portal and installed. Once this process is complete, all the controller spinners turn green in the MSX Portal, indicating that all controllers are up without any alarms. For more information on viewing control plane status in the MSX Portal, see [Monitoring SD-WAN Control Plane Status](#).

What to do next

Synchronize your Smart Account to upload the device list on your Control Plane. For more information, see [Synchronizing Smart Accounts from the Control Plane](#).

Synchronizing Smart Accounts from the Control Plane

After the Control Plane instances are created, you can sync your Smart Accounts from the SD-WAN Control Plane Portal to download the device list information for device onboarding.



Note Ensure the devices are associated with the virtual account before synchronizing the details into the Control Plane.

To download device list on tenant's Control Plane:

-
- Step 1** Log in to Cisco SD-WAN Control Plane (vManage). For more information, see [Logging in to the Cisco SD-WAN Control Plane](#).
- Step 2** In vManage Portal, choose Configuration > Devices. The Configure | Devices screen appears.
- Step 3** Enter the username and password information for the Control Plane Overlay.
- Step 4** Under the WAN Edge List, choose Sync Smart Account > Sync.
- All devices assigned to this virtual account will appear under the WAN Edge List tab.
-

Managing SSL Certificates

Use this procedure to generate and upload the SSL certificate after changing the domain name of the Control Plane.

Step 1 Generate a web SSL certificate for your domain name and upload it on the Control Plane (vManage). For more information, see the *Cisco SD-WAN documentation*, or contact Cisco Technical Assistant Centre (TAC).

Note Ensure the new domain name points to the MSX-generated domain name of the control plane.

Step 2 Edit the control plane details from the MSX Portal to use the new URL of the Control Plane. For more information, see [Editing an SD-WAN Control Plane](#).

Change SD-WAN Controllers Password

After creating a new user with netadmin privilege on the Control Plane, use this procedure only if you want the controllers to use the new credential.

Before you begin

Generate the certificates and ensure the controllers are configured.

Step 1 Log in to the SD-WAN Control Plane console as the admin user. For more information, see [Logging in to the Cisco SD-WAN Control Plane](#).

Step 2 In SD-WAN Control Plane console, click Tools > SSH Terminal.

Step 3 SSH to one of the controller.

All the controllers associated with your smart account appears in the Controllers tab. Access your controllers using the IP addresses listed in the Controllers window.

Step 4 Use the following command to change the password of a controller:

```
conf
system aaa user MyNewUsername password MyNewPassword
group netadmin
commit
end
```

Step 5 Repeat Step 3 and 4 for other controllers.

Step 6 Verify that you can login to each of these controllers with the newly created username and password.

Importing and Exporting Cisco SD-WAN Device Template

For running the Cisco SD-WAN-managed devices in an overlay network, you must apply appropriate network topologies and configurations. These configurations can be applied to a device using device template. These device templates must be created on vManage every time a new Cisco SD-WAN system is set up for a new tenant. For more information on how to create the device templates, see [Cisco SD-WAN documentation](#).

To avoid creating a new device template on vManage system, every time a new tenant is onboarded, you can do one of the following through Cisco MSX:

- Use out-of-the-box device templates provided in MSX. There are seven out-of-the-box device templates, which you can modify as per your requirements. Export these out-of-the-box device templates to your tenant's control plane and use them as it is or modify them as per your requirements. For details on attributes available in each of these templates, see [Out-of-the-Box Cisco SD-WAN Device Templates Available Within MSX](#).
- Use a tenant's device templates. If you want to use the device templates that are already created within the particular tenant's Cisco SD-WAN control plane, the import functionality in Cisco MSX allows you to import these templates into the centralized Cisco MSX library. After the import, you can push these templates to the new tenant's SD-WAN control plane.

Import and Export of Device Templates Containing Security Policies

MSX also supports the import and export of the device templates that contain security policies. MSX supports the following security policies:

- URL Filtering
- Intrusion Protection Service (IPS)
- Advanced Malware Protection (AMP)

The following are the limitations of importing and exporting device templates that include security policies:

- If the device template consists of security policy other than the supported policies, then the import process would fail.

The version of the control plane where you plan to export the device template (For example: 20.3.2) must be the same or later than the version of the control plane from where you originally imported it (For example: 19.2.3).



Note Exporting device template to an older version of the control plane might result in failure if some of the feature templates are not supported on the older control plane.

- While exporting the device templates, you might notice the following behaviour:
 - During validation, if there is a connectivity or control plane issue, the export process may be interrupted, and the security policies are not created. In such scenario, export the device templates again.
 - During export, if there is a connectivity or control plane issue, the export process may be interrupted, and some security policies are not created. In such scenario, consider exporting the device template again. Only the missing policies from the previous export are created.
- Cisco MSX does not import or export the Threat Grid API key associated with the AMP security policy. For the AMP security policy to work successfully, enter a valid key in the destination control plane. For more information, see "Configure Threat Grid API Key" section in the "Advanced Malware Protection" chapter of the [Cisco SD-WAN Security Configuration Guide](#).

For information on Cisco platform that supports SD-WAN security, see [Cisco SD-WAN](#) documentation.

To import and export the device templates, see the procedures below.

Importing Device Templates from a Tenant Cisco SD-WAN System to the MSX Library

Before You Begin

- Subscribe to the SD-WAN service for a specific tenant, set up a Control Plane, and ensure that the Control plane is up and running. For more information, see [Setting Up Control Plane for Cisco SD-WAN](#).
- Ensure that the device templates are available on vManage . For more information on creating device templates on vManage, see [Cisco SD-WAN documentation](#).
- Use Tenant Admin role or create or edit an existing role with the permissions listed below and then assign the role to a user. To create or modify a new role, from the MSX main menu, click Roles > Add Roles or edit role option (Edit icon), and assign the following permissions to the roles:
 - From the Services, Configurations, and Devices category, assign the following permissions:
 - Service Configurations (View/Manage)
 - Service Configuration Assignments (View/Manage)
 - Service Configuration Audit (View)
 - From the Users, Roles, and Tenants category, assign the 'All Tenants' permission.
 - From the Bulk Import Sites/Devices/Tenants/Users category, assign Bulk Import (Manage) permission.



Note For the Tenant Admin role or any new role, it is necessary to apply the Bulk Import (Manage) permission for the device template functionality.

To import the existing device templates from SD-WAN vManage to the MSX Library:

-
- Step 1** Log in to the Cisco MSX portal using your credentials.
 - Step 2** From the left hand pane, choose Settings > Template Management.
 - Step 3** Select the SD-WAN tile to display the Template Management window.
 - Step 4** To import a device template into the MSX library:
 - a) On the Template Management window, click the + icon to display the Template Import Wizard.
 - b) Click > and select a tenant from the drop-down list from where the template has to be imported.
 - c) Click >. The window displays the list of available templates for the selected tenant.
 - d) Select a template and click > to start the import process.
 - e) Track the progress in the Template Activity window. You can access the Template Activity screen in one of the following ways:
 - During the import process, click View Template Activity option from the Import window.
 - After the import process, click the History icon from the SD-WAN Template Management window.

If the import process fails, hover the mouse pointer over the failed status on the Template Activity window to view detailed information.

You can also delete a template by selecting a template you want to delete, and click (...) > Delete option.

Exporting Device Templates from the MSX Library to a Tenant Cisco SD-WAN System

To reuse an existing device template from one tenant system to another tenant, you must first import these templates into MSX. After the import, you can select the templates from the MSX library and export it to another tenant's system.

Before You Begin

1. Ensure that the device templates are available in the MSX library. If there are no templates available, import the templates from an existing tenant's SD-WAN system (vManage) to the MSX library. For more information, see [Importing Device Templates from a Tenant Cisco SD-WAN System to the MSX Library](#).
2. Use Tenant Admin role or create or edit an existing role with the permissions listed below and then assign the role to a user. To create/modify a new role, from the MSX main menu, click Roles > Add Roles or edit role option (Edit icon), and assign the following permissions to the role from the Services, Configurations, and Devices category.
 - Service Configurations (View/Manage)
 - Service Configuration Assignments (View/Manage)
 - Service Configuration Audit (View)
 - From the Bulk Import Sites/Devices/Tenants/Users category, assign Bulk Import (Manage) permission.



Note For the Tenant Admin role or any new role, it is necessary to apply the Bulk Import (Manage) permission for the device template functionality.

Use the below procedure to push the device templates available in the MSX library to the new tenant's SD-WAN control plane.

-
- Step 1** Log in to the Cisco MSX portal.
 - Step 2** From the left hand pane, choose Settings > Template Management.
 - Step 3** Select the SD-WAN tile to see the list of available templates on the Template Management window. The SD-WAN Template Management window lists templates that are currently available in the MSX library. If you do not see any templates on this screen, first import templates into MSX library. See the procedure [Importing Device Templates from a Tenant Cisco SD-WAN System to the MSX Library](#).
 - Step 4** Select one or more templates and click (...) > Assign Tenants option to display the wizard.
 - You can also expand the template, and click Assign Tenants option to display the wizard.
 - You can do a bulk export of the device templates from the MSX Library to a new tenant's SD-WAN system by selecting all the templates, and click (...) > Assign Tenants option.

- Step 5** Choose one or more tenants from the drop-down list and click > to start the export process.
- Step 6** Click Confirm Assignment to save and apply the changes.
- Step 7** Track the progress in the Template Activity window. You can access the Template Activity window in one of the following ways:
- During the export process, click View Template Activity option from the Begin Assignment window.
 - After the export process, click the History icon to track the status from the SD-WAN Template Management window.

If the export process fails, hover the mouse pointer over the failed status on the Template Activity window to view detailed information.

Deleting or Unassigning a Template Assigned to a Tenant:

You can delete or unassign one or more templates assigned to a tenant using the following Service Configuration Assignment APIs:

- GET /api/v1/serviceconfigurations/assign/all : Use this API to determine the ID for Template Name and the Tenant Name you want to unassign. From the JSON response, search for the Service Config name and assignedTenantName that match to your template name and tenant name. Get the serviceConfigId and assignedTenantId.
- DELETE /api/v1/serviceconfigurations/assign/{serviceConfigId}: Use this API to unassign tenant from service configuration. Enter the serviceConfigId and assignedTenantId that was from the payload in the previous step.

For more information on these APIs, refer the Swagger documentation that can be accessed from MSX portal > Account Settings > Swagger > Service Configuration Microservice API.

Attaching Control Plane

Use this procedure to associate an existing control plane to a tenant:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** From the left pane, click Tenant Workspace > Services.
- Step 3** From the SD-WAN service panel, click Setup to attach a control plane.
- Step 4** Click Get Started to launch the Add Control Plane wizard.
- Step 5** Click the Attach Existing Control Plane radio button to attach an existing control plane. Enter the SD-WAN Control Plane URL (Such as <https://www.example.com>), organization name, username, and password of the control plane.
- Note**
- The username field must start with only lower case alphabets and can have only lower case alphabets, numeric values from 0 to 9, "-", and space.
 - The password field supports all alphanumeric characters except space.
 - Organization name cannot contain (), <, >, {, }, [,], \
- Step 6** Click Submit to attach the control plane.
- A notification appears after the control plane is attached.

- Step 7** Click Close to view the status of the Add Control Plane wizard in the SD-WAN service panel.
- Step 8** Click Done to view the Setup Complete notification.
- Step 9** Click OK to view the status of the attached control plane and the instances in the SD-WAN service panel.

What to do next

After the sync with vManage, you can deploy a site or device for Cisco SD-WAN. For more information on deploying a device for Cisco SD-WAN, see [Deploying a Site or Device for Cisco SD-WAN](#).

Deploying a Device for Cisco SD-WAN

Deploying a device on Cisco SD-WAN is a two-step process.

Procedure

	Command or Action	Purpose
Step 1	Adding a Device (vEdge Cloud or vEdge SP Cloud).	For more information, see one of the procedures: <ul style="list-style-type: none"> • Adding a vEdge Cloud Device • Adding a vEdge SP Cloud Device
Step 2	Provisioning a Device (vEdge Cloud or vEdge SP Cloud).	For more information, see Provisioning a Device . <ul style="list-style-type: none"> • If you have multiple sites, you can use bulk import option in MSX to import their details into MSX and provision one device at a time. For more information, see Importing Multiple Site Data from Cisco SD-WAN into MSX. • If you have to provision a physical vEdges or IOS XE, see Adding a Physical Device.

Adding a vEdge Cloud Device

Before You Begin

The following is the list of prerequisites for this task:

- A tenant and a tenant user is created, see [Managing Tenants](#) and [Managing User Roles](#).
- Subscribe SD-WAN service and set up a Control Plane for the tenant. Control plane should be up and running. For more information, see [Setting Up Control Plane for Cisco SD-WAN](#).
- Under SD-WAN Service category, select SD-WAN Data Plane manage permission to allow a user to provision a device.

The service chain template is defined and is available for the tenant user, see [Managing Cisco SD-WAN vEdge Cloud TDE Templates](#).

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

Step 2 From the left hand pane, click Tenant Workspace > Services.

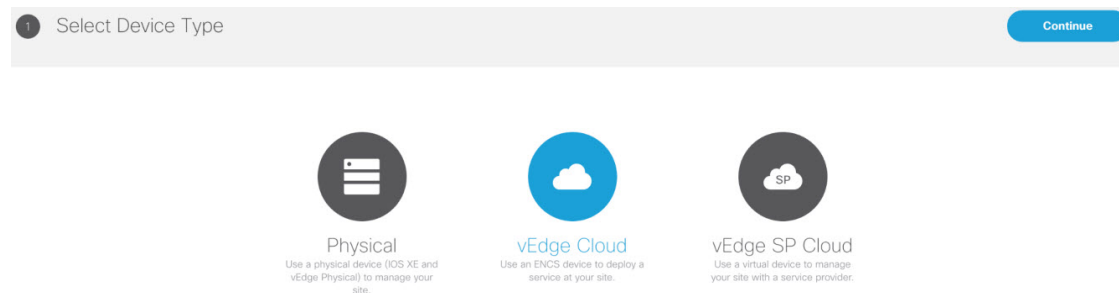
Step 3 In the SD-WAN service panel, click the + icon and click Add Device.

The SD-WAN home page appears and displays the device summary page for the selected tenant.

Step 4 Click Add Device. The figure below shows the add device information for single link and dual link cloud.

Note The Add Device button is enabled only if the control plane is provisioned for the tenant and tenant has SD-WAN Data Plane permission enabled, see [Setting Up Control Plane for Cisco SD-WAN](#).

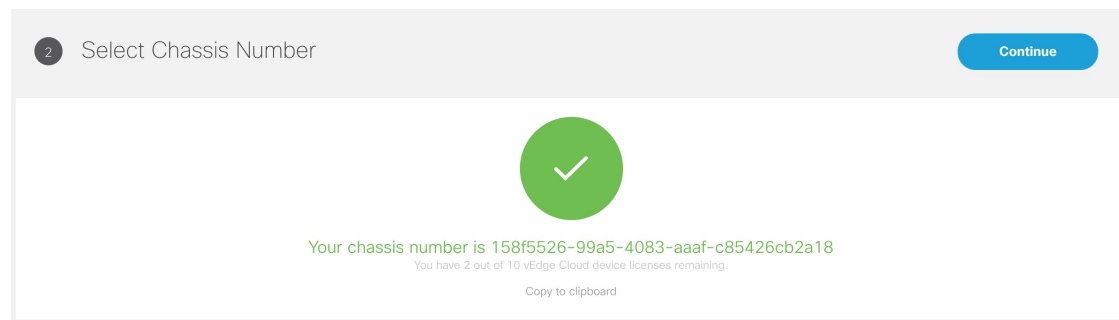
Figure 8: Selecting the Device Type



Step 5 Select vEdge Cloud to provision the vEdge cloud device.

Step 6 Click Continue. The chassis ID is pre-filled based on availability. If no chassis ID is available, then an error message is displayed.

Figure 9: Selecting the Chassis Number



Step 7 Review the vEdge device chassis ID and click Continue.

Note The chassis ID is prepopulated based on the devices allowed list that was uploaded in the control plane associated to your smart account. For more information, see [Synchronizing Smart Accounts from the Control Plane](#).

Step 8 Enter the location of the device, map coordinates, and the support details.

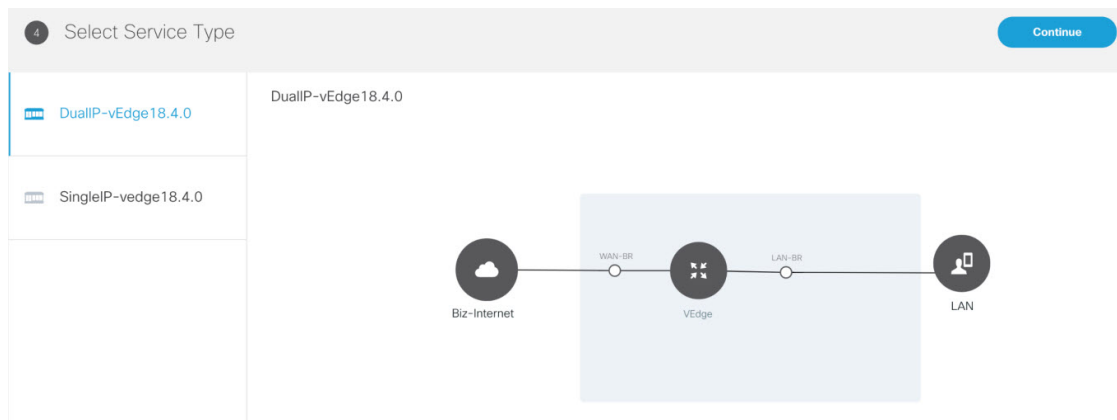
Step 9 Click Continue.

Step 10 Select a service topology. Choose single or dual link topology that you want to deploy. vEdge templates visible in this screen is assigned to a tenant through SD-Branch template setting.

- Note**
- The SingleIP template supports only singleIP onboarding, that is, only a single IP is used by ENCS for deployment.
 - The DualIP template supports dualIP onboarding, that is, two IPs are used by ENCS for deployment with or without a secure tunnel.

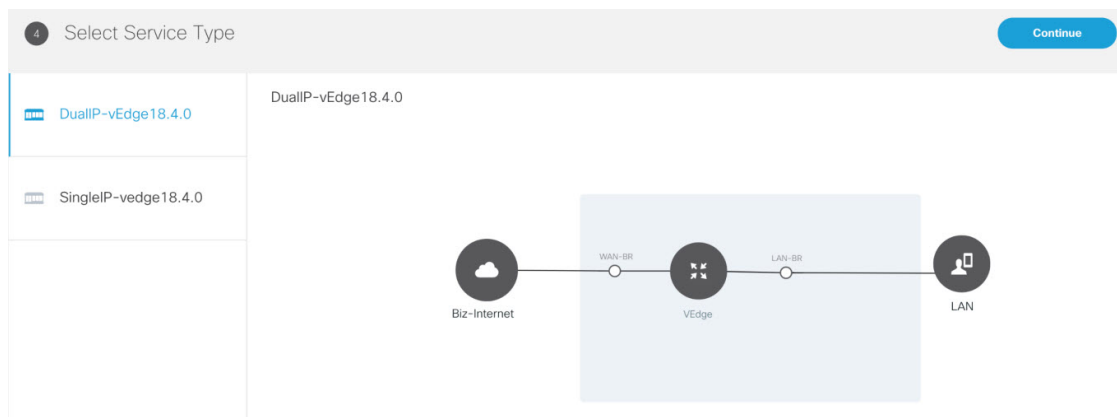
These onboarding types are described in the Step 15.

Figure 10: Selecting the Service Type



Step 11 Click Continue and enter values for the selected template.

Figure 11: Entering the Service Details



- Note** If you are using the templates from DevNet without customizations, the OTP, Organization, UUID, and VBOND fields are pre-filled for the site. If the names of TDE variables are customized, you must enter these manually.

Cisco MSX system does not validate these manually edited fields and may throw errors later during the Add device flow if the values are incorrect. To get the correct values for these fields, access the Control Plane (vManage) Configuration > Devices page > select a *free* / unassigned vEdge Cloud Device (In Token generated State) > Generate Bootstrap Configuration, and choose Cloud-init option to see the values for the four variables.

Step 12 Continue to Service Infrastructure and select the device type, and the serial number for that device type. Depending on the service topology selected for your site in Step 14, one of the following onboarding types is shown.

- **Single Public IP addresses:** Requires only one public WAN IP address that is shared between the NFVIS and VNF. This onboarding type also uses IPsec Tunnel.

Note When using single IP:

- The ENCS's public IP is moved to the vEdge's VPN0 on interface ge0/0 (biz-internet).
 - Interface ge0/2 on VPN 2 is configured for NFVIS internal management, which is used by NFVIS to transit the vEdge in order to setup the secure tunnel with Cisco MSX.
 - NAT is enabled on VPN 0 for the preceding set up to work.
- **2 Public IP addresses:** Requires two public WAN IP addresses, one IP for VNF and one for NFVIS IP. This onboarding type uses IPsec Tunnel.

Note 2 Public IP Addresses and Single Public IP onboarding types require secure tunnel between Cisco MSX and NFVIS. This tunnel is used for all communications from Cisco MSX to the site. If you are selecting these onboarding types, make sure to configure SD-Branch's IP subnet pool for ENCS NFVIS internal management. For more information, see [Configuring Subnet Pools](#). If there are issues establishing VPN tunnel, see [IPsec Tunnel Cannot be Established](#).

- **Open Network Policy:** Requires two WAN IP addresses for deployment and no IPsec Tunnel support. If the device is deployed behind NAT, the NAT device must support port forwarding. Open the ports to communicate with the Cisco MSX SD-WAN Orchestration system. For information on the Cisco SD-WAN-specific ports required for Cisco MSX SD-WAN Orchestration system, see [Cisco SD-WAN document](#).

Step 13 Click Continue.

Step 14 In the Review Device Order screen review all entries. Review and edit the entries, if necessary.

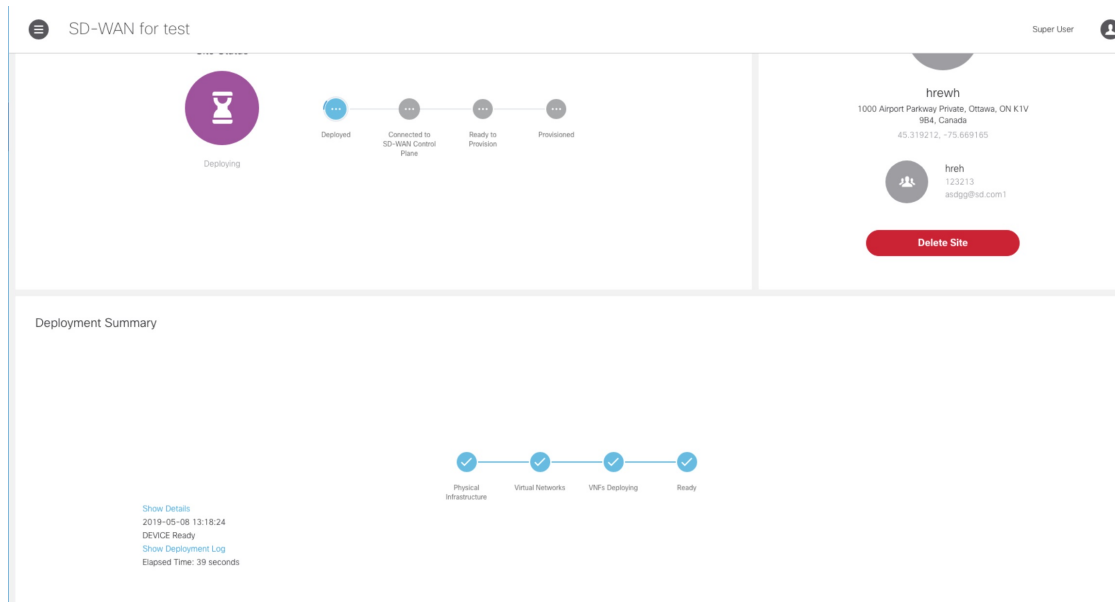
Step 15 Click Submit to display the Device and Deployment Summary on the screen. This screen shows the values that were configured for this device.

The deployment summary is displayed on the screen and disappears once the device is deployed. At this time, you will also see the device that is being deployed on the map for the location you have selected. Status of the device will change its color based on the deployment and connectivity status. To understand statuses of vEdge Cloud deployment, see [Device Statuses for vEdge Cloud](#).

Note A tenant cannot create a site using this wizard. To create a site, choose Tenant Workspace > Services/Sites/Devices, click the + icon on the top right corner and select Add Site.

To assign the device to a specific site in Cisco MSX, choose Tenant Workspace > Devices, select the device and click Assign to Site. For more information, see [Assigning a Device to a Site](#).

Figure 12: Deployment Summary



What to do next

- Connect the device and set up initial configurations. For more information, see [Setting Up Initial Configuration on the ENCS CPE \(First-Time Use Only\)](#).
- Provision a device to push the configurations to the device. For more information on attaching these templates to the device, see [Provisioning a Device](#).

Setting Up Initial Configuration on the ENCS CPE (First-Time Use Only)

After the order is placed, the SD-WAN service is set up and the ENCS is shipped to your device location by the service provider.

After the device is installed on premises, connect the device to the respective corporate LAN, the PnP management interface, and so on, depending upon the service template you had selected for the service order. The device is identified based on UDI or serial number that was provided for the service during the Add Site flow.

ENCS devices that are shipped to the customer premises have a preconfigured Day-1 configuration. When the device is powered on for the first time, the Day-1 discovery configuration wakes up in the absence of the startup configuration file and attempts to discover the address of the PnP server. The Day -1 configuration uses HTTPS (with Crypt/Cert) to connect to the PnP Server. If you are setting up the ENCS for the first time, there are a few other configuration details that need to be specified for ENCS. Specify the following additional configuration details (first time use only) on the ENCS CPE:

- PNP server IP address
- PNP server port
- Transport as HTTPS

- Upload the cacert.pem file
- DNS Server or IP address of Cisco MSX

To configure these parameters on individual CPEs:

-
- Step 1** Log in to the NFVIS portal for the CPE.
- Step 2** In the main menu, choose Host, Plug-n-Play. The Plug-n-Play screen appears.
- Step 3** Click Edit.
- Step 4** Enter the PNP server IP address.
- Step 5** Set the PNP server port to 8443.
- Step 6** Select HTTPS for the transport.
- Step 7** To upload the cacert.pem file, click the Choose File and select the file.
The certificates (ca.pem and ca-key.pem) are located at /etc/ssl/vms-certs on the Inception and kube-master nodes.
- Step 8** Click Save.
- Step 9** In the main menu, choose Host, Settings.
- Step 10** Enter or update the IP addresses of the DNS servers.
- Step 11** Click Save.
-

Adding a vEdge SP Cloud Device

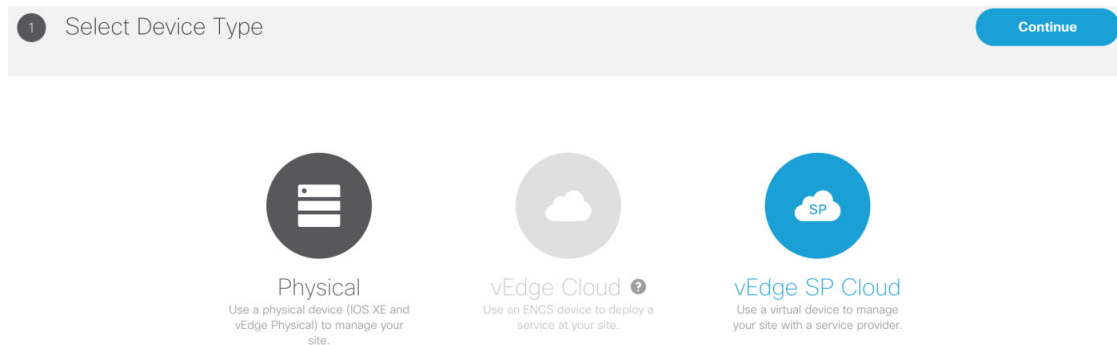
Before You Begin

The following is the list of prerequisites for this task:

- A tenant and a tenant user is created, see [Managing Tenants](#) and [Managing User Roles](#).
- Subscribe SD-WAN service and set up a Control Plane for the tenant. Control plane should be up and running. For more information, see [Setting Up Control Plane for Cisco SD-WAN](#).

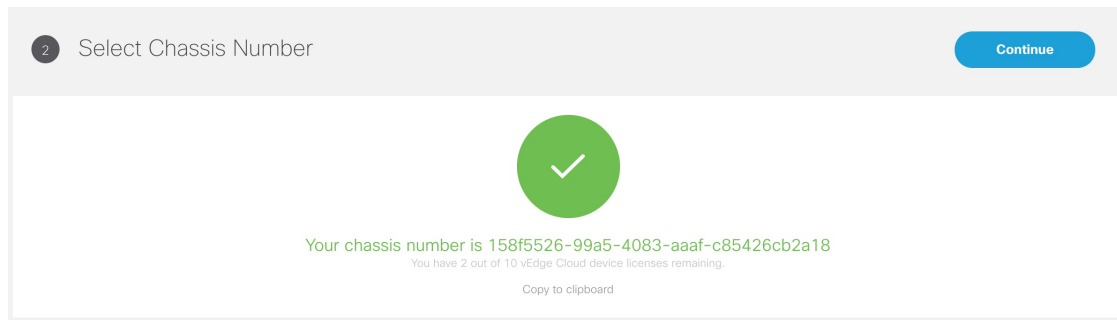
-
- Step 1** Log in to the Cisco MSX portal using your credentials.
- Step 2** From the left hand pane, click Tenant Workspace > Services.
- Step 3** In the SD-WAN service panel, click the + icon and click Add Device.
The SD-WAN home page appears and displays the device summary page for the selected tenant.
- Step 4** Click Add Device.

Note The Add Device button is enabled only if the control plane is provisioned for the tenant, see [Setting Up Control Plane for Cisco SD-WAN](#).

Figure 13: Selecting the Device Type

Step 5 Select vEdge SP Cloud to provision the vEdge cloud device on the service provider cloud. Click Continue.

Step 6 In the Select Chassis Number section, the chassis ID is pre-filled based on availability. If no chassis ID is available, then an error message is displayed.

Figure 14: Selecting the Chassis Number

Step 7 Review the vEdge device chassis ID and click Continue.


Step 8 In the Device Information section, enter the location of the device, map coordinates, and the support details. Click Continue.

Step 9 In the Service Details section, enter the information for the fields that can be modified, and click Continue. Select the single link or dual link and based on this selection you can assign static IP to Biz-Internet, VPN 512 and MPLS or go with the default which is DHCP.


Note System IP should be unique in that Control Plane which means two same system IP cannot be chosen for two different sites in the same Control Plane.

Step 10 In the Review Device Order section, review all entries.

6 Review Device Order
Submit



St. Petersburg, FL, USA
27.767601, -82.640291



+448281222606
abc@gmail.com

Configuration

TOKEN	28cfa169e7c047e6a4f8e2d1cc6047a
CHASSIS NUMBER	12c9781f-0f19-47d8-a639-e93b64b023e0
ORGANIZATION NAME	vmsoverlay1
VBOND ADDRESS	35.168.115.27
SYSTEM IP	127.0.0.1
SITE ID	1
HOSTNAME	2
BIZ-INTERNET	DHCP
VPN 512	DHCP
MPLS	DHCP

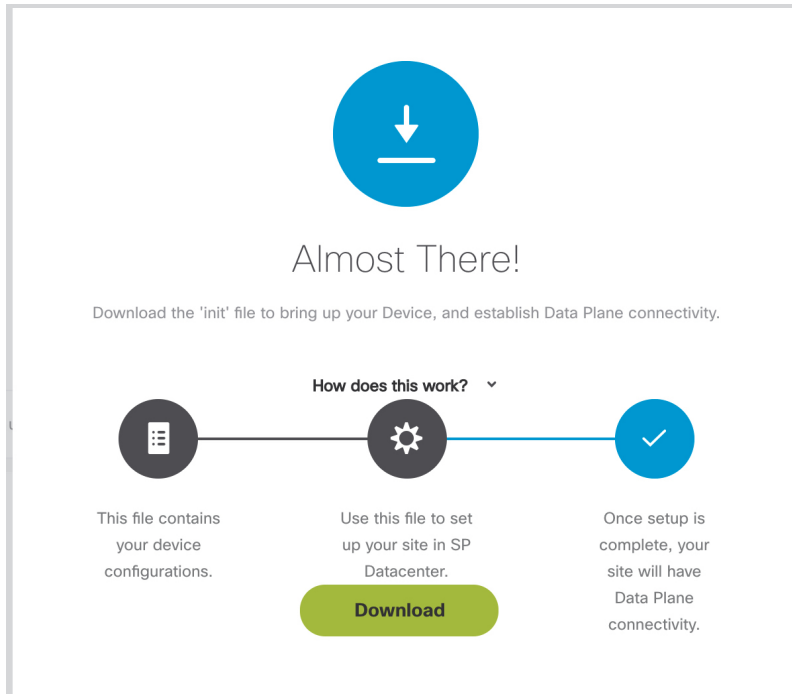
Step 11 To confirm the order, click Submit.

After you click Submit, you will get a pop-up to download the SP Cloud file that is used for the private cloud and can be used to deploy a site.

Step 12 Click Download to download your device config file.

The customer device details are saved in Cisco MSX and the vEdge SP cloud customer device configuration file download option appears. When you download the file, by default this file will be placed in the 'Download' folder. Deploy these configuration files on the vEdge. Ensure you have the vEdge image available on the Service Provider cloud infrastructure. Download the vEdge latest image and vEdge templates [here](#).

Figure 15: Downloading the Device Config File



Note A tenant cannot create a site using this wizard. To create a site, choose Tenant Workspace > Services/Sites/Devices, click the + icon on the top right corner and select Add Site.

To assign the device to a specific site in Cisco MSX, choose Tenant Workspace > Devices, select the device and click Assign to Site. For more information, see [Assigning a Device to a Site](#).

After the configuration is deployed and the vEdge is able to connect to SD-WAN Control Plane, you can view the provisioning statuses for vEdge SP Cloud. For more information see [Device Statuses for vEdge SP Cloud and External Sites](#).

What to do next

- Provision a device to push the configurations to the device. For more information on attaching these templates to the device, see [Provisioning a Device](#).

Adding a Physical Device

Use this procedure to add a physical device (vEdges and IOS XE) for your SD-WAN network. Cisco MSX collects the details required to provision this device. Once the data is submitted, the details are sent to vManage, and the specific device is provisioned.



Note If a physical device was added from the Control Plane web interface (vManage dashboard), the Cisco MSX portal lists this device with the status as ‘UP’ on the device summary page for the tenant. MSX portal will also reflect the device templates changes that were applied or removed from the Control Plane web interface.

Before You Begin

Assign the following permissions to a user who can add physical device and provision the device:

- Under Bulk Import Sites/Devices/Tenants/Users category, select Bulk Import (Manage) permission.
- Under SD-WAN Service category, select SD-WAN Data Plane manage permission to allow a user to provision a device.

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

Step 2 From the left hand pane, click Tenant Workspace > Services.

Step 3 In the SD-WAN service panel, click the + icon and click Add Device.

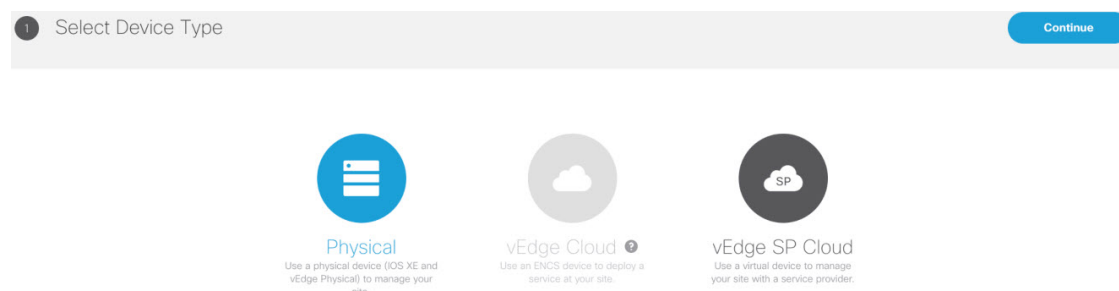
The SD-WAN home page appears and displays the device summary page for the selected tenant.

Step 4 Click Add Device to add a new vEdge or an IOS XE device.

Note The Add Device button is enabled only if the control plane is provisioned for the tenant, see [Setting Up Control Plane for Cisco SD-WAN](#).

Step 5 Select Physical to provision vEdge or IOX XE device. Click Continue.

Figure 16: Selecting the Device Type



Step 6 Select a device type and provide the serial number for that device type.

Step 7 Enter the location of the device, map coordinates, and the support details.

Step 8 Select a device template to be used for provisioning the device and click Continue. The templates are listed based on the selected device type in the previous step.

Step 9 Enter the device details, such as ID, Chassis Number, System IP, and so on. Only ‘Required’ fields are populated in this form. Click Submit to initiate the provisioning process and push the configuration data into the Control Plane. During this time, Cisco MSX validates if the device details match with the information on the Control Plane. If the device data on Cisco MSX is same as the data on the Control Plane, the provisioning process proceeds, and device status changes to ‘Provisioning’. During this process, if there are any errors, device status changes to ‘Provisioning Failed’.

Note While getting chassis ID for a specific device using the data-plane-controller APIs, Cisco MSX translates the forward slash in the chassis ID as %2F to avoid bad API request. For more information on the SD-WAN Service API, refer to the Swagger documentation that can be accessed from Cisco MSX portal > Account Settings > Developer Settings > API Documentation > Swagger UI > SD-WAN Microservice API.

Step 10 Edit and update the device details on the Cisco MSX. Under the Provisioning Details section, if the device details are incomplete or incorrect, you can click Edit Details to edit the device details and click Provision Device to push the updated configurations to the device.

Note A tenant cannot create a site using this wizard. To create a site, choose Tenant Workspace > Services/Sites/Devices, click the + icon on the top right corner and select Add Site.

To assign the device to a specific site in Cisco MSX, choose Tenant Workspace > Devices, select the device and click Assign to Site. For more information, see [Assigning a Device to a Site](#).

To view provisioning statuses, see [Monitoring Cisco SD-WAN Device Status](#).

Assigning a Device to a Site

A tenant can assign one or more devices to a site. Use this procedure to assign a device to a site.

Before you begin

1. Create or attach a Cisco SD-WAN control plane. For more information, see [Setting Up Control Plane for Cisco SD-WAN](#).

Step 1 Log in to the Cisco MSX portal.

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

Step 3 Select a device, click on the ellipsis (...) and click Assign to Site.

The Assign Device to Site wizard appears.

Step 4 Click Get Started to launch the wizard.

Step 5 In the Select Site section:

Click the Assign to Existing Site radio button to assign the device to an existing site. Enter the site name.

Or

Click the Create New Site radio button to add a new site. Enter the site name, site address, supplemental location, and description of the site. Check the Add Site Contact check box to provide the contact details.

Step 6 Click >. A notification appears after the device is assigned to the new site.

Step 7 Click View Site to view the status of the site.

Importing Multiple Site Data from Cisco SD-WAN into MSX

Cisco MSX allows you to import details of multiple sites from Cisco SD-WAN and provision one site at a time on Cisco SD-WAN. After performing bulk import, you can validate the data imported for each site, view each site, and provision one site at a time from the Cisco MSX Portal.

You can provision the following types of devices after importing data from multiple sites:

- Physical (vEdge, IOS XE)
- vEdge Cloud
- vEdge SP Cloud
- Any site that was added outside of SD-WAN

Sites that were added outside of SD-WAN are displayed as External Sites in the map or the list view on the SD-WAN home page in the Cisco MSX portal. Like any other sites, Cisco MSX also lists site details for the external sites, such as Site ID, System IP, statuses, and so on in the List view.

Before You Begin

1. Subscribe to SD-WAN service and set up a Control Plane. Control plane must be up and running. For more information, see [Setting Up Control Plane for Cisco SD-WAN](#).
2. Assign the following permissions to a user who can download the site template file and perform a bulk import of the site details into Cisco MSX:
 - Under SD-WAN Service category, select SD-WAN Bulk Site (View) permission to allow a user to download the template to their local machine and to view the template.
 - Under Bulk Import Sites/Devices/Tenants/Users category, select Bulk Import (Manage) permission to allow a user to import the data into Cisco MSX.
 - Under SD-WAN Service category, select SD-WAN Data Plane (Manage) permission to allow a user to provision a site.
3. Perform the following tasks on SD-WAN Control Plane (vManage):
 - Add devices to Smart/Virtual Account. Once the Control Plane instances are created, synchronize with Smart Accounts from the SD-WAN Control Plane Portal to download the device list information for device onboarding. For more information on how to upload device allowed list manually or synchronizing device information using smart account, see [Synchronizing Smart Accounts from the Control Plane](#).
 - Create Device Templates on SD-WAN Control Plane based on your tenant deployment. For more information on creating these templates on the Control Plane, see Cisco SD-WAN documentation.
4. Deploy a customer site on Cisco MSX. For more information, see [Deploying a Site or Device for Cisco SD-WAN](#).
5. Depending on whether you are provisioning physical or vEdge Cloud devices, make sure that these devices are ordered and shipped to the tenant locations. At this point, devices may not be operational since they do not have configurations to define their role. These devices appear as 'Unknown' on the map or the list view on the SD-WAN Service screen.

Physical devices do not have any address configured for the sites to plot them on the map, so these devices appear as 'Unmapped Sites' on the map or the list view.

Step 1 Download a Site Template File.

Using a site template file, you can enter data such as device information, site details, for multiple sites and import these details into Cisco MSX. The template file pulls active device templates available on the SD-WAN Control Plane. For each device model, the templates shows you the fields that are mandatory to provision this device on the SD-WAN Control Plane. To download a site template:

- Log in to the Cisco MSX portal using your credentials.
- From the left pane, choose Tenant Workspace > Service Controls.
- Click the Bulk Import tile, then click Generate Site Template File option to download the Site template file.

Note The downloaded Site Template file includes previously provisioned sites and their details. You can update this file any number of times, if required.

Note Cisco MSX supports CSV and JSON file format for the site templates. JSON has information in the form of tool-tips, which show details such as, data type, allowed values for each field, and other useful metadata. You can download and import the JSON file only using the API. To get site template data in JSON format, use the data plane endpoint in the bulk-site-controller section of the SD-WAN Service API. For more information on the SD-WAN Service API, refer to the Swagger documentation that can be accessed from Cisco MSX portal > Account Settings > Developer Settings > API Documentation > Swagger UI > SD-WAN Microservice API.

Step 2 Prepare the Site Template file.

Before editing the Template file:

- Determine the sites for which you want to import the details for provisioning.
- For each site, identify the template that should be applied.

Step 3 Edit the downloaded Template file only after associating the sites with the device template. Enter the values in all the appropriate fields that are marked as required (R).

Note While entering data in this Template file you can use quotes, spaces, commas, and special characters.

A sample of a downloaded Site Template table is given here:

Figure 17: Site Template Table

Device Model	Chassis Number	Site ID	System IP	Host name	Site Name	Device Template Name					Prefix (vpn_ipv6_ipv6_prefix)	Address (vpn_next_hop_ipv6_address_0)	Distance (vpn_next_hop_ipv6_distance_0)
vedge-100-B	R	R	R	R	R	mttest			
vedge-cloud	R	R	R	R	R	Xin-Template1			
vedge-100-M	R	R	R	R	R	demo_device_template	O	O[Prefix(vpn_ipv6_ipv6_prefix)]	O[Prefix(vpn_ipv6_ipv6_prefix)]	
vedge-100-M	R	R	R	R	R	ott-physical-vedge-07-Test-Template			
vedge-100-B	R	R	R	R	R	ott-physical-vedge-05-Base-Template			
vedge-100-M	R	R	R	R	R	Bulk_Site_Test_Profile2			
vedge-100-M	R	R	R	R	R	test_device_template	R	R	R	R

Legend

- R: Required field
- O: Optional field
- Blank Field: Not Applicable

From the above table, the `demo_device_template` (Device Template) are marked as optional (O). It has both primary optional and related optional fields.

- Prefix (`vpn_ipv6_ipv6_prefix`): Primary optional field
- Address (`vpn_next_hop_ipv6_address_0`): Related optional field
- Distance (`vpn_next_hop_ipv6_distance_0`): Related optional field

The downloaded Template file may have both primary and related fields, that are marked as optional (O). There can be more than one primary optional fields (for example, primary optional 1, primary optional 2).

- In the case of `demo_device_template`, if you enter data in the primary optional field, then you must also enter data in the related optional fields. If you do not enter any data in primary optional field, then it is not required to enter data in related optional field.
- In the case of `test_device_template`, all the fields are marked as required (R). Enter data in all the fields.

When you upload the Template file, it undergoes process validation. The related optional field variables are validated only when the primary optional field data is entered.

If the Template file is uploaded without any modifications, then the site status remains unchanged and retain its previous status.

Step 4 To import provisioning details for multiple sites:

- a. On the left pane, choose Tenant Workspace > Service Controls.
- b. Click the Bulk Import tile, then click Import Sites to import the site template that was edited in Step 3. Edit the downloaded Template file only after associating the sites with the device template. Enter the values in all the appropriate fields that are marked as required (R).
- c. If the data filled in the Template file is correct, then site details are imported to Cisco MSX and the site is now ready for provisioning.

If the data filled was incorrect or incomplete, sites cannot be provisioned until the details are corrected, and the Template file is imported again in Cisco MSX. During this period, Cisco MSX displays various validation messages to validate the accuracy of the imported data.

You can see the status of devices in Tenant Workspace > Devices. Select the device from device list for which you need to edit or update information. Click Device Details.

- Click Edit Details in the Provisioning Details page to edit directly from the portal instead of importing a new CSV file again.
- You can also edit the device template. Select the desired device template from the drop down, variable values of the previous device templates are automatically populated. Click the Save button to save the latest template changes. You can edit it any number of times, whenever required.

The figure below shows one of the validation scenario, where the errors are recorded on the Site Details window for a tenant.

Note We recommend that you download the error list as the information on this screen is temporary and disappears after you exit this page

Figure 18: Validation Message

Import Summary for Tenant

csv-template-10102018.csv file

Details

- ✓ 43 out of 47 sites data has been successfully added.
- ✗ 4 out of 47 sites have errors. Please correct your CSV file, then upload again.
You can also [download the list](#).
- ⚠ 2 out of 47 sites have warnings. Please review them below.

<p>SJC_Ops</p> <p>Site ID: 356</p> <p>Row #: 27</p>	<div style="border: 1px solid #ccc; padding: 5px;"> <p>✗ Errors</p> <hr/> <p>Missing value for Address(vpn0_next_hop_ip_address_0)</p> <hr/> <p>Incorrect value for Area Number (vpn0_ospf_internetworking_area)</p> <hr/> <p>Missing value for Bandwidth Upstream(vpn0_private1_if_bandwidth_upstream)</p> </div>
---	--

What to do Next?

After importing multiple site data, you can now provision a site to configure the device. For more information on attaching these templates to the device, see [Provisioning a Device](#).

Check the Status of Various SD-WAN Components

To check on various SD-WAN components, use the GET APIs to query the SD-WAN database. For more information on the SD-WAN services APIs, refer to the Swagger documentation that can be accessed from MSX portal > Account Settings > Developer Settings > API Documentation > Swagger UI > SD-WAN Microservice API.



Note You should have SD-WAN maintenance authorization to access these APIs.

The figure below shows the list of Get APIs that can be used to query the database.

Figure 19: List of Get API for Querying the Database

maintenance-controller : Maintenance Controller		Show/Hide	List Operations	Expand Operations
GET	/v1/maintenance/accounts			Get all existing accounts data from Orchestrator
GET	/v1/maintenance/accounts/{id}			Get specific account data from Orchestrator
GET	/v1/maintenance/corpnetworks			Get all existing corp network data from Orchestrator
GET	/v1/maintenance/corpnetworks/{id}			Get specific corp network data from Orchestrator
GET	/v1/maintenance/customer/{id}/overlay			Get customer overlays data from Orchestrator
GET	/v1/maintenance/customers			Get all existing customers data from Orchestrator
GET	/v1/maintenance/customers/{id}			Get specific customer data from Orchestrator
GET	/v1/maintenance/devices			Get specific device data from vManage
GET	/v1/maintenance/orchsettings/record			Get orchestration settings
GET	/v1/maintenance/orgsettings			Get organization settings from vManage
GET	/v1/maintenance/overlay/instance/record			Get all existing tenant overlay instances record data from VMS system
GET	/v1/maintenance/overlay/record			Get all existing tenant overlays record data from VMS system
GET	/v1/maintenance/overlays			Get all existing overlays data from Orchestrator
GET	/v1/maintenance/overlays/instance			Get all existing overlays instances data from Orchestrator
GET	/v1/maintenance/overlays/{id}			Get specific overlay data from Orchestrator
GET	/v1/maintenance/overlays/{id}/instance			Get specific overlay instances data from Orchestrator
GET	/v1/maintenance/sites			Get sites data from vManage
GET	/v1/maintenance/sites/record			Get sites record from VMS, SDWAN DB

The figure below shows a sample query to access the list of accounts from vOrchestrator using the GET APIs.

Figure 20: Accessing the List of Accounts from vOrchestrator

The screenshot displays a REST client interface with the following details:

- Request URL:** `curl -X GET --header 'Accept: application/json' :9111/sdwan/v1/maintenance/accounts'`
- Request Headers:** `{ "Accept": "application/json" }`
- Response Body:**

```
{
  "success": true,
  "responseObject": {
    "count": 35,
    "next": null,
    "previous": null,
    "results": [
      {
        "a_pk": 130,
        "a_id": "benAcct1",
        "a_name": "benAcct1"
      },
      {
        "a_pk": 131,
        "a_id": "christyAcct1",
        "a_name": "christyAcct1"
      }
    ]
  }
}
```
- API Root / Account List:** GET /api/v1/accounts/
- HTTP 200 OK:** Allow: GET, POST; Content-Type: application/json; Vary: Accept
- Response Body (JSON):**

```
{
  "count": 35,
  "next": null,
  "previous": null,
  "results": [
    {
      "a_pk": 130,
      "a_id": "benAcct1",
      "a_name": "benAcct1"
    },
    {
      "a_pk": 131,
      "a_id": "christyAcct1",
      "a_name": "christyAcct1"
    },
    {
      "a_pk": 86,
      "a_id": "123456789",
      "a_name": "customer1"
    }
  ]
}
```

Annotations in the image include "VMS SDWAN GET APIs" pointing to the request details and "Details from vOrchestrator" pointing to the response body.

Provisioning a Device

Do one of the following:

- Bulk import device details that are required for provisioning. For more information, see [Importing Multiple Site Data from Cisco SD-WAN into MSX](#).
- Collect the device details for individual devices using the Add Device procedure. For more information, see [Deploying a Site or Device for Cisco SD-WAN](#).

Use the provisioning process to push the data on the device into the Control Plane. This process sets the device for day one configurations. To provision a device:

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

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

The Devices window is displayed with the list of devices associated to the tenant.

Step 3 From the list of devices, select the device that is ready to be provisioned.

Step 4 Click Device Details.

The Device Summary page is displayed. You will see Device Template and Provisioning Details section in the Device Summary page.

Step 5 Click Provision Device under the Provisioning Details section to initiate the provisioning process.

The provisioning process on the Control Plane takes approximately 5 to 10 minutes. During this time, Cisco MSX displays various validation messages to validate if the device template variables match with the information on the Control Plane. Depending on the device synchronization status and the validity of template variables passed by the user, site status changes to 'Provisioned' to 'Provisioning Failed'.

- Provisioning: If the device template variables imported in Cisco MSX are same as the variables on the Control Plane, the provisioning process proceeds, and site status changes to 'Provisioning.'
- Provisioning Failed: If there are any errors, site status changes to 'Provisioning Failed', and Cisco MSX system records these errors on the Cisco MSX Portal or in the Event Log.
- Provisioned: If there are no errors, and device remain in Sync after changes are applied, site status changes to 'Provisioned'.

You can also edit a provisioned site using Edit Details options. Click the Provision Device to deploy the template values to device. Enter values in all the fields, if values are not entered then it displays an error or warning message, it indicates status as 'Incomplete'.

Configuring Traffic Policies

Cisco SD-WAN traffic policies dynamically control data packet forwarding decisions by looking at the applications type, tunnel performance, available paths status and forwarding rules. These policies monitor the

network performance—jitter, packet loss, and delay—and forward critical applications over the best-performing path.

The traffic policies when applied uses vManage centralized policies capability that applies the rules to all available vSmart controllers, and the vSmart controller automatically pushes it to the available vEdge or cEdge (IOS-XE) routers. Because of these centralized policies, the traffic policy changes that you perform on Cisco MSX are automatically pushed to vManage, and changes directly done on vManage for the policies supported by Cisco MSX will be visible in Cisco MSX.

- Configure Path Preference settings. For more information, see [Configuring Path Preference Settings](#).
- Configure Application Relevance settings. For more information, see [Configuring Application Relevance Settings](#).

Before You Begin

- Create or attach Control Plane, see [Setting Up Control Plane for Cisco SD-WAN](#).
- Ensure you have the following permissions to configure traffic policies:
 - SD-WAN Traffic Policy: Users with manage permission can add and modify Application Relevance policy or Path Preference policy to the SD-WAN fabric.
 - View Event Log: Users with this permission can view the status of the policies in the event log.

For information on how to associate these permissions to a role, see [Managing Roles in Cisco MSX](#).

- Ensure vSmart controller is up and running. If a vSmart controller is down the policy changes are not applied.

Configuring Path Preference Settings

Traffic transport path settings forward applications over the best-performing path based on the defined application policy. These settings help to load-balance the traffic efficiently by using the available bandwidth.

Use the procedure described in this section to customize the data traffic to the specific transport preference for each of the traffic classes. (Traffic classes are categories of traffic [packets] that are grouped on the basis of similarity). The following are the categories of traffic classes available in Cisco MSX:

- Voice class refers to VoIP bearer traffic only.
- Network Control Management class is intended for network management protocols, such as SNMP, syslog, domain name system, and IP routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and so on.
- Interactive video refers to IP video conferencing.
- Streaming video is either unicast or multicast unidirectional video.
- Call Signaling class is intended for voice and video signaling traffic, such as Skinny Client Control Protocol (SCCP), SIP, H.323, and so on.
- Bulk data class is intended for background and foreground operations, such as large file transfers, database synchronization, email, database access, and interactive messaging.

- Scavenger class defines a less-than-best effort service. In the event of link congestion, this class is dropped most aggressively.
- Default class is also the best-effort class. Unless an application has been assigned for preferential or deferential service, it will remain in this default class.
- Unmatched Traffic category applies to applications that do not match other specified categories.

Perform this procedure to configure path preference settings:

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

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

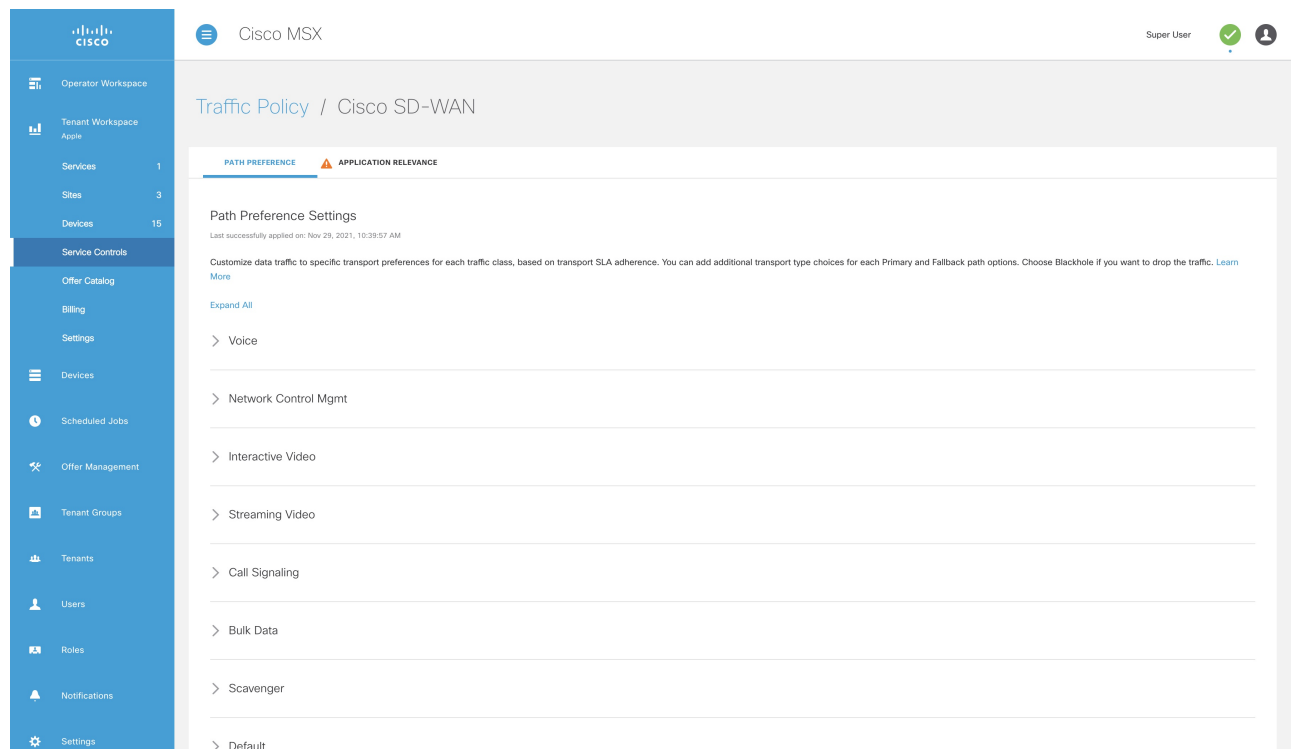
The Service Controls page with the relevant controls for the subscribed services is displayed.

Step 3 Select the Traffic Policy tile to configure the path preference settings.

Note The traffic policy can be configured only when the control plane has been created or attached for the tenants.

Step 4 Click the Path Preference tab, and expand each of the traffic class.

Figure 21: Configuring Path Preference



Step 5 Select the primary and the fallback routing path for a selected traffic class.

Step 6 Review or modify the routing policy path, and fallback preference. Choose Blackhole, if you do not want to set up a backup path.

Step 7 Click Apply.

The policy takes approximately about 3 to 4 minutes to apply. To see the status of the applied policy, see the event logs.

If the settings fail to apply, click Retry to try again with the same setting or click Cancel to use the previous settings.

What to do next

Configure Application Relevance settings. For more information, see [Configuring Application Relevance Settings](#).

Configuring Application Relevance Settings

An application-aware routing policy matches applications with the data plane tunnel performance characteristics that are necessary to transmit the applications data traffic. The primary purpose of application-aware routing policy is to optimize the path for data traffic. Using this policy, network architects can clearly identify which applications are relevant to their business and which are not.



Note You can configure the Application Relevance settings only if the Cisco SD-WAN version is 18.2 or later.

To configure Application Relevance Settings:

- Step 1** Log in to the Cisco MSX portal using your credentials.
- Step 2** From the left pane, choose Tenant Workspace > Service Controls.
The Service Controls page with the relevant controls for the subscribed services is displayed.
- Step 3** Select the Traffic Policy tile to configure the path preference settings.
Note The traffic policy can be configured only when the control plane has been created or attached for the tenants.
- Step 4** Click the Application Relevance tab to apply the business relevance for the listed applications.
Note The first time you set up applications, you cannot edit the relevance as, by default, the relevance is applied. Only after the default is saved, you can edit the existing relevance.
- Step 5** Filter from the available applications using the search bar available on the right side of the web interface. For information on the out-of-box applications available with Cisco MSX, see [Applications Available with Cisco MSX SD-WAN](#).
- Step 6** Select the Application type and edit the business relevance of the selected application by selecting the relevance from the drop-down list. The Cisco MSX web interface shows the relevance of the selected application type in the Traffic Class column. Business relevance can have one of the following settings:
- **Business Relevant:** These applications are known to contribute to business objectives of the organization and may include voice, multimedia applications, collaborative applications, database applications, email applications, file/content transfer applications, backup applications, and so on., as well as control plane, signaling, and network management protocols.
 - **Business Irrelevant:** These applications do not support business objectives and are typically consumer-oriented. These applications are known to have no contribution to business-objectives and are often personal or entertainment-oriented in nature. Such applications may include video-on-demand (for example, Netflix, YouTube, and so on), gaming traffic, peer-to-peer file-sharing applications, and other applications.

- **Default:** These applications may or may not contribute to business objectives. For example, HTTP/HTTPS at times may be used for work or for personal reasons. As such, it may not always be possible to assign a static business-relevant designation to such applications. Such applications should be marked as default.

Figure 22: Configuring Application Relevance

Path Preference **Application Relevance**

Application Relevance Settings

Last successfully applied on: May 5, 2019, 10:10:32 PM

These settings control how traffic is prioritized for your applications. You can change the relevance of one or more applications at any given time. Traffic Class indicates the resulting application category based on the relevance selected. [Learn More](#)

Application	Relevance	Traffic Class
4CHAN	Business Irrelevant ▼	Scavenger
ABCNews	Business Irrelevant ▼	Scavenger
AccuWeather	Business Irrelevant ▼	Scavenger
Active Networks	Default ▼	Default
AddThis	Business Irrelevant ▼	Scavenger
Adobe Connect	Business Relevant ▼	Interactive Video
AIM Transfer	Business Irrelevant ▼	Scavenger
Amazon	Business Irrelevant ▼	Scavenger
Ameba.jp	Business Irrelevant ▼	Scavenger
AnalogBit tcp-over-dns	Business Irrelevant ▼	Scavenger
AOL Messenger	Business Irrelevant ▼	Scavenger
Apple AirPlay	Business Irrelevant ▼	Scavenger

Cancel Apply

Step 7 Review or modify the Application relevance settings and click Apply.

A Turquoise mark beside an application indicates that the application relevance is being applied and new settings cannot be applied until the current process is completed.

Important Notes:

- If application policy is changed on vManage by moving applications from one category to other that does not match the SD-WAN Application Relevance and Traffic Class rules, then it leads to Application Mismatch. If the settings fail to apply, click Retry to try again with the same setting or click Cancel to use the previous settings.
- MSX 4.2 supports additional applications compared to MSX 4.1. Hence, if you upgrade from 4.1, there will be an application mismatch between Cisco MSX and Cisco SD-WAN. In this case, we recommend that you synchronize these applications on Cisco SD-WAN by using the Apply MSX Settings option on the Mismatched Applications window.


What to Do Next

Monitor the traffic path and the application queues. For more information, see [Monitoring the Traffic Policy](#).

Deactivate a Traffic Policy

An operator can deactivate a traffic policy only from Cisco SD-WAN control plane (vManage).

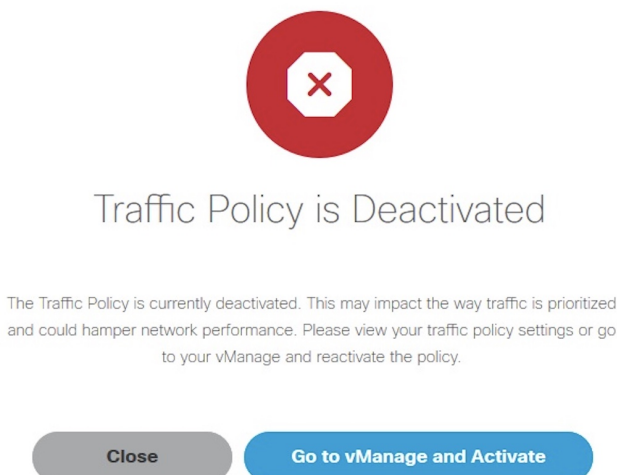
To deactivate the traffic policy:

-
- Step 1** Log in to SD-WAN Control Plane.
 - Step 2** In the main menu, click Configurations > Policies.
 - Step 3** Select the policy that you want to deactivate, click the  icon
 - Step 4** Choose Deactivate. Status of the deactivated policy will be indicated.

The SD-WAN provides information to the Cisco MSX users about the policy deactivation in the form of error messages. If the policies are deactivated on vManage, you cannot configure traffic policy from the Cisco MSX portal. You must first activate the centralized policy on the vManage to configure traffic policy from the Cisco MSX portal.

The following is an error message that is displayed on the Cisco MSX portal for the deactivated policy.

Figure 23: Deactivating the Traffic Policy



Maintaining Cisco SD-WAN Deployments

This section covers the maintenance tasks for Cisco SD-WAN services.

Editing an SD-WAN Control Plane

To edit a control plane:

Step 1 Log in to the Cisco MSX Portal.

Step 2 From the left pane, click Tenant Workspace > Services.

Step 3 In the SD-WAN service panel, click on the ellipsis (...) and click Edit Control Plane.

Step 4 Edit the control plane information that you had provided earlier for the selected site.

You can edit the details of the SD-WAN Control Plane, such as URL, organization name, username, and password of the control plane.

- Note**
- Username field must start with only lower case alphabets and can have only lower case alphabets, numeric values from 0 to 9, "-", and space.
 - Password field supports all alphanumeric characters except space. Use the eye icon to view the existing password. You can enter the new password in this field to override the existing password. Only users with permissions to create, attach, delete, or detach a control plane (that is, SD-WAN Control Plane manage permission) can view or override the existing password.
 - Organization name cannot contain (), <, >, ?, {, }, [,], \, "

Editing a Provisioned Device

Use the procedure below to modify the device details after the device is provisioned and has established a connection with the MSX control plane.

To edit a provisioned device in Cisco SD-WAN:

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

Step 2 From the left hand pane, click Tenant Workspace > Devices.

Step 3 Select a device and click Device Details.

In the Device Template section, click Edit Details to update the configuration details. Click Save. Alternatively, you can also reimport the site template CSV or JSON file with the updated values. For more information on how to import the site template file, see [Importing Multiple Site Data from Cisco SD-WAN into MSX](#).

Step 4 After you update the device, the Provision Device button is enabled. Click Provision Device to provision the device.

The provisioning process on the Control Plane takes approximately 5 to 10 minutes. During this time, Cisco MSX displays various validation messages to validate if the device template variables match with the information on the Control Plane. Depending on the device synchronization status and the validity of template variables passed by the user, device status changes to 'Provisioned' to 'Provisioned Failed'.

For more details on these statuses and the next steps, see [Monitoring Cisco SD-WAN Device Status](#).

Upgrading Control and Data Plane

You can upgrade the software image running on both Control and Data Plane. The upgrade process comprises of uploading the new software image, upgrading the device software, and activating the software image.



Note It is recommended that all devices run the same software version. If this is not possible, you must ensure that the SD-WAN Control Plane server (vManage) software version is higher version than that of vSmart, vBond controller and vEdges.

Uploading Software Images

Before you can upgrade any device to a new software version, you need to either upload the software image to the SD-WAN Control Plane (vManage) server or point to a remote server on which the software image is available.

To upload the software image:

-
- Step 1** Log in to the SD-WAN Control Plane (vManage). For more information, see [Logging in to the Cisco SD-WAN Control Plane](#).
 - Step 2** In the Control Plane, select the Maintenance > Software Upgrade. The Maintenance | Software Upgrade screen appears.
 - Step 3** Click the Device List button that is located on the right side of the title bar and select Repository. The Software Repository screen appears.
 - Step 4** Click Add New Software.
 - Step 5** Select the location from which to download the software images.
 - Step 6** If you select vManage, the Upload Software to vManage dialog box appears.
 - a. Click Choose Files to select software images for the device.
 - b. Click Upload to upload the images to the repository. The software image is displayed in the Repository table and is available for installing on the devices.
 - Step 7** If you select Remote Server, the Location of Software on Remote Server dialog box opens.
 - a. Enter the version number of the software image.
 - b. Enter the URL of the FTP or HTTP server on which the software images reside.
 - c. Click Add to add the images to the repository. The software image is displayed in the Repository table and is available for installing on the devices
-

Upgrading vEdge Devices

To upgrade the software image on a device:

-
- Step 1** Log on to vManage.

- Step 2** In vManage, select the Maintenance > Software Upgrade. The Maintenance | Software Upgrade screen appears.
- Step 3** In the title bar, click the vEdge tab.
- Step 4** Verify that the device that needs to be upgraded is reachable.
- Step 5** Select one or more devices on which to upgrade the software image.
- Step 6** Click the Upgrade button. The Software Upgrade dialog box opens.
- Step 7** Select the software version to install on the device. If the software is located on a Remote Server, select the VPN in which the software image is located.
- Step 8** To automatically activate the new software version and reboot the device, select the Activate and Reboot check box.
- Step 9** Click Upgrade. A progress bar indicates the status of the software upgrade.
- If the control connection to the SD-WAN Control Plane does not come up within the configured time limit, SD-WAN Control Plane automatically reverts the device to the previously running software image.

Activating New Software Image on vEdge Devices

If you did not select the Activate and boot check box when upgrading the software image, the device continues to use the existing configuration.

To activate new software image on vEdge devices:

-
- Step 1** Log on to vManage.
- Step 2** In vManage, select the Maintenance > Software Upgrade. The Maintenance | Software Upgrade screen appears.
- Step 3** In the title bar, click the WAN Edge tab.
- Step 4** Select one or more devices on which to activate the new software image.
- Step 5** Click the Activate button. The Activate Software dialog box opens.
- Step 6** Select the software version to activate on the device.
- Step 7** Click the Activate button. The SD-WAN Control Plane reboots the device and activates the new software image.
- If the control connection to the SD-WAN Control Plane does not come up within the configured time limit, SD-WAN Control Plane automatically reverts the device to the previously running software image.

Deleting a Device

The procedure for deleting vEdge Cloud and vEdge SP Cloud is the same. However, deleting a vEdge cloud device is a slower process than deleting a vEdge SP Cloud device, and takes around 5-10 minutes.

Deleting a vEdge cloud device is a three-step process:

- First, the vEdge device is decommissioned—the configuration on the device is removed, certificates are cleared, and the chassis ID is made available again in SD-WAN Control Plane. At this point, the reachability status will be in Red and overall site status will be Gray.
- Second, the delete process then undeploy the vEdge device from the ENCS device.
- Final step is the SD-WAN database clean-up after which device can no longer be viewed on the map.



Note Only users with the permission 'SD-WAN Data Plane' can delete sites. For more information, see [Managing Roles in Cisco MSX](#).

Deleting a vEdge SP Cloud is a faster process as this process instantly clears up the SD-WAN database.

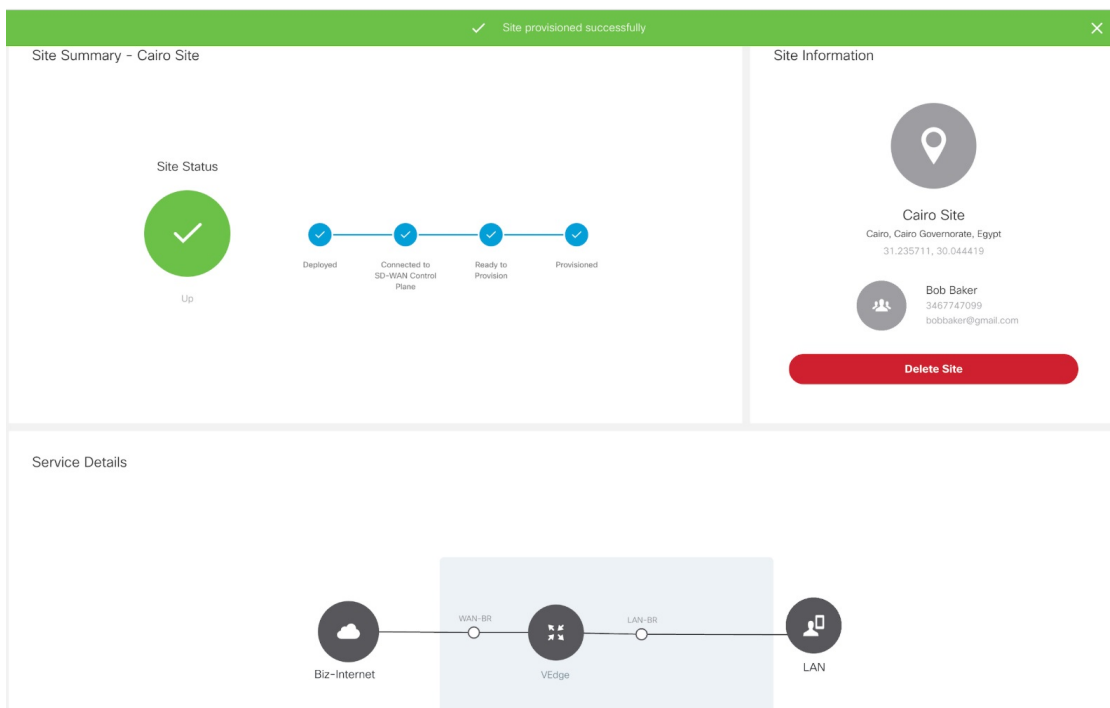
This section covers procedure on deleting a customer site on vEdge Cloud and vEdge SP Cloud. For more information on the site status, see [Monitoring SD-WAN Service Status](#).

Deleting a Device

To delete a customer device:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, click Dashboard.
- Step 3** Select the tenant from the drop-down.
- Step 4** Click SD-WAN. The SD-WAN Service Offer screen appears.
- Step 5** Click SD-WAN.
- Step 6** Select the SD-WAN service. The SD-WAN screen appears.
- Step 7** In the Map View, click the device that you want to delete. The Device Summary screen appears.

Figure 24: Deleting a Device



- Step 8** Click Delete Device. This permanently deletes all information about the site and the device from Cisco MSX.

If the delete operation fails, the device status is displayed in the Device Summary as Deleting Failed. In this case, you need to click Force Delete Device. Click Force Delete Device in the confirmation window.

This deletes all the information about the device from Cisco MSX.

Figure 25: Force Deleting a Device



Detaching an SD-WAN Control Plane

After you detach a control plane, management of any ENCS devices used to deploy vEdge Cloud devices will no longer be available using the MSX SDWAN service. If you reattach the control plane, you can manage the vEdge Cloud devices.

Before you Begin

Only users with the permission 'SD-WAN Control Plane' can detach a Control Plane.

Step 1 Log in to the Cisco MSX portal.

Step 2 From the left pane, click Tenant Workspace > Services.

Step 3 In the SD-WAN service panel, click on the ellipsis (...) and click Detach Control Plane.

The control plane detachment process may take a few minutes as MSX clears up a few things in the background, such as templates assigned to tenants in the background.

Cisco MSX does not unsubscribe the SD-WAN service when you detach the control plane. To unsubscribe from the SD-WAN service for a specific tenant, click on the ellipsis (...) and click Unsubscribe. For more information, see [Unsubscribing the SD-WAN Service](#).

Unsubscribing the SD-WAN Service

Use this procedure to unsubscribe from the SD-WAN service for a specific tenant. You cannot unsubscribe an SD-WAN service for Meraki.

-
- Step 1** Log in to the Cisco MSX Portal.
- Step 2** From the left hand pane, click Tenant Workspace > Services.
- Step 3** In the SD-WAN service panel, click on the ellipsis (...) and click Unsubscribe.
The Unsubscribe from SD-WAN Service window is displayed.
- Step 4** Click Unsubscribe.
The Unsubscribe Initiated notification is displayed.
- Step 5** Click Close.
The unsubscription process first deletes the control plane if created or detaches if attached, and then unsubscribes from the SD-WAN service. The estimated time for the unsubscription process depends on the number of devices in the system. You can monitor the unsubscription status on the SD-WAN service panel or in the event logs in Cisco MSX.
-



CHAPTER 7

Deploying Cisco Meraki SD-WAN Services on MSX

This section details the procedures for deploying Cisco Meraki SD-WAN services on Cisco Managed Services Accelerator (MSX).

- [Deployment Workflow for Meraki SD-WAN, on page 79](#)
- [Postdeployment Tasks for Meraki SD-WAN, on page 82](#)
- [Maintaining Cisco Meraki SD-WAN Deployments , on page 82](#)

Deployment Workflow for Meraki SD-WAN

Cisco MSX allows seamless integration with Meraki's SD-WAN service providing capability to create SD-WAN networks and managing the devices in them.

The Meraki cloud solution is a centralized management service that allows users to manage all of their Meraki network devices with a single simple and secure platform. Meraki networks are used to contain devices and their configurations and map to sites on Cisco MSX.

To deploy a SD-WAN service for Meraki:

Table 12: SD-WAN Service Deployment Workflow for Meraki

Task	See
1. Attach control plane for Meraki SD-WAN.	Setting Up SD-WAN Control and Management Plane for Meraki
2. Create sites.	Adding a New Site or Device for Meraki
3. Perform post deployment activities on Meraki SD-WAN	Maintaining Cisco Meraki SD-WAN Deployments

Setting Up SD-WAN Control and Management Plane for Meraki

To create the Meraki SD-WAN control plane service:

Before you begin

Configure Meraki-specific initial settings in MSX. For more information, see [Setting Up Meraki SD-WAN-Specific Configurations in MSX](#).

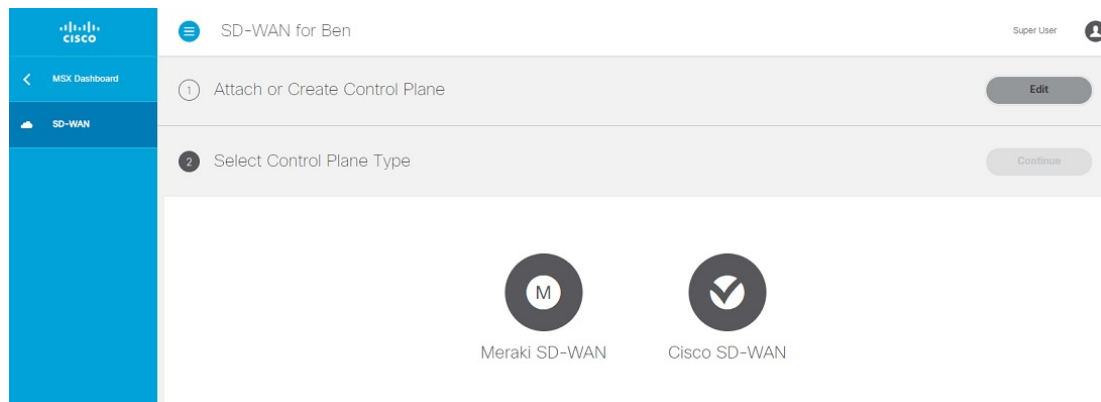
- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, click Tenant Workspace > Services.
- Step 3** In the SD-WAN service panel, click on the ellipsis (...) and click Meraki SD-WAN Home.
- Step 4** Click Add Control Plane to launch the wizard.
- Step 5** Select Attach to use an existing control plane. Click Continue.
- Step 6** In the Select Control Plane Type section, select Meraki SD-WAN to attach a Meraki SD-WAN control plane. The selected controller will appear in blue.
- Step 7** Click Continue.
- Step 8** Enter the API Access Key.
- Step 9** Enter the Organization ID.

The organization ID helps to uniquely identify tenant's Meraki SD-WAN control plane. This ID appears in the field if you have already configured Meraki in Tenant Workspace > Settings. We recommend that you configure this ID in the Meraki Organizations Settings.

- Step 10** Click Submit.

The Meraki SD-WAN Control plane is attached.

Figure 26: Attaching the Meraki SD-WAN Control Plane



Adding a New Device for Meraki

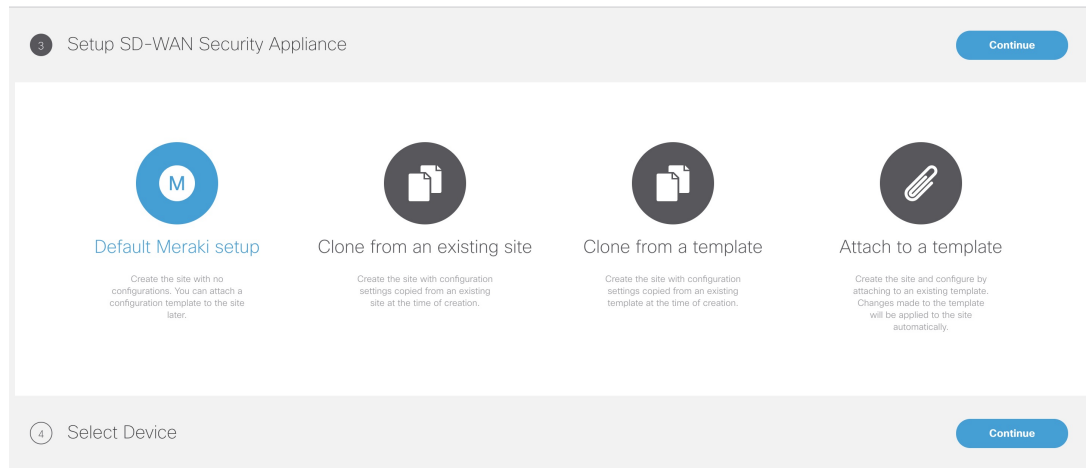
Before You Begin

Set up the Meraki control plane for the tenant and ensure that the status is active. For more information, see [Setting Up Meraki SD-WAN-Specific Configurations in MSX](#).

To create a new device:

-
- Step 1** Log in to the Cisco MSX portal.
- Step 2** From the left pane, click Tenant Workspace > Services.
- Step 3** In the SD-WAN service panel, click on the ellipsis (...) and click Meraki SD-WAN Home. The SD-WAN home page appears and displays the Device Summary window for the selected tenant.
- Step 4** Click Add Device button to add a new Meraki device.
- Note** The Add Device button is enabled only if the control plane is provisioned for the tenant.
- Step 5** Select Control Plane Type. Select Meraki as the control plane type and click Continue.
- If the tenant has only Meraki control plane deployed, only the Meraki controller type is enabled. If the tenant has both Cisco SD-WAN and Meraki control planes, you can choose to add site on either Meraki or Cisco SD-WAN control planes. For more information, see [Deploying a Site or Device for Cisco SD-WAN](#).
- Step 6** Enter the device information such as Location, Latitude, Longitude, and Support details, and click Continue.
- Step 7** Select a Device Type. Choose from one of the following device types you want to set up on your Meraki site:
- Access Point: Set up a site with only wireless devices.
 - Security: Set up a site with only security devices.
 - Switch: Set up a site with network switches.
 - Combined: Set up a site with a combination of wireless access points and security appliance devices.
- Step 8** Set up Meraki device. Choose from one of the following options:
- a. Default Meraki Setup: Create the device without any template configurations, but later you can attach the template to the device.
 - b. Clone from an existing device: Create the device with configuration settings copied from an existing device to a new device. From the Select Device drop-down list, select the device from where the configuration settings must be copied. The options shown in the drop-down depends on the device or the network type you chose in Step 8. After cloning, configuration changes made to the source device are not inherited into the new device.
 - c. Clone from a Template: Create the device with configuration copied from an existing template into a new device. From the Select Template drop-down list, select the template from where the configuration must be copied. The options shown in the drop-down depends on the device or the network type you chose in Step 8.
 - d. Attach to a Template: Create the device and then associate it to an existing template. From the Select Template drop-down list, select the template that can be associated with the new device. The options shown in the drop-down depends on the device or the network type you chose in Step 8. Any changes in the template are automatically applied to all the associated device.

Figure 27: Setting Up the SD-WAN Security Network



Step 9 Select a device to add. From the Select a Device to Add drop-down list, choose the device to be added from the device inventory. The options shown in this drop-down depends on the device or the network type you chose in Step 7. After creating a device, from the Device Summary page, you can use the option 'Add Additional Devices' to add more devices.

Step 10 Click Submit. The device summary page appears.

Postdeployment Tasks for Meraki SD-WAN

The post deployment tasks for the Meraki SD-WAN are:

Deploying an Additional Controller Type

Cisco MSX allows you to create new or attach a Cisco SD-WAN control plane to a tenant that already has a Meraki control plane deployed. Thus, allowing you to manage both Cisco SD-WAN and Meraki control plane and site information at the same time.

For deploying a Cisco SD-WAN control plane to the tenant, see [Setting Up Control Plane for Cisco SD-WAN](#).

After both the control planes are deployed, you can select sites based on controller type filter option in List and Map view.

Maintaining Cisco Meraki SD-WAN Deployments

This section covers the maintenance tasks for Cisco Meraki SD-WAN deployments.

Configuring Application Relevance Settings for Meraki SD-WAN

Use application relevance settings in MSX to give a particular application higher priority, among others, and apply these settings across MSX-managed Meraki SD-WAN sites.



Note The application relevance setting is supported only for following Meraki sites/network type:

- Sites with MX device models (SD-WAN Security appliance)
- Sites that are not attached to any templates.

Use this procedure to configure application relevance settings in MSX to assign a particular application higher priority among others.

Before you begin

- Make sure one or more Meraki application class model template are assigned and available to the tenants. For more information, see [Managing Meraki Traffic Class Access for Tenants](#).
- Create or attach Control Plane, see [Setting Up SD-WAN Control and Management Plane for Meraki](#).
- Ensure you have the following permissions to configure traffic policies:
 - SD-WAN Traffic Policy: Users with manage permission can add and modify Application Relevance policy or Path Preference policy to the SD-WAN fabric.
 - Service Configuration Application: Users with manage permission can configure application relevance for Meraki applications. You can find this permission under Services, Configurations, and Devices category of permissions.

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

Step 2 From the left hand pane, click Dashboard.

Step 3 In the Subscription dashlet, click SD-WAN and click SD-WAN Home.

Step 4 Select the tenant from the drop-down and click Traffic Policy in the main menu.

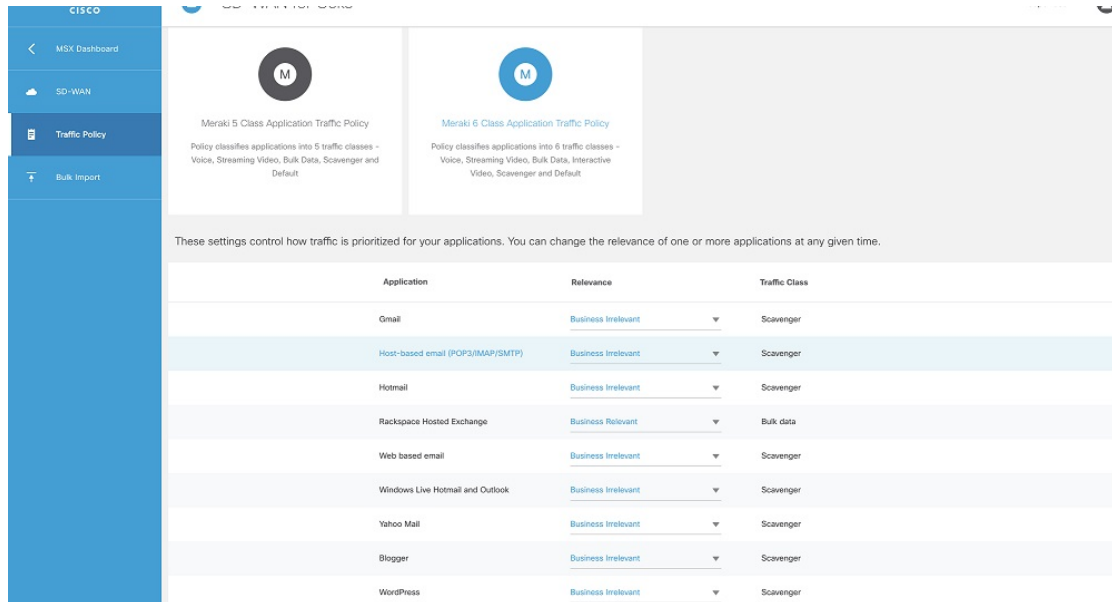
Step 5 Select Meraki SD-WAN Traffic Policy.

Note The application relevance settings can be configured only when the control plane has been created or attached for the tenants.

Step 6 In the Application Relevance tab, select a policy class model that suits your requirements.

A policy class model is based on the number of traffic classes it includes. Depending on the selected class, the list of applications for the chosen class model appears on the same page. For information on the out-of-box applications available with Meraki SD-WAN in MSX, see [Applications Available with Cisco MSX SD-WAN](#).

Figure 28: Meraki Policy Class Models



Step 7 Edit the application relevance for the applications. To edit, select an application, and choose one of the following business relevance settings from the relevance drop-down list.

- **Default:** Applications classified as Default are given a Normal priority.

These applications may or may not contribute to business objectives. For example, HTTP/HTTPS at times may be used for work or for personal reasons. As such, it may not always be possible to assign a static business-relevant designation to such applications. Such applications should be marked as default.

- **Business Relevant:** Applications classified as relevant (important for business) will be placed high in the priority queue.

These applications are known to contribute to business objectives of the organization and may include voice, multimedia applications, collaborative applications, database applications, email applications, file/content transfer applications, backup applications, and so on., as well as control plane, signaling, and network management protocols.

- **Business Irrelevant:** Applications classified as irrelevant (not important for business) moved to lowest traffic class priority.

These applications do not support business objectives and are typically consumer-oriented. These applications are known to have no contribution to business-objectives and are often personal or entertainment-oriented in nature. Such applications may include video-on-demand (for example, Netflix, YouTube, and so on), gaming traffic, peer-to-peer file-sharing applications, and other applications.

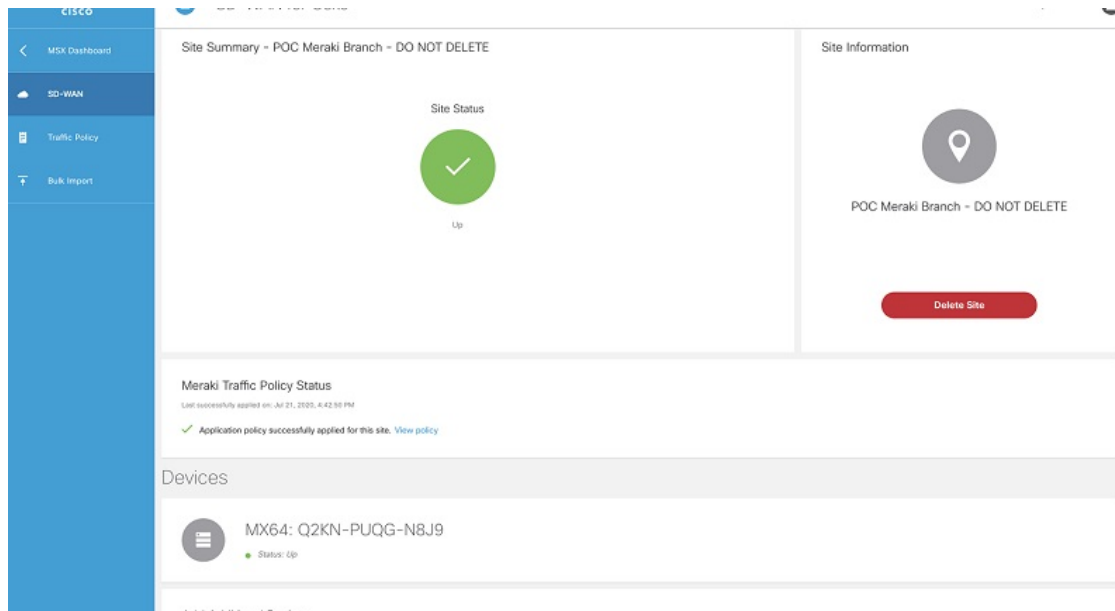
Step 8 Review or modify the Application relevance settings and click Apply to Meraki Sites to apply these changes across all Meraki sites for the selected tenant.

Step 9 Click Apply on the Confirm Policy Apply dialog box to proceed with applying the changes across Meraki sites.

Note A Turquoise mark beside an application indicates that the application relevance is being applied and new settings cannot be applied until the current process is completed.

After applying the policy, you can view the status under Meraki Traffic Policy Status section on the Site Summary page.

Figure 29: Applied Policy Status on the Site Summary Page



Deleting the Meraki Site

To delete the Meraki site:

- Step 1** Log in to the Cisco MSX portal using your credentials.
- Step 2** From the left hand pane, click Dashboard.
- Step 3** Click SD-WAN. The SD-WAN window is displayed.
- Step 4** Select the tenant from the drop-down.
The SD-WAN Home screen refreshes and displays site status and control plane status for the selected tenant.
- Step 5** In the List view, select the Meraki controller type. Cisco MSX displays all the sites with Meraki control plane.
- Step 6** Select the Site for which you want to view the summary. The site summary screen appears.
- Step 7** Click Delete Site. This action permanently deletes all information about the site and device from the Cisco MSX.

Detaching the Control Plane for Meraki

To detach the control plane for Meraki:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu of the Cisco MSX Portal, click Dashboard.
- Step 3** Click SD-WAN. The SD-WAN screen appears.

- Step 4** Select the tenant from the drop-down.
The SD-WAN Home screen refreshes and displays site status and control plane status for the selected tenant.
- Step 5** In the List view, select the Meraki as the controller type. All the sites of Meraki control plane are displayed.
- Step 6** Select the Site. The site summary screen appears. The Meraki control plane dashboard is shown.
- Step 7** To detach control plane, click the Detach Control Plane button.
-



CHAPTER 8

Monitoring Cisco SD-WAN and Meraki SD-WAN Services in MSX

Cisco MSX new GUI includes a MSX Dashboard and a Tenant Workspace, that are visible only if users have subscribed to the Cisco MSX Enterprise Access (EA) service pack.

This chapter contains the following sections:

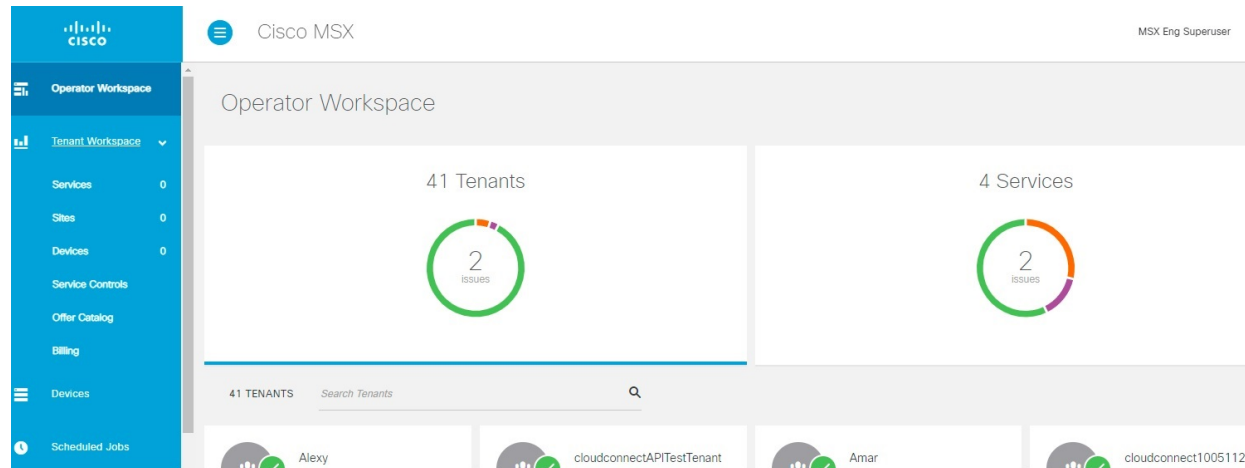
- [Monitoring SD-WAN Service Status on the Cisco MSX GUI, on page 87](#)
- [Monitoring Cisco SD-WAN Device Status, on page 90](#)
- [Understanding Cisco SD-WAN Device Statuses, on page 91](#)
- [Monitoring SD-WAN Control Plane Status , on page 101](#)
- [Monitoring Tunnel Health, on page 103](#)
- [Monitoring SD-WAN Reporting Metrics Using Third-Party Network Monitoring Applications, on page 106](#)
- [Monitoring the Traffic Policy, on page 106](#)
- [Viewing Event Logs, on page 107](#)

Monitoring SD-WAN Service Status on the Cisco MSX GUI

The new GUI has the following workspaces:

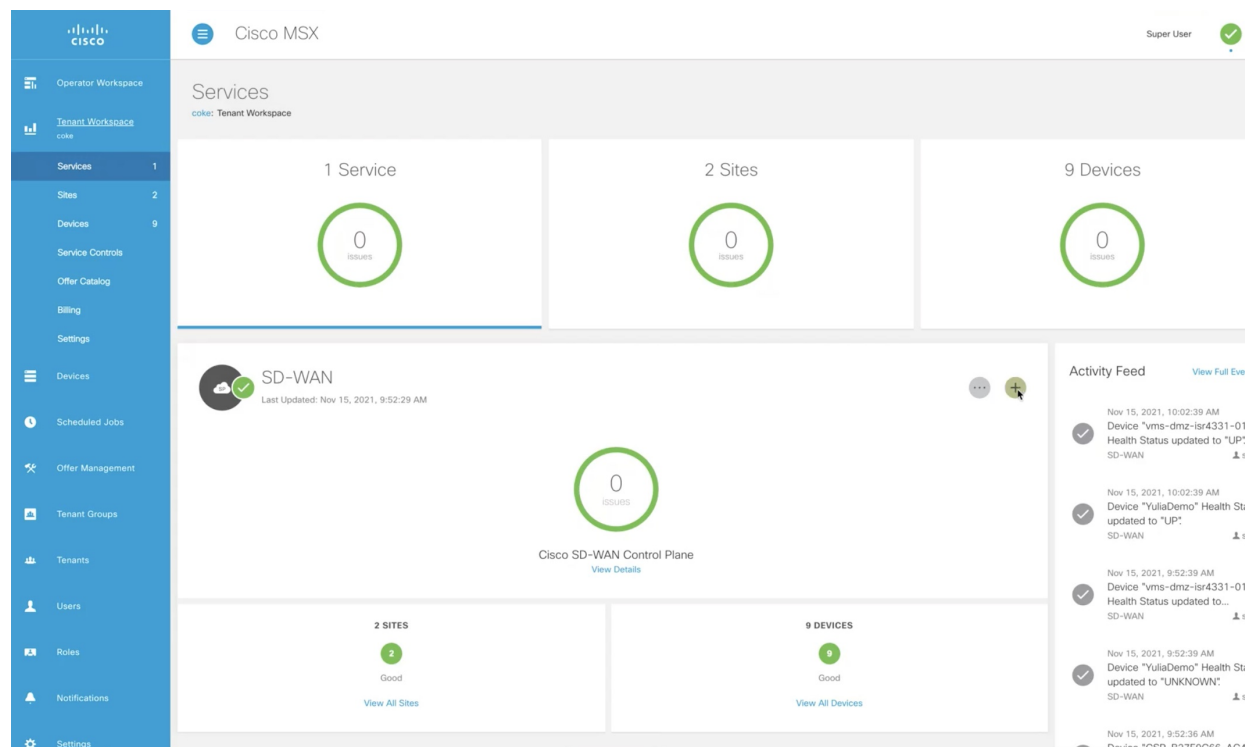
- Operator workspace: Lists all the tenants and the services these tenants have subscribed to. The Operator Workspace has dashlets such as Tenants and Services. The tenant-centric portal is role-based and is accessible by operators.

Figure 30: Operator Workspace



- Tenant Workspace: Allows tenants to access information related to their subscribed services. The following are the menus that are available in the tenant workspace:

Figure 31: Tenant Workspace



- Services: Display all services subscribed by a tenant, service status, other service metrics, and control plane status.

For more information on service statuses in the Tenant Workspace, see [Understanding Cisco SD-WAN Service Statuses](#).

- Sites: Display an overview of the tenant's sites, site status, and allows access to site details.

- **Devices:** Displays an overview of the tenant's devices, device status, and allows access to device details.



Note Displays both mapped or unmapped sites or devices.

For more information on device statuses in the Tenant Workspace, see [Monitoring Cisco SD-WAN Device Status](#).

- **Service Controls:** Display the custom service controls that are used by the services. For Cisco MSX SD-WAN service pack, you can view traffic policies used by a tenant and perform bulk import of device templates.
- **Offer Catalog:** Display existing subscriptions and allows subscribing to new services.
- **Billing:** Display billing information about the tenant's subscriptions. For more information on billing, see [Managing Billing](#).
- **Activity Feed:** The Cisco MSX portal allows a tenant to view several events pertaining to the subscriptions, sites, devices, template, and services. The events that are logged in the Events Log window are also used in the Activity Feed. To view the Activity Feed, choose Tenant Workspace > Services window. These contextual event feeds are also displayed on the Sites Detail window and Devices Detail window.

Understanding Cisco SD-WAN Service Statuses

The service panel in the Tenant workspace allows tenants to see the next steps that can be performed for their subscribed services. After the services are set up and the network has connectivity, the panel also shows the services-related metrics.

Tenants can monitor the status of the SD-WAN service in the Service tab and the SD-WAN service panel. This overall service status is calculated based on the service lifecycle status.

The following table illustrates the SD-WAN service lifecycle status:

Color	SD-WAN Service Status	Description
Blue	Ready to Provision	SD-WAN control plane is not attached or created.
Purple	Provisioning Deprovisioning	Provisioning: Cisco MSX is attaching, or creating the SD-WAN control plane. Deprovisioning: Cisco MSX is deleting, or detaching the SD-WAN control plane.
Green	Provisioned	Cisco MSX has attached or created the SD-WAN control plane.
Orange	Failed	Provisioning or deprovisioning of the control plane failed.

Monitoring Cisco SD-WAN Device Status

The Devices menu option in the Tenant Workspace provides the devices' overall status. The Devices menu displays both mapped (latitude and longitude defined) or unmapped devices.

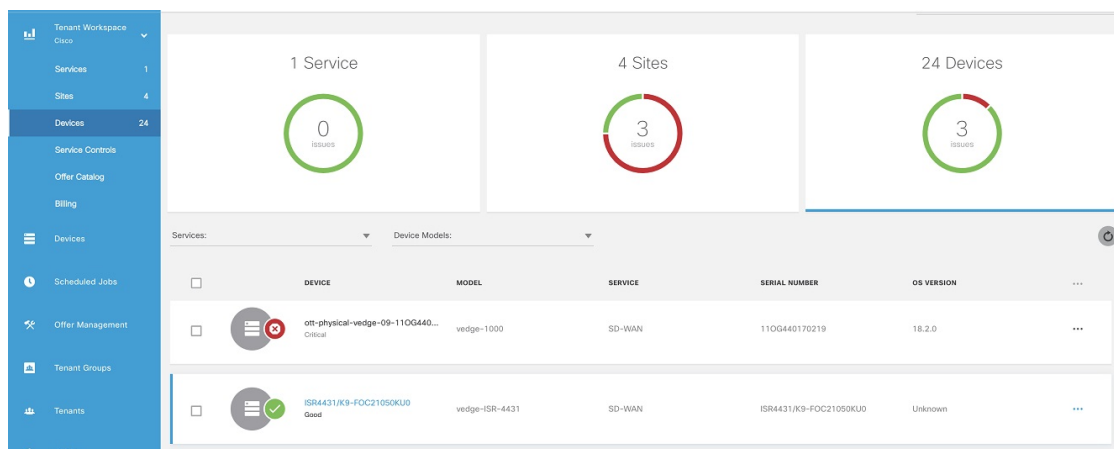
Using this procedure, you can view the SD-WAN and Meraki device statuses.

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

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

The Devices Overview window is displayed with overall status of the devices.

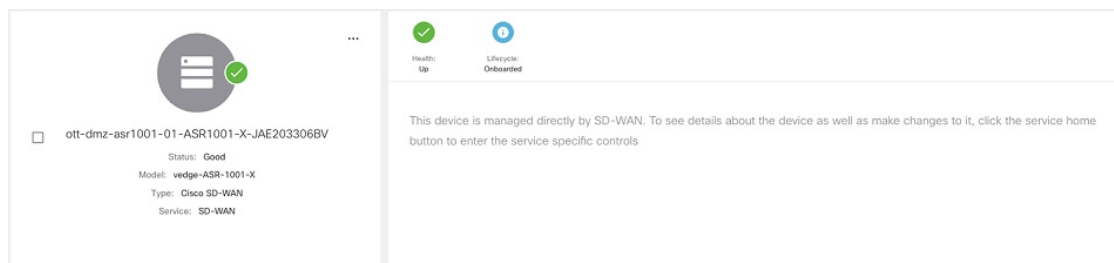
Figure 32: Device Overview window



Step 3 To view the status of a device, hover the mouse over the device and click to view the device summary.

The device view expands and its overall status is displayed along with its health and lifecycle status.

Figure 33: Device Expanded View



Note For more information on the Cisco MSX device status for SD-WAN devices, see [Understanding Cisco SD-WAN Device Statuses](#).

Step 4 Click Device Details to view additional details of the device such as reachability, control plane name, last sync time, IP address, device template details.

Device template shows the device template and its related information that was applied to that particular device. Related information includes device model, chassis number, system IP, hostname, and device template name.

For more information about the sync time, see [Understanding Cisco SDWAN Synchronization](#).

Understanding Cisco SDWAN Synchronization

MSX synchronizes device inventory and configurations with the Cisco SD-WAN. During the sync time, MSX polls the controller, checks for updates, and updates the device details in MSX. This synchronization occurs every n minutes. By default, the sync time is 60 minutes.

The data presented on the device window is refreshed every (n) minutes depending on the time set.

Configuring the Sync Time

You can use the Task Scheduler Administration API to configure the sync time. As an operator, you can use PUT API (/api/v1/taskscheduler/{taskID}) and update the value of recurrenceCronExpression to modify this duration.

Understanding Cisco SD-WAN Device Statuses

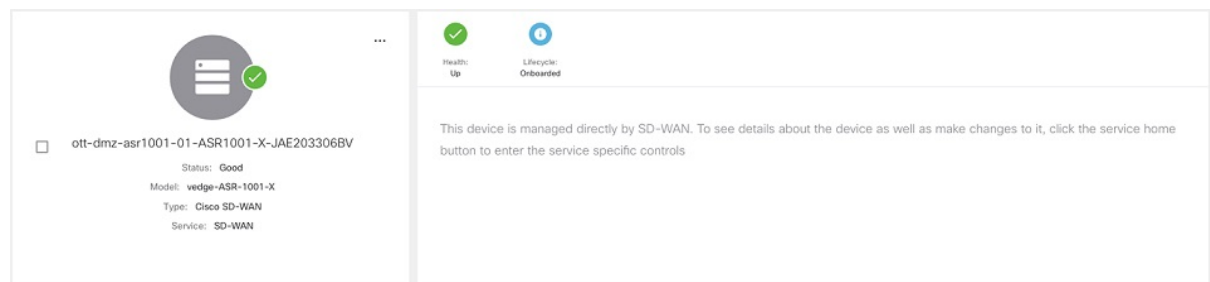
The overall device status (indicated by the Status option on the left-hand side of the Devices window) is categorized as In Progress, Critical, Poor, Fair, Good, and Unknown.



Note

The device status in the legacy GUI is not the same as the status in the new MSX GUI. The overall device status is calculated based on the device lifecycle status (indicated by the Lifecycle bubble on the right-hand side). However, in some cases, overall device status also includes the device health status (indicated by the Health bubble on the right-hand side). The Device health status is considered only when the devices have system_ip configured or have VNFs successfully deployed and connected.

The following figure illustrates overall device status, device health, and lifecycle status for an SD-WAN device.



Within Cisco MSX, any status type are numbered from 1 to 7, with the highest number 7 indicating the status as 'Critical' and the lowest number 1 indicating the status as 'Good'. An overall status looks into the available statuses (lifecycle or device health or both) for a device and picks the highest number and maps it to the below overall statuses.

Overall Status vs Severity Number in Cisco MSX

Overall Status	In Progress	Critical	Poor	Fair	Unknown	Good
Severity Number	9	7	6	5	3	1

The following table illustrates the mapping of SD-WAN lifecycle status and their severity level which defines the overall device status:

SD-WAN Device Lifecycle Status Shown in the Devices Window	What These Lifecycle Status Indicate	Severity Number (Determines the Overall Status in the GUI)	Overall Status Indication Based on the Severity Number
Configuring	Incomplete: Device is not ready to be provisioned because the data filled was incorrect or incomplete. The device will be in this status until the details are corrected, and the template file is imported again into MSX.	3	Unknown
Configuring	Ready to Provision: Device is connected and bulk data is imported. All provisioning details are completed and device is ready to provision.	3	Unknown
Provisioning	Provisioning: Provisioning process pushes the configuration data into the Control Plane such that the site is set up for day one configurations. The provisioning process on the Control Plane takes approximately 5 to 10 minutes.	3	Unknown
Provisioning Failed	Provisioning Failed: The Site Status changes to 'Provisioning Failed' if the configuration data imported does not match with the values on the Control Plane.	6	Poor
Provisioned	Provisioned: Site was provisioned successfully.	1	Good
Onboarded	Deployed: ENCS site is deployed and vEdge is able to communicate to the Control Plane.	1	Good
Onboarding	Deploying: ENCS site deployment with a vEdge is in progress.	3	Unknown
Onboarding Failed	Deployment Failed: Could not bring up vEdge using ENCS.	6	Poor

SD-WAN Device Lifecycle Status Shown in the Devices Window	What These Lifecycle Status Indicate	Severity Number (Determines the Overall Status in the GUI)	Overall Status Indication Based on the Severity Number
Deleting	Deleting: Deleting a device is in progress.	3	Unknown
Deleting Failed	Deleting Failed: Deleting the device failed.	6	Poor




Depending on whether you are provisioning a physical, vEdge cloud, or vEdge SP Cloud, the site statuses and the next steps varies. For more information on these site statuses for these device types, see the sections below:




Device Statuses for Physical Device

The table below shows the status of Physical device (vEdge or IOS XE) with various validation messages shown on MSX, along with next steps.

Table 13: Device Statuses for Physical Device

Summary Status	Description	Next Steps
	<p>The device is in the process of being shipped to customer site. At this point, MSX portal does not show physical devices on the map as these still do not have any address or map coordinates for the sites to plot them on the map. The site is plotted as 'Unmapped sites' on MSX map.</p>	<p>Connect the device. After the device is installed on the premise, connect the device, it goes through the ZTP (Zero Touch Provisioning) process and gets connected to the Control Plane.</p>
	<p>The device has established connectivity to the Control Plane, but does not have the provisioning data to provision a device.</p>	<p>Import bulk data. For information, on how to import, see Importing Multiple Site Data from Cisco SD-WAN into MSX.</p> <p>After importing, MSX displays various validation messages to indicate the errors or missing information in the template file. You can click View Details in the validation message to display the Site Import Summary with the error list.</p> <p>Note We recommend that you download the error list as the information this screen is temporary and will disappear after you exit this page.</p>


Summary Status	Description	Next Steps
 <p>Incomplete</p>	<ul style="list-style-type: none"> • Incomplete: Device is not ready to be provisioned because the data filled was incorrect or incomplete. The device will be in this status until the details are corrected, and the template file is imported again into MSX. 	<ul style="list-style-type: none"> • For device with 'Incomplete' status, see Provisioning Details under Device Summary. This section lists the fields that have missing data. Enter the missing details in the Site template file and import again.
 <p>Ready to Provision</p>	<ul style="list-style-type: none"> • Ready to Provision: Device is connected and bulk data is imported. All provisioning details are complete and device is ready to provision. 	<ul style="list-style-type: none"> • For device with 'Ready to Provision' status, see Provisioning Details under Device Summary, click Provision Device to initiate the provisioning process.
 <p>Up</p>	<ul style="list-style-type: none"> • Up: Device was provisioned successfully. • Critical: Device was up and was provisioned, but after a while it lost connectivity to the SD-WAN Control Plane. 	<p>If the status is 'Critical', troubleshoot SD-WAN control plane connectivity issue. For more information, see Troubleshooting Cisco SD-WAN Reachability Issues.</p>




Summary Status	Description	Next Steps
<p>Site Status</p>  <p>Provisioning</p>  <p>Provisioning Failed</p>	<ul style="list-style-type: none"> • Provisioning: Provisioning process pushes the configuration data into the Control Plane such that the device is set up for day one configurations. The provisioning process on the Control Plane takes approximately 5 to 10 minutes. • Provisioning Failed: The Device Status changes to 'Provisioning Failed' if the configuration data imported does not match with the values on the Control Plane. See Next Steps for more details. 	<p>Provisioning could fail because of one of the following reasons.</p> <ul style="list-style-type: none"> • Data could not be validated as the template on MSX modified since the last upload. Correct the entries that are missing or incorrect. For information, on how to edit these entries, see Step 5 in Importing Multiple Site Data from Cisco SD-WAN into MSX. • If the information does not match with the data on the control plane, provisioning fails, and the missing or incorrect fields are highlighted in the Device Summary. Correct the entries that are missing or incorrect. For information, on how to edit these entries, see Step 5 in Importing Multiple Site Data from Cisco SD-WAN into MSX. • Unexpected errors on the Control Plane. If the state of the device appears as Out-of-Sync under the Basic Details, check the Event Log to get more details on the errors. For more information, see Viewing Event Logs.
 <p>Offline</p>	<p>Offline: A device is in the process of being shipped has been uploaded and provisioned on the Control Plane. When the device is connected and has reachability to the Control Plane, the template on the Control Plane is applied on the device.</p>	<p>Connect the device.</p>

Device Statuses for vEdge SP Cloud

The table below show the statuses for vEdge SP Cloud with various validation messages shown on MSX, along with next steps.

Table 14: Device Statuses for vEdge SP Cloud

Summary Status	Description	Next Steps
 <p>Unknown</p>	<p>Unknown: Device has been added on MSX portal and the configurations are downloaded by the service provider. The Unknown state indicates the time period when the Service Provider uses the downloaded configurations to bring up a vEdge cloud to finish deployment.</p> <p>The device during this phase waits for the vEdge to be deployed and connected back to SD-WAN Control Plane.</p>	<p>During this state, bulk data can be imported and provision the SP Cloud through MSX. For information, on how to import, see Importing Multiple Site Data from Cisco SD-WAN into MSX.</p>



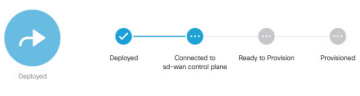


Summary Status	Description	Next Steps
 <p>Connected</p> <p>Not Connected</p>	<ul style="list-style-type: none"> • Connected: Device deployment is complete and vEdge is able to communicate to the Control Plane, but does not have the provisioning data to provision a device. • Not Connected: Not Connected indicates a state when a connection was established once and then connection with Control Plane was lost because of Interface being shutdown. 	<ul style="list-style-type: none"> • If in 'Connected' status, next step is to import bulk data. For information, on how to import, see Importing Multiple Site Data from Cisco SD-WAN into MSX. <p>After importing, MSX displays various validation messages to indicate the errors or missing information in the template file. You can click View Details in the validation message to display the Site Import Summary with the error list.</p> <p>Note We recommend that you download the error list as the information on this screen is temporary and will disappear after you exit this page.</p> <ul style="list-style-type: none"> • If the status is 'Not Connected', troubleshoot SD-WAN control plane connectivity issue. For more information, see Troubleshooting Cisco SD-WAN Reachability Issues.
 <p>Ready to Provision</p> <p>Ready to Provision</p>	<p>Ready to Provision: In both cases, that is, connected to control plane and not connected to control plane, bulk data can be imported, and the devices are ready to be provisioned.</p>	<p>For device with 'Ready to Provision' status, see Provisioning Details under Device Summary, click Provision Device to initiate the provisioning process.</p>
 <p>Incomplete</p>	<p>Incomplete: Device is not ready to be provisioned because the data filled was incorrect or incomplete. The device will be in this status until the details are corrected, and the template file is imported again into MSX.</p>	<p>For device with 'Incomplete' status, see Provisioning Details under Device Summary. This section lists the fields that have missing data. Enter the missing details in the Site template file and import again.</p>





The remaining statuses for the vEdge SP cloud are similar to the Physical devices. For more information on the other statuses, see [Device Statuses for Physical Device](#).




Device Statuses for vEdge Cloud

The table below show the site status for vEdge Cloud with various validation messages shown on MSX, along with next steps.

Table 15: Device Statuses for vEdge Cloud

Summary Status	Description	Next Steps
 <p>Deploying</p>	ENCS site deployment with a vEdge is in progress.	
 <p>Not Connected</p>	Not Connected: vEdge is deployed but is not able to establish connection with the Control Plane.	<ul style="list-style-type: none"> If not connected, troubleshoot SD-WAN control plane connectivity issue. For more information, see Troubleshooting Cisco SD-WAN Reachability Issues. After the connection is established, you can import bulk data from multiple sites and provisioning one device at a time. For more information, see Provisioning a Device.
 <p>Deployed</p>	<ul style="list-style-type: none"> Deployed: ENCS site is deployed and vEdge is able to communicate to the Control Plane. 	Troubleshoot the data plane. For more information, see Data Plane Troubleshooting .
 <p>Deployment Failed*</p>	<ul style="list-style-type: none"> Deployment Failed: Could not bring up vEdge using ENCS. 	
 <p>Connected</p>	Connected: vEdge is deployed and connected to Control Plane. System is now ready for bulk import of data from multiple sites.	After the connection is established, you can import bulk data for provisioning the site. For more information, see Importing Multiple Site Data from Cisco SD-WAN into MSX .

Summary Status	Description	Next Steps
 	<p>Incomplete: Device is not ready to be provisioned because the data filled was incorrect or incomplete. The device will be in this status until the details are corrected, and the template file is imported again into MSX.</p>	<ul style="list-style-type: none"> For site with 'Incomplete' status, see Provisioning Details under Device Summary. This section lists the fields that have missing data. Enter the missing details in the Site template file and import again.
 	<p>Ready to Provision: Device is connected and bulk data is imported. All provisioning details is complete and device is ready to provision.</p>	<ul style="list-style-type: none"> For device with 'Ready to Provision' status, see Provisioning Details under Device Summary, click Provision Device to initiate the provisioning process.

Summary Status	Description	Next Steps
 	<ul style="list-style-type: none"> • Provisioning: Provisioning process pushes the configuration data into the Control Plane such that the site is set up for day one configurations. The provisioning process on the Control Plane takes approximately 5 to 10 minutes. • Provisioning Failed: The Device Status changes to 'Provisioning Failed' if the configuration data imported does not match with the values on the Control Plane. See Next Steps for more details. 	<p>Provisioning could fail because of one of the following reasons.</p> <ul style="list-style-type: none"> • Data could not be validated as the template on MSX was modified since the last upload. Correct the entries that are missing or incorrect, and import the site template file again. For information, on how to edit, see step 5 in Importing Multiple Site Data from Cisco SD-WAN into MSX. <p>Note You can directly edit the site template from MSX any number of time as required.</p> <ul style="list-style-type: none"> • If the information does not match with the data on the control plane, provisioning fails, and the missing or incorrect fields are highlighted in the Device Summary. Correct the entries that are missing or incorrect, and import the site template file again. For information, on how to edit, see step 5 in Importing Multiple Site Data from Cisco SD-WAN into MSX. • Unexpected errors on the Control Plane. If the state of the device appears as Out-of-Sync under the Basic Details, check the Event Log to get more details on the errors. For more information, see Viewing Event Logs.
	<ul style="list-style-type: none"> • Up: Device was provisioned successfully. • Critical: Device was up and was provisioned, but after a while it lost connectivity to the SD-WAN Control Plane. 	<p>If the status is 'Critical', troubleshoot SD-WAN control plane connectivity issue. For more information, see Troubleshooting Cisco SD-WAN Reachability Issues.</p>

Site Statuses for Meraki SD-WAN Devices

The table below shows the site statuses for Meraki SD-WAN sites shown on MSX, along with the next steps.

Table 16: Site Statuses for Meraki Devices

Site Summary Status	Description	Next Steps
Up	At least one of the devices has uplink connectivity to the WAN network.	Configure SD-WAN Traffic Shaping rules for the network in the Meraki dashboard.
Down	Devices added to the site do not have connectivity to the WAN network.	Check the uplink configuration for the devices added to the site. For more information, see Checking Device Connections .
Needs Input	No devices added to Meraki site.	Add devices to establish connectivity to a WAN network. For more information, see Adding a New Site or Device for Meraki .
Unknown	Unable to collect information on device status. Unexpected errors on the Control Plane.	<ul style="list-style-type: none"> • Check if the Meraki beat is operational. For more information, see Checking Meraki Beat. • For a recently added device, wait for a few minutes as the device transitions to the actual status.

Monitoring SD-WAN Control Plane Status

In MSX SD-WAN, Control Plane allows you to centrally manage the devices for a tenant, including provisioning, monitoring, and so on.

Before you begin

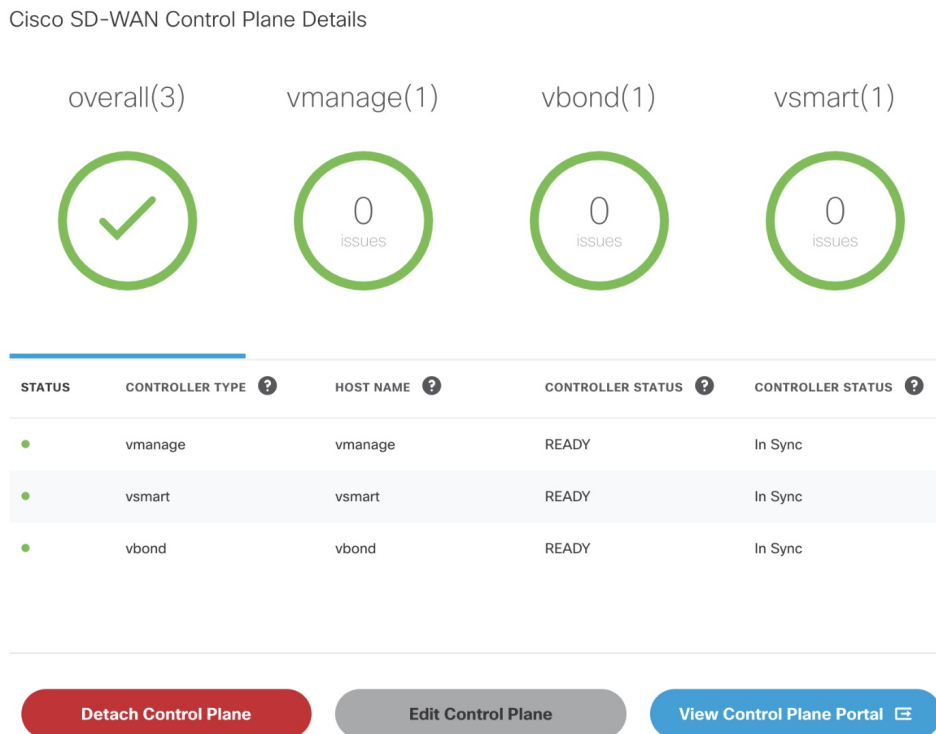
- Set up a control plane for your tenant.
 - For Cisco SD-WAN control plane, see [Setting Up Control Plane for Cisco SD-WAN](#)
 - For Meraki SD-WAN control plane, see [Setting Up SD-WAN Control and Management Plane for Meraki](#).
- Complete control plane's post deployment configurations.
 - For Cisco SD-WAN control plane, see [Postdeployment Tasks for SD-WAN Control Plane](#).
 - For Meraki SD-WAN control plane, see [Maintaining Cisco Meraki SD-WAN Deployments](#).

To monitor the status of the SD-WAN control plane:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** From the left pane, click Tenant Workspace > Services.
- Step 3** In the SD-WAN service panel, click on the ellipsis (...) and click Control Plane Details.

The following is the Cisco SD-WAN Control plane status after the certification, the security groups, and other configurations are completed.

Figure 34: Cisco SD-WAN Control Plane Status

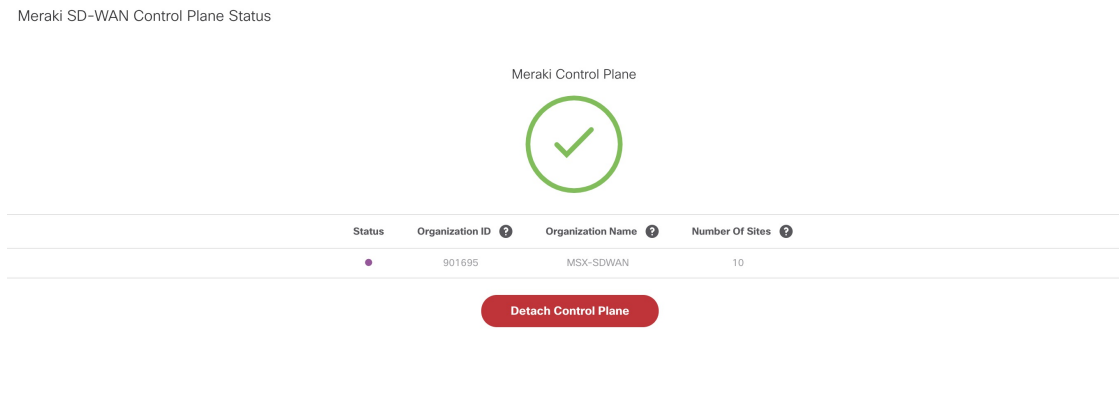


Note If your Cisco SD-WAN control plane remains in the 'Not Configured' state or is unable to connect to the control plane due to the authentication issue, see [Troubleshooting Control Plane](#).

- Step 4** To view the Meraki Control Plane status, click on the ellipsis (...) in the SD-WAN service panel and click Meraki SD-WAN Home. You can see this option only if the Meraki feature is enabled.

The following is the Meraki Control Plane status.

Figure 35: Meraki Control Plane Status



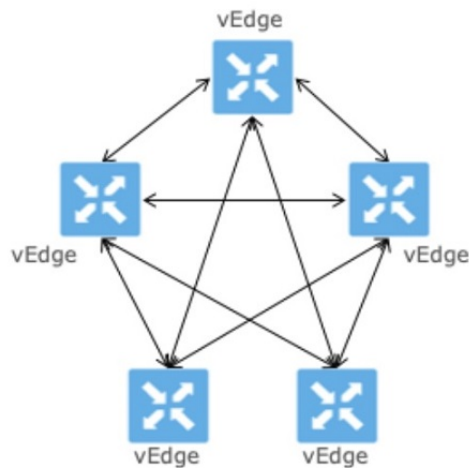
Monitoring Tunnel Health

The tunnel health graph gives an overview of the health of the IPsec tunnels from the SD-WAN device.

The tunnel report in MSX shows how many of these tunnels are up, which is an indication of whether the device is at risk of losing connectivity.

For example: In the following figure, tunnels are established for vEdge with every other vEdge in the network. If more tunnels are down, it could indicate that vEdge device from where tunnels are established is experiencing degradation. If only a small subset of tunnel links are down, it means other vEdge devices may be possibly experiencing degradation.

Figure 36: Tunnel Connectivity Between vEdge Devices



Tunnel Health Reporting or Tunnel Health Status Calculations:

Tunnels Up % = (Number of Tunnels in Up state / Total Number of Tunnels) * 100

For example:

If there are 200 tunnels and 80 tunnels are up, the Tunnel Up % will be $(80/200)*100 = 40\%$

For other tunnel performance metrics, such as data loss, latency, jitter information, click View Tunnel details on Control Plane to launch the tunnel details. For more information on these metrics, see Cisco SD-WAN documentation.

To view the control plane status for the SD-WAN service:

Before you begin

To monitor tunnel health, make sure users have the following permission assigned:

- Under Services, Configurations, and Devices category, select Service Metrics (View) permission permission.

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

Step 2 From the left hand pane, choose Tenant Workspace > Services.

The Services Overview window is displayed.

Step 3 Click on the SD-WAN Home option to display the tenant-specific Site Summary window.

Step 4 Click the Toggle button on the top right-hand side of the page to toggle between the list and map view with the list of sites for the selected tenant.

Note Both list view and map view displays all the sites (Meraki and Cisco SD-WAN) for the selected tenant.

Step 5 Select a site/device from the list of devices. The Site Summary window appears with site information and basic device details, such as chassis number, system IP, site ID, and so on.

The Site Status in the details page changes based on the various status of SD-WAN devices along with status of tunnel health. For more information on the the site/device lifecycle statuses, see [Monitoring Cisco SD-WAN Device Status](#).

The following table displays the Tunnel Health status that appears below the overall Site Status image based on the Tunnel Up %.

Tunnel Health Status	Tunnel Up %
Good	70-100
Fair	35-69
Critical	0-34

Note If MSX is unable to determine the tunnel health, the Tunnel Health status changes to an 'Unknown' state.

The following are a few examples of the overall Site/Device Status depending on control plane status and the text beneath the image is based on the tunnel health status.

Figure 37: Connected to control plane but the tunnels are starting to degrade (fair)

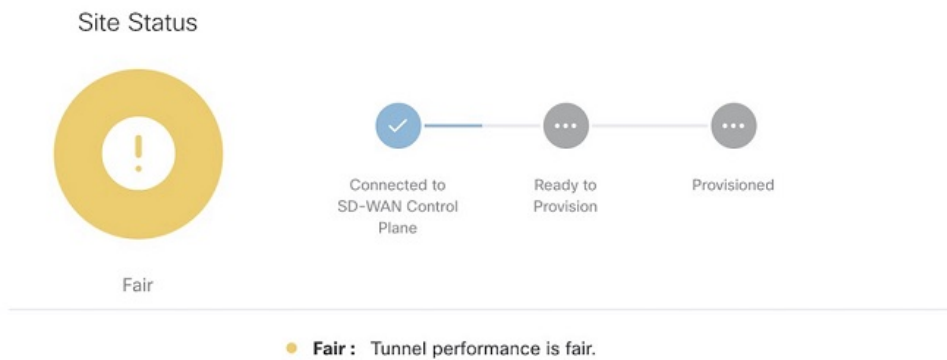
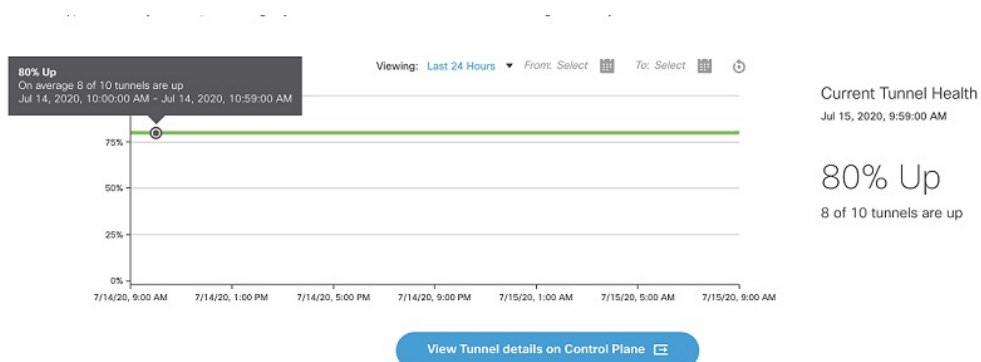


Figure 38: No connectivity to Control Plane but tunnel performance is fair



Step 6 On the Site Summary window, scroll down to the Tunnel Health section to view the current tunnel metrics. A graphical representation of all existing tunnels for the device appears.

Figure 39: Tunnel Health Graph



Where:

X axis - Time range

Y axis - Tunnels Up % (values 0-100)

Step 7 Select the time interval for displaying the tunnel health for that period. Choose one of the available time intervals from the Viewing drop-down list or click Custom to choose a time duration of your choice for which the reporting is displayed. Provide the day and time from when the reporting data must be collected until the specified end time. By default, last 24 hours chart is loaded.

Hover over the aggregated data points on the chart to get specific details, including the timestamp when the event occurred. These aggregated data points are system-generated. For more information on these data points, click on the Learn More link.

Monitoring SD-WAN Reporting Metrics Using Third-Party Network Monitoring Applications

You can integrate third-party network monitoring applications with SD-WAN on Cisco MSX, for example, LiveAction for real-time network insight. If integrated with SD-WAN, users can launch the application dashboard from the MSX Portal.

Before You Begin

Integrate LiveAction with MSX.

To launch a third-party monitoring portal from the Cisco MSX Portal:

-
- Step 1** Log in to the MSX portal using your credentials.
 - Step 2** From the left hand pane, click Dashboard. The Dashboard window is displayed.
 - Step 3** Click the SD-WAN Home button. The SD-WAN Home window is displayed.
 - Step 4** Select the tenant from the drop-down. The SD-WAN Home window refresh and displays the control plane status for the selected tenant.
 - Step 5** To launch the application dashboard, click Launch Monitoring Portal. The application dashboard opens up in a separate browser.
-

Monitoring the Traffic Policy

Monitoring the Traffic Paths

To confirm traffic path:

-
- Step 1** Log in to the vEdge or cEdge (IOX XE) server.

Step 2 Turn on application visibility on the vEdge or cEdge. To do so use the following commands:

Example:

```
config
policy
flow-visibility
commit
```

Step 3 Send traffic through the vEdge or cEdge.

Step 4 Check the path for vEdge and cEdge:

- For vEdge, use the following command:

Example:

```
show app cflowd flows | tab
```

- For cEdge, use the following command:

Example:

Monitoring the Application Queue

To confirm application queues:

Step 1 Log in to the vEdge or the cEdge server.

Step 2 Send traffic through the vEdge or cEdge.

Step 3 Check the queues for vEdge and cEdge:

- For vEdge, use the following command:

```
show policy data-policy-filter
```

- For cEdge, use the following command:

```
show sdwan policy data-policy-filter
```

The output will show all the available application queue.

Viewing Event Logs

To view the event logs:

Before you begin

Ensure you have the View Event Log permissions to view the status of the policies in the event log.

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click Event Log. The Event Log screen appears.

Figure 40: MSX Event Log

The screenshot shows the 'Event Log' interface with a search bar and filter options. The table below represents the data shown in the interface.

SEVERITY	TENANT	SERVICE	OBJECT	DESCRIPTION	USER	TIMESTAMP
✖			"clientId":"nfv-service","userId":"41ef9a00-cdfa-11ea-90bc-33b3b5253429","username":"sy... cdfa-11ea-90bc-33b3b5253429","tenantName":"... tenant","providerId":"fe3ad89c-449f-42f2-b4f8-b10ab7bc0266"	Can't find device by 29147328ce03-f852f1b9419c4d50b282ba28bf0700f9-sdwan. Failed to registerDevice to UFP.	system	7/9/20, 9:32 AM
ℹ			Schedule_task: 218aa717-acfd-bcab-3f36-1e52927a6af0	Scheduled a new task for [POST:sdwanservice/v1/controlplanemanager/29147328-ce03-48ec-94ad-f31914830ca5/synchronize] api. Task Id: [218aa717-acfd-bcab-3f36-1e52927a6af0]. Next execution time: [2020-07-09 04:15:00+0000]	superuser	7/9/20, 9:32 AM

Step 3 Select the tenant from the drop-down for which the event log has to be displayed.

Step 4 To filter the event log records, select the filter type from the drop-down. To list event logs for a specific duration, select the Custom Range check box and specify the dates.



APPENDIX

Appendixes

- [Troubleshooting Cisco SD-WAN Issues, on page 111](#)
- [Troubleshooting Cisco Meraki SD-WAN Issues, on page 129](#)
- [Applications Available with Cisco MSX SD-WAN, on page 137](#)
- [Out-of-the-Box Cisco SD-WAN Device Templates Available Within MSX, on page 139](#)
- [Sample Payloads for Creating Cisco SD-WAN Control Plane on Openstack, on page 149](#)



APPENDIX **A**

Troubleshooting Cisco SD-WAN Issues

This section describes problems, possible causes, recommended actions, and error messages, if applicable to the problem.

- [Troubleshooting Cisco SD-WAN Reachability Issues](#), on page 111
- [Troubleshooting ENCS Reachability Issues](#), on page 114
- [Changing MSX Trace Logging Level During Runtime](#), on page 115
- [Troubleshooting Control Plane](#), on page 117
- [Data Plane Troubleshooting](#), on page 122
- [PnP Server Troubleshooting Commands](#), on page 124
- [IPsec Tunnel Cannot be Established](#), on page 126

Troubleshooting Cisco SD-WAN Reachability Issues

Table 17: SD-WAN Reachability Issues

Color	Green	Red	Comment
Deployment Status	Provisioned	Provisioned-Failed: See Troubleshooting notes. For more information, see Troubleshooting Cisco SD-WAN vEdge-Cloud Deployment Deployment Errors .	Checks that VNF(s) is fully deployed and in active state.
Reachability Status	Reachable	Not Reachable: See Troubleshooting notes. For more information, see Troubleshooting Cisco SD-WAN vEdge Reachability Errors .	Checks the connectivity between the deployed vEdge and Cisco SD-WAN Control Plane.

Troubleshooting Cisco SD-WAN vEdge-Cloud Deployment Errors

After the service packs are deployed on MSX, the customer configuration templates are imported into the Cisco Network Services Orchestrator (NSO) platform for automating network orchestration. These configurations are then pushed from MSX to customer devices as part of the orchestration of device configuration. If the SD-WAN provisioning is not successful, most times, it is due to wrong parameters in the deployment data on NSO. There are multiple NSO instances if you are deploying more than one service pack. Therefore, these steps must be performed on the service pack-specific NSO node. SD-WAN uses SD-Branch's NSO, so in this case, the nso node will be nso-vbranch.

Step 1 Log in to one of the kubernetes master nodes.

```
# grep master inventory/inventory
[kube-master]
kubernetes-master-ctsai-east-2-1 ansible_host=<master_1_ip_address> ansible_user=centos
ansible_become=true
kubernetes-master-ctsai-east-2-2 ansible_host=<master_2_ip_address> ansible_user=centos
ansible_become=true
kubernetes-master-ctsai-east-2-3 ansible_host=<master_3_ip_address> ansible_user=centos
ansible_become=true
# ssh -F ssh.cfg centos@<master_1_ip_address>
```

Step 2 Access the NSO node using this command:

```
kubect1 -n vms exec -it nso-vbranch-0 -c nso-vbranch /bin/sh
```

Step 3 Change to vms user.

```
su vmsnso
```

Step 4 Run NSO CLI

```
ncs_cli -u admin
```

Step 5 Get the branch-cpe name, using the following command:

```
vmsnso@ncs> show branch-infra:branch-infra
```

Example:

```
branch-cpe axj9AUv5A06MXXSSWWSAAA {
  provider admin;
  type ENCS;
  serial <Device serial number>;
  var SD-Branch_DEVICE_TYPE {
    val ENCS;
  }
  var contact {
    val "Samuel";
  }
  var email {
    val noreply@cisco.com;
  }
  var phone {
    val 1112221234;
  }
  vnf SD-Branch-vEdge-18.3.0 {
    vdu vEdge;
  }
}
```

Step 6 Check the deployment summary, using the following command. Replace the branch-cpe name with the name that was identified in step 2.

```
vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe <name_from_above_command> plan component
state | tab
```

For example:

Example:

```
vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe axj9AUv5A06MXXSSWWSAAA plan component
state | tab
```



```
NAME STATE STATUS WHEN ref MESSAGE
```

```
self init reached 2018-09-06T19:30:32 -
ready failed 2018-09-06T20:33:11 -
axj9AUv5A06MdGMqHpmQ5ffN init reached 2018-09-06T19:30:32 -
pnp-callhome reached 2018-09-06T19:30:32 -
ready reached 2018-09-06T19:31:28 - Ready
vEdge_SD-Branch-vEdge-18.3.0 init reached 2018-09-06T19:31:36 -
ready reached 2018-09-06T19:32:30 - Ready
vEdge_axj9AUv5A06MdGMqHpmQ5ffN init reached 2018-09-06T19:32:31 -
vm-deployed reached 2018-09-06T19:32:58 -
vm-alive reached 2018-09-06T19:42:58 -
ready failed 2018-09-06T20:33:11 - NFWIS Error - Recovery: Recovery completed with errors for VM:
[axj9AUv5A06MdGMq_vEdge-_0_828e4709-1644-4706-946a-12d7fa71c8e3]
vm-recovered failed 2018-09-06T20:33:11 -
```

The summary displays the problem, if any. In the above example, SYSTEM_IP variable is wrong, because of which ENCS was unable to configure the VNF and was unable to attach the deployed Control plane on MSX.

Troubleshooting Cisco SD-WAN vEdge Reachability Errors

If there is no connectivity between the deployed vEdge and Cisco SD-WAN Control Plane:

Step 1 Login to the deployed vEdge and check the status of deployed vEdges.

- For a physical vEdge, directly login to the vEdge device.
- For an IOS XE device, login to IOS device then login to SD-WAN instance installed on the device.

```
ssh admin@<vEdge IP address>
a5fG2U3kulIE8EqDfHzPHKYZ# show system deployments
NAME ID STATE
-----
a5fG2U3kulIE8EqDfHzPHKYZ_vEdge.vEdge-vEdge 6 running
a5fG2U3kulIE8EqDfHzPHKYZ# vmConsole a5fG2U3kulIE8EqDfHzPHKYZ_vEdge.vEdge-vEdge
Connected to domain a5fG2U3kulIE8EqDfHzPHKYZ_vEdge.vEdge-vEdge
Escape character is ^]
viptela 18.3.0
Site001 login: admin
Password:
Welcome to Viptela CLI
admin connected from 127.0.0.1 using console on Canada_Site001
Site001#
```

Step 2 Check the status of control connection, using the following command:

```
show control connections

Site001# show control connections
PEER PEER CONTROLLER
PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP
TYPE PROT SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR PROXY STATE UPTIME ID
```

```

vbond dtls 0.0.0.0 0 0 <vbond IP> 12346 5<vbond ip> 12346 default - connect 0
Site001#
Site001# show control connections
Site001#

```

If nothing shows up in the output, it shows that the vEdge is unable to establish dtls connection to vBond.

Step 3 To check why the connection has not been established, use the following command.

```
show control connections-history
```

```

Site001# show control connections-history
Legend for Errors
ACSRREJ - Challenge rejected by peer. NOVCMCFG - No cfg in vmanage for device.
BDSGVERFL - Board ID Signature Verify Failure. NOZTPEN - No/Bad chassis-number entry in ZTP.
BIDNTPR - Board ID not Initialized. OPERDOWN - Interface went oper down.
BIDNTVRFD - Peer Board ID Cert not verified. ORPTMO - Server's peer timed out.
BIDSIG - Board ID signing failure. RMGSPR - Remove Global saved peer.
CERTEXPRD - Certificate Expired RXTRDWN - Received Teardown.
CRTREJSER - Challenge response rejected by peer. RDSIGFBD - Read Signature from Board ID failed.
CRTVERFL - Fail to verify Peer Certificate. SERNTPRES - Serial Number not present.
CTORGNMIS - Certificate Org name mismatch. SSLNFAIL - Failure to create new SSL context.
DCONFAIL - DTLS connection failure. STNMODETD - Teardown extra vBond in STUN server mode.
DEVALC - Device memory Alloc failures. SYSIPCHNG - System-IP changed.
DHSTMO - DTLS HandShake Timeout. SYSPRCH - System property changed
DISCVBD - Disconnect vBond after register reply. TMRALC - Timer Object Memory Failure.
DISTLOC - TLOC Disabled. TUNALC - Tunnel Object Memory Failure.
DUPCLHELO - Recd a Dup Client Hello, Reset G1 Peer. TXCHTOBD - Failed to send challenge to BoardID.
DUPSER - Duplicate Serial Number. UNMSGBDRG - Unknown Message type or Bad Register msg.
DUPSYSIPDEL- Duplicate System IP. UNAUTHHEL - Recd Hello from Unauthenticated peer.
HAFAIL - SSL Handshake failure. VBDEST - vDaemon process terminated.
IP_TOS - Socket Options failure. VECRTREV - vEdge Certification revoked.
LISFD - Listener Socket FD Error. VSCRTREV - vSmart Certificate revoked.
MGRTBLCKD - Migration blocked. Wait for local TMO. VB_TMO - Peer vBond Timed out.
MEMALCFL - Memory Allocation Failure. VM_TMO - Peer vManage Timed out.
NOACTVB - No Active vBond found to connect. VP_TMO - Peer vEdge Timed out.
NOERR - No Error. VS_TMO - Peer vSmart Timed out.
NOSLPRCRT - Unable to get peer's certificate. XTVMTRDN - Teardown extra vManage.
NEWVBNOVMNG- New vBond with no vMng connections. XTVSTRDN - Teardown extra vSmart.
NTPRVMIINT - Not preferred interface to vManage. STENTRY - Delete same tloc stale entry.
EMBARGOFAIL - Embargo check failed

PEER PEER
PEER PEER PEER SITE DOMAIN PEER PRIVATE PEER PUBLIC LOCAL REMOTE REPEAT
TYPE PROTOCOL SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR STATE ERROR ERROR COUNT
DOWNTIME

```

```

vbond dtls 0.0.0.0 0 0 <vbond IP> 12346 52.206.47.80 12346 default connect DCONFAIL NOERR 14
2018-09-06T16:44:56+0000
Site001#

```

As seen above, the LOCAL ERROR is mostly "DCONFAIL" which means DTLS connection failure. This happens when the vEdge is unable to reach the vBond either due to network connectivity issues or firewall is blocking the DTLS connection. For an understanding of other reachability errors, see the [Cisco SD-WAN knowledge base](#).

Troubleshooting ENCS Reachability Issues

If the ENCS device is unreachable or unavailable, then do the following:

Step 1 Log into the ENCS box. Use SSH to connect to the ENCS box.

```
ssh <username>@<management IP address>
```

Step 2 Do the following on the ENCS box:

a. Enter the configuration mode.

```
config
```

b. Revert the IP to the WAN interface of the ENCS, if the ENCS was set in the single IP mode.

```
no single-ip-mode
```

c. Remove the VPN configurations.

```
no secure-overlay
```

d. Remove all deployments.

```
no vm_lifecycle tenants tenant admin deployments deployment
```

Note If a specific VNF needs to be deleted, enter the deployment name in the above command.

e. Removes all images.

```
no vm_lifecycle images image
```

Note If a specific image needs to be deleted, enter the image name in the above command.

f. Save the changes and exit the configuration mode.

```
commit and-quit
```

g. Restarts PNP process.

```
pnp action command restart
```

Changing MSX Trace Logging Level During Runtime

Using the procedure in this section you can change any MSX trace logging level during the runtime. The following shows SD-WAN log definition in logback.xml.

```
<property name="LOG_FILE" value="logs/sdwanservice.log"/>

<!-- the rollover settings with mean a max size per log of 100Mb and 7 days -->
<property name="MAX_HISTORY" value="7"/>
<property name="MAX_FILE_SIZE" value="100MB"/>

<include resource="com/cisco/nfv/logging/nfv_base_logback.xml"/>
```

```

<!-- the specific loggers -->
<logger name="com.cisco.phiservice" level="DEBUG"/>
<logger name="com.cisco.vms.sdwan.service" level="DEBUG"/>
<logger name="com.cisco.vms.sdwan.service.integration.viptela" level="DEBUG"/>
<logger name="com.cisco.vms.svcpack.logging" level="DEBUG"/>

<logger name="org.springframework" level="INFO"/>
<logger name="org.springframework.security.oauth2" level="INFO"/>
<logger name="org.springframework.integration" level="OFF"/>
<logger name="org.springframework.oauth" level="OFF"/>
<logger name="org.springframework.http" level="ERROR"/>

```

To change the logging level during runtime:

Step 1 Obtain the MSX client credentials.

Use the credential you use for logging in to the MSX Portal. If you do not have these credentials, contact your Service Provider Administrator.

Step 2 Obtain an access token from the MSX authorization Server. Use the following curl command to get the access token. Use the following curl command to get the access token.

```

curl -X POST 'https://<MSX_URL>/idm/v2/token?grant_type=password' -H 'Authorization: Basic
<MSX_BASIC_AUTH>' \
-H 'Content-Type: application/x-www-form-urlencoded' \
-H 'cache-control: no-cache' \
-d 'username=<MSXportal_username>&password=<MSXportal_password>'

```

Where:

- Replace <MSX_URL> by real MSX URL
- Replace <MSX_BASIC_AUTH> with real value of the Authorization of clientID and clientSecret, which is base64 of “clientID:clientSecret”. User defined their OAuth2 Authentication clientID and clientSecret in Settings > BSS Integration > REST Configuration
- Replace <MSXportal_username> by Portal username
- Replace <MSXportal_password> by Portal password

Step 3 Check the current package logging level. Use the following curl command to check the current package log level:

```

curl -X GET https://<MSX_URL>/<service>/admin/loggers/<package> -H 'Authorization: Bearer
<access_token>' \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache'

```

Where:

- Replace <MSX_URL> by real MSX URL
- Replace <service> by service endpoint (For example: sdwan.service)
- Replace <package> by real package name (For example: com.cisco.vms.sdwan.service.integration.viptela)
- Replace <access_token> from Step 2.

Step 4 Change the package logging level. Use the following curl command to update the package log level:

```
curl -X POST https://<MSX_URL>/<service>/admin/loggers/<package> -H 'Authorization: Bearer
<access_token>' \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d '{
  "configuredLevel": "<LOG_LEVEL>"
}'
```

Where:

- Replace <MSX_URL> by real MSX URL
- Replace <service> by service endpoint (for example: sdwanservice)
- Replace <package> by real package name (for example: com.cisco.vms.sdwanservice)

Note This package name does not necessarily be defined in logback.xml, as long as this package exists in the source code.

- Replace <access_token> from Step 2.
- Replace <LOG_LEVEL> by log level you want to set.

Step 5 Verify the changes in package logger logging level. Repeat Step 3. Use the following curl command to verify the log level after the changes:

```
curl -X GET http://<MSX_URL>/<service>/admin/loggers/<package> -H 'Authorization: Bearer
<access_token>' \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache'
# with output for logging level
{"configuredLevel":"TRACE","effectiveLevel":"TRACE"}
```

Where:

- Replace <MSX_URL> by real MSX URL
- Replace <service> by service endpoint (for example: sdwanservice)
- Replace <package> by real package name

Troubleshooting Control Plane

Troubleshooting Control Plane on OpenStack

If MSX is unable to reach the OpenStack control plane, then it should be due to some issues pertaining to proxy settings.



Note When both MSX and OpenStack cloud are on the corp network, proxy is not required. Ensure that the vManage IP address is added to the "no proxy" list in the "sdwanservice-rc.yml" and then restart the SD-WAN pod.

This figure shows the list of Get APIs that can be used to query the database.

Figure 41: List of Get APIs for Querying the Database

osorch		Show/Hide	List Operations	Expand Operations
GET	/osorch/alive			Check if system is alive
GET	/osorch/v1/vims			Get all VIMs
GET	/osorch/v1/vims/{vimID}			Get a VIM
GET	/osorch/v1/vims/{vimID}/validate			Check a VIM config
GET	/osorch/v1/vims/{vimID}/flavors			Get a list of flavors on a VIM
GET	/osorch/v1/vims/{vimID}/flavors/{flavorName}			Get a Flavor
GET	/osorch/v1/vims/{vimID}/images			Get a list of images on a VIM
GET	/osorch/v1/vims/{vimID}/images/{imageName}			Get an image
GET	/osorch/v1/vims/{vimID}/volumes			Get a list of volumes on a VIM
GET	/osorch/v1/vims/{vimID}/volumes/{volumeName}			Get an volume
GET	/osorch/v1/cps			Get all Control Planes
GET	/osorch/v1/cps/{cpID}			Get a Control Plane
GET	/osorch/v1/jobs			Get all Jobs
GET	/osorch/v1/jobs/{jobID}			Get a Job by ID
GET	/osorch/v1/templates			List all the Ansible templates
GET	/osorch/v1/templates/{templateName}			Get a Template by Name

This figure shows a sample query to access the list of templates from the OS orchestrator using the curl command in this GET API page

Figure 42: Accessing the List Templates from OS Orchestrator

GET /osorch/v1/templates List all the Ansible templates

Parameters

Parameter	Value	Description	Parameter Type	Data Type
Authorization	Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ1b3RlcnR5bG9ja3V1IiwiaWF0IjoiMTY1MjY1MjY1IiwiaWF0IjoiMTY1MjY1MjY1In0	JWT token in the form 'Bearer {token}'. Tokens are retrieved by making a login call to the platform.	header	string

Response Messages

HTTP Status Code	Reason	Response Model	Headers
200	OK		
500	Internal Error		

default
[Try it out!](#) [Hide Response](#)

Curl

```
curl -X GET --header 'Accept: application/json' --header 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJ1b3RlcnR5bG9ja3V1IiwiaWF0IjoiMTY1MjY1MjY1IiwiaWF0IjoiMTY1MjY1MjY1In0'
```

Request URL

```
https://ssi-sdwan.lab.ciscomsx.com:443/osorch/v1/templates
```

Response Body

```
[
  "ca-csr.json",
  "ca.j2",
  "clouds.j2",
  "controllers.yml.tpl",
  "hosts.j2",
  "ntp.j2",
  "openstack.yml.tpl",
  "ports.j2",
  "ports.yml.tpl",
  "vbond-fip-3-noCA.j2",
  "vbond-fip-3.j2",
  "vmanage-fip-noCA.j2",
  "vmanage-fip.j2",
  "vmanage-new-2.j2",
  "vsmart-fip-noCA.j2",
  "vsmart-fip.j2",
  "vsmart.j2"
]
```

Troubleshooting the OS orchestrator Logs

To access the OS orchestrator logs:

-
- Step 1** Log in to the Kubernetes-master mode.
- Step 2** Execute the given command to get the OS orchestrator pod name:
- ```
kubectl -n vms get po
```
- Step 3** To log in to the container, execute the given command:
- ```
kubectl -n vms exec -it <osorch_log_name> bash
```
- Step 4** To check the logs, execute the given command:
- ```
cd logs >
<jobID>_ansible.log
```

jobID: Specifies the job ID to access the specific job.

If there are errors during the creation of a control plane these logs can offer some guidance, it verifies the incorrect parameters and ways to resolve issues.

## Change Control Plane Password or Vault Failures

### Error Message

Failed to authenticate control plane user.

### Solution

Use the Swagger interface to update the credentials for the control plane manager. The password input in base64.

*Figure 43: Changing the Control Plane Password*

**PUT** /v1/controlplanemanager/{id}/credentials

**Implementation Notes**  
Update tenant control plane credentials in VMS system

**Parameters**

| Parameter           | Value                                                            | Description                   |
|---------------------|------------------------------------------------------------------|-------------------------------|
| id                  | 0693072f-d25d-487c-89de-6dc10acf919c                             | VMS tenantId                  |
| controlPlaneCredDTO | {<br>"password": "dGFJdHJhaW5pbmc=",<br>"username": "admin"<br>} | SD-WAN Control Plane Cred DTO |

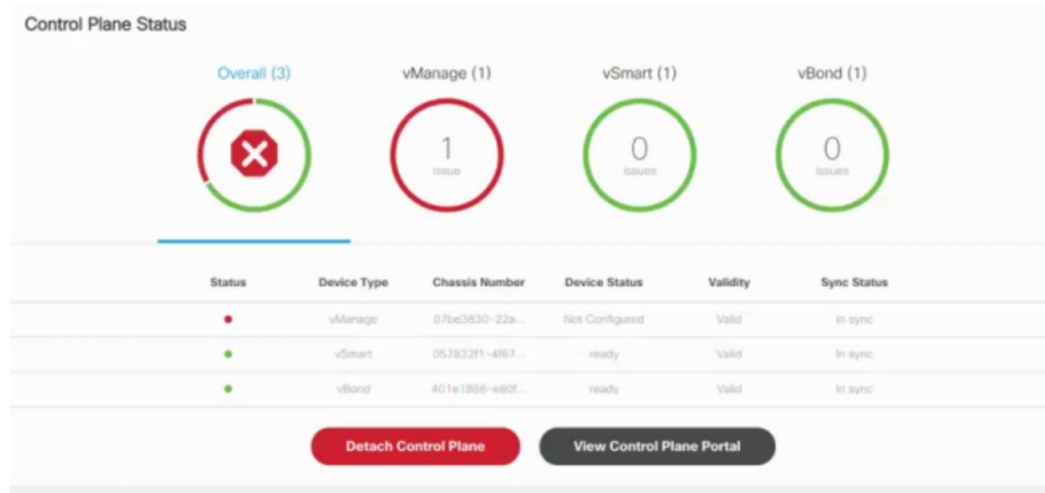
## Fixing Control Plane Device Status State

### Problem

After adding a new control plane, the Control Plane (vManage) remains in 'Not Configured' state, as shown below:



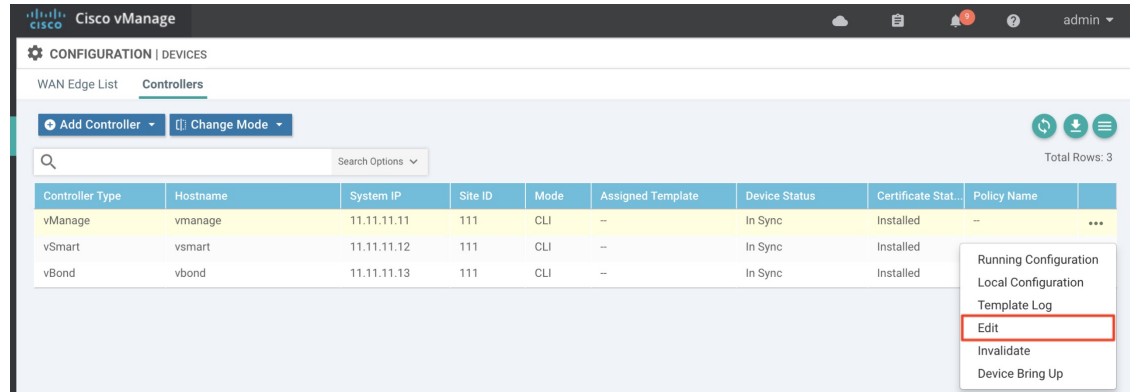
Figure 44: Control Plane Status



Reason

Incorrect way of changing the control plane password. This issue was due to changing the Control Plane password from vManage Console > Configuration > Devices > Controllers.

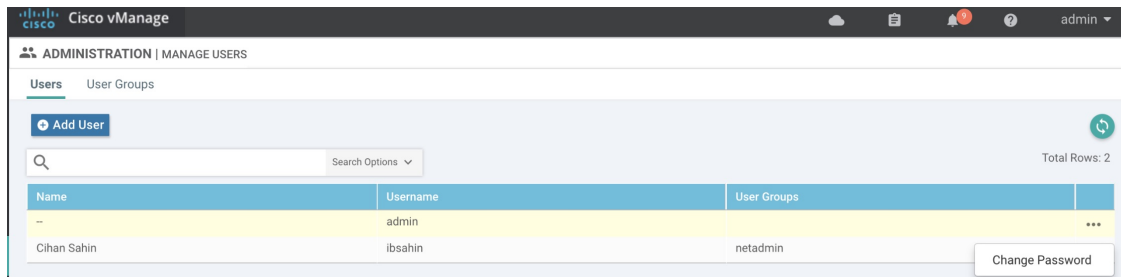
Figure 45: Changing the Control Plane Password from vManage



Solution

**Step 1** Change the Control Plane password from vManage Console > Administration > Manage Users > Users.

Figure 46: Changing the Control Plane Password from vManage



**Step 2** Restart nms application server on vManage.

```
vmmanage# request nms application-server restart
```

**Note** The server takes a few minutes to start.

## Data Plane Troubleshooting

Check the deployment status of the vEdge device:

1. Check NSO device status.
2. Check data plane deployment in the MSX Portal.

Check the reachability status (vEdge to control plane):

1. Check the vManage device state.
2. Check that the site status in SD-WAN is green.

## Data Plane Deployment Status: NSO Device Status

Example:

```
vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe agH89ZqVcqVObcI6Pyv1jU56 plan
component state
NAME STATE STATUS WHEN ref MESSAGE

self init reached 2017-11-12T04:55:12 -
ready reached 2017-11-12T04:57:33 -
agH89ZqVcqVObcI6Pyv1jU56 init reached 2017-11-12T04:55:12 -
pnp-callhome reached 2017-11-12T04:55:12 -
ready reached 2017-11-12T04:56:10 - Ready
vEdge_SD-Branch-vEdge init reached 2017-11-12T04:56:11 -
ready reached 2017-11-12T04:56:34 - Ready
vEdge_agH89ZqVcqVObcI6Pyv1jU56 init reached 2017-11-12T04:56:35 -
vm-deployed reached 2017-11-12T04:56:50 -
vm-alive reached 2017-11-12T04:57:33 -
ready reached 2017-11-12T04:57:33 - Ready
```

## Data Plane Deployment Status (MSX Portal)

To view the data plane deployment status:

- Step 1** Log in to the Cisco MSX Portal.
- Step 2** In the main menu, click Dashboard.
- Step 3** Select the tenant from the drop-down.
- Step 4** Click SD-WAN. The SD-WAN Service Offer screen appears.
- Step 5** Click SD-WAN.
- Step 6** Select the SD-WAN service. The SD-WAN screen appears.

## Reachability Status: vManage Device State

To view the reachability status:

**Step 1** Log in to vManage.

**Step 2** In vManage, choose Configuration > Devices. The Configure | Devices window is displayed.

**Figure 47: Reachability Status of the Devices**

| State | Device Model | Chassis Number                        | Serial No./Token         | Hostname      | System IP | Site ID |                       |
|-------|--------------|---------------------------------------|--------------------------|---------------|-----------|---------|-----------------------|
| 🟢     | vEdge Cloud  | 104920e9-ee97-4f98-88d3-b385acbb03... | Token - 2fb5defbdabef... | -             | -         | -       | Running Configuration |
| 🟢     | vEdge Cloud  | 8b57277e-7790-4826-b85c-763a558ee...  | Token - 9380b5a8929c...  | -             | -         | -       | Local Configuration   |
| 🟡     | vEdge Cloud  | 3aca2c89-6b97-4fc8-a741-be48ff5c448   | Token - aa52101a1dc5...  | -             | -         | -       | Delete vEdge          |
| 🟢     | vEdge Cloud  | e887118a-c434-46ab-9957-068c38cc6...  | Token - c8423a838bd2...  | Gap50         | 1.1.1.22  | 222     | Copy Configuration    |
| 🟡     | vEdge Cloud  | 346389cf-4009-4ca4-81a3-508e378ae2... | Token - 772422fc175d5... | -             | -         | -       | Decommission vEdge    |
| 🟢     | vEdge Cloud  | e0b0477b-9e4d-4832-8bdf-af6ae1e70e... | Token - d093d134d909...  | -             | -         | -       | Template Log          |
| 🟡     | vEdge Cloud  | 159483d1-d488-4116-bc05-1f30c88fe0... | c2620faa                 | DhruvSite     | 1.1.1.99  | 222     | CLI                   |
| 🟢     | vEdge Cloud  | 0bf3774-0825-4591-b095-a1d97d6b33...  | Token - cb8b37d7661ff... | montrealadwan | 1.1.1.14  | 567     | CLI                   |
| 🟢     | vEdge Cloud  | 6978c2a4-8f5e-4489-8500-80e8048f60... | f44d3aee                 | -             | -         | -       | CLI                   |
| 🟢     | vEdge Cloud  | 34e8f7dc-288c-4c90-a06d-86719d818a... | Token - 6f76d6ec5bfe3... | -             | -         | -       | CLI                   |

- The State column indicates if the certificate is installed.
- In the Serial No./Token column, you should have a serial number and not a token.
- Click Running Configuration to view the configuration running on the device.
- If reachability is not achieved, then verify the variables that were passed during the site deployment (especially VPN\_0).

## Data Plane Reachability Status (MSX Portal)

To view the data plane reachability status:

**Step 1** Log in to the Cisco MSX Portal.

**Step 2** In the main menu, click Dashboard.

**Step 3** Select the tenant from the drop-down.

**Step 4** Click SD-WAN. The SD-WAN Service Offer screen appears.

**Step 5** Click SD-WAN.

**Step 6** Select the SD-WAN service. The SD-WAN screen appears.

## PnP Server Troubleshooting Commands

### List of Devices in Contact with the PnP Server

```
admin@ncs-sm-SD-Branch> show pnp list
SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT

FTX1738AJME 173.36.207.85 true true true 2017-10-24 23:44:44
FTX1738AJMG 173.36.207.81 true true true 2017-10-24 23:43:50
FTX1740ALBX 173.36.207.80 true true true 2017-10-24 23:44:21
SSI184904LG 173.36.207.82 true true true 2017-10-24 23:43:56
SSI185104LT 173.36.207.84 true true true 2016-10-24 23:43:57
[ok] [2016-10-24 23:45:49]
```



#### Note

- The Last Contact column displays the last date and time when the PnP server was in contact with the CPE. If the CPE has not been in recent contact with the PnP server, it may be due to connectivity or reachability issues between the PnP server and the CPE.
- Identify the active NSO instance using the following command:

```
curl -v http://consul.service.consul:8500/v1/catalog/service/nso-ha | python -m json.tool
```

### CPE in Contact with the PnP Server (Without a Service)

```
admin@ncs-sm-SD-Branch> show branch-infra:branch-infra branch-cpe
%No entries found
[ok] [2016-10-24 23:45:49]
```

### CPE in Contact with the PnP Server (With a Service)

```
admin@ncs-sm-SD-Branch> show branch-infra:branch-infra-status branch-cpe
amXqvXDO9zW2IZ1eho2cOBrD plan component state status
NAME STATE STATUS

self init reached
 ready reached
amXqvXDO9zW2IZ1eho2cOBrD init reached
 pnp-callhome reached
 ready reached
[ok] [2017-10-25 14:20:40]
```

### CPE in Contact with the PnP Server (Detailed)

```
vmsnso@ncs> show branch-infra:branch-infra-status branch-cpe amXqvXDO9zW2IZ1eho2cOBrD plan
component
plan component self
type self
```

```

state init
 status reached
 when 2017-10-25T14:15:20
 message ""
state ready
 status reached
 when 2017-10-25T14:16:57
 message ""
real-name amXqvXDO9zW2IZleho2cOBrD
plan component amXqvXDO9zW2IZleho2cOBrD
type branch-cpe
state init
 status reached
 when 2017-10-25T14:15:20
 message ""
state pnp-callhome
 status reached
 when 2017-10-25T14:16:22
 message ""
state ready
 status reached
 when 2017-10-25T14:16:57
 message Ready
real-name amXqvXDO9zW2IZleho2cOBrD
provider CiscoSystems
device amXqvXDO9zW2IZleho2cOBrD_ENCS
[ok][2017-10-25 14:23:10]

```

## View CPE Details

```

vmsnso@ncs> show pnp list

SERIAL IP ADDRESS CONFIGURED ADDED SYNCED LAST CONTACT

FGL21388017 10.85.189.20 true true true 2017-10-25 14:24:07
FGL2138801A 10.85.189.23 false false false 2017-10-25 14:21:16
FGL2138801E 10.85.189.24 false false false 2017-10-25 14:21:40

[ok][2017-10-25 14:24:20]
vmsnso@ncs> configure

Entering configuration mode private
[ok][2017-10-25 14:24:31]

[edit]
vmsnso@ncs% show branch-infra:branch-infra branch-cpe serial FGL21388017
branch-cpe amXqvXDO9zW2IZleho2cOBrD {
 provider CiscoSystems;
 type ENCS;
 serial FGL21388017;
 var SD-Branch_DEVICE_TYPE {
 val ENCS;
 }
 var contact {
 val Customer;
 }
 var email {
 val abc@example.ocm;
 }
 var phone {
 val null;
 }
}

```

```
[ok] [2017-10-25 14:24:34]
[edit]
vmsnso@ncs% exit
[ok] [2017-10-25 14:24:53]
```

## IPsec Tunnel Cannot be Established

### Problem

Device fails to establish secure VPN tunnel between NFVIS and CSR Mgmt hub router.

### Solution

To establish secure VPN tunnel:

**Step 1** Log in to the device and run the following command:

#### Example:

```
vmsnso@ncs% show pnp day0-common | display set
```

**Step 2** Ensure day0-common has correct values specified for the following parameters:

#### Example:

```
INT_MGMT_SUBNET_DHCP set to false
INT_MGMT_SUBNET_GW <GW IP address>
INT_MGMT_SUBNET_INVERSE_MASK <subnet mask>
INT_MGMT_SUBNET_IP <subnet value>
INT_MGMT_SUBNET_IPVERSION <IPv4 or ipv6>
INT_MGMT_SUBNET_NETMASK <subnet netmask value>
LOCAL_PRESHARED_KEY <Pre-shared key for VPN authentication on the ENCS>
MGMT_HUB_OVERLAY_IP_ADDR <IP address of the interface connecting to MSX internal host on the CSR mgmt
hub>
MGMT_HUB_OVERLAY_NET <Supernet of the subnets on MSX side>
MGMT_HUB_IP <Public IP address of the CSR mgmt hub>
REMOTE_ID <Local identity configured on the CSR mgmt hub's VPN configuration>
REMOTE_PRESHARED_KEY <Pre-share key for VPN authentication on the CSR mgmt hub>
SECURE_OVERLAY_NAME
SOURCE-BRIDGE
```

**Step 3** Ensure CSR Hub VPN configuration matches NFVIS's.

**Step 4** Edit CSR Hub's Security group and ensure the following ports are open. The following ports are used for communication from MSX to the NFVIS via the CSR mgmt hub VPN.

- 22022 - 22024: VNF ports
- 21045: VNF port
- 830: Netconf port
- 443: Metric collection from the ENCS

Figure 48: Editing the Security Group

The screenshot shows the AWS IAM console interface for managing security groups. At the top, there is a 'Create Security Group' button and an 'Actions' dropdown menu. Below this is a search bar with the text 'Filter by tags and attributes or search by keyword'. A table lists several security groups with columns for Name, Group ID, Group Name, VPC ID, and Description. The 'csr-mgmt-hub' security group is selected, indicated by a blue checkmark in the first column. Below the table, the details for the selected security group 'sg-05fd38052c97f62ab' are shown, including tabs for 'Description', 'Inbound', 'Outbound', and 'Tags'. The 'Inbound' tab is currently active, and an 'Edit' button is visible below the tabs.

| <input type="checkbox"/>            | Name | Group ID             | Group Name   | VPC ID                | Description                  |
|-------------------------------------|------|----------------------|--------------|-----------------------|------------------------------|
| <input type="checkbox"/>            |      | sg-00bc5bdf4f60205e0 | dataplatfrom | vpc-0e764a8c99a7630d6 | data platform security group |
| <input type="checkbox"/>            |      | sg-0120a624c4fe920bf | k8s-nodes    | vpc-0e764a8c99a7630d6 | k8s-nodes security group     |
| <input type="checkbox"/>            |      | sg-047b5dfa7bbf7fe54 | default      | vpc-07225c7e3415a9f64 | default VPC security group   |
| <input type="checkbox"/>            |      | sg-057c1ab78e44e682e | k8s-masters  | vpc-0e764a8c99a7630d6 | k8s-masters security group   |
| <input checked="" type="checkbox"/> |      | sg-05fd38052c97f62ab | csr-mgmt-hub | vpc-0e764a8c99a7630d6 | csr-mgmt-hub security group  |

**Step 5** Configure route to NFVIS's secure IP. The default is 10.128.0.0/16 (Assigned by SD-Branch). This can be changed using:

- SD-Branch\_variables.yml file at the install time
- SD-Branch settings API







## APPENDIX **B**

# Troubleshooting Cisco Meraki SD-WAN Issues

This section describes problems, possible causes, and recommended actions that you may encounter in Cisco Meraki SD-WAN deployments.

- [Handling Meraki Rate Limiting Issue on MSX, on page 129](#)
- [Checking Meraki Beat, on page 130](#)
- [Checking Device Status, on page 130](#)
- [Checking Device Connections, on page 134](#)

## Handling Meraki Rate Limiting Issue on MSX

### Error Message

Http Error 429: This error code indicates that you have submitted more than 5 API calls in one second to the Meraki system, triggering the rate limit. Meraki Dashboard API has a rate-limiting of 5 API calls per second per organization.

### Solution

Modify the rate-limiting parameters through consul. Before you modify, make sure you have API access keys for Meraki. For more information, see [Managing Meraki Traffic Class Access for Tenants](#).

The following are the parameters that need to be modified:

- `meraki.ratelimit.max.attempts`: Use this parameters to configure the maximum attempts allowed for Meraki. Use the following command to configure this parameter. Run this curl command on the master Kubernetes node.

```
curl -s -k -X 'x-consul-token: <consul token>' PUT -H "Content-Type: application/json"
-d "<Number of retries>"
https://consul.service.consul:8500/v1/kv/userconfiguration/sdwanservice/meraki.ratelimit.max.attempts
| python -mjson.tool
```

- `meraki.ratelimit.backoff`: Use this parameter to retry the Meraki request after a specified backoff time. Use the following command to configure this parameter. Run this curl command on the master Kubernetes node.

```
curl -s -k -X 'x-consul-token<consul-token>' PUT -H "Content-Type: application/json"
-d "<Backoff in milliseconds>"
https://consul.service.consul:8500/v1/kv/userconfiguration/sdwanservice/meraki.ratelimit.backoff
| python -mjson.tool
```



**Note** Replace {consul-token} with your actual consul token value from the passwords.yml file.

## Checking Meraki Beat

Use the following endpoint to check if Meraki beat is up and running:

**<IP\_address>3441/admin/health**

Where:

<IP\_address> is the IP address of the Meraki system.

Response:

```
{"description": " metrics collector", "status": "UP"}description
```

If status is not Up, use the instructions in the deployment log to bring Meraki Beat up and running in kubernetes node. Check deployment logs for more information.

## Checking Device Status

### Checking Meraki Device Health

Use the following POST API to return all the query templates related to devices.

**POST /api/v2/querytemplates/device**

**Response:**

```
{
 "success": true,
 "responseObject": [
 {
 "type": "*",
 "profile": "*",
 "specificType": "*",
 "templateName": "query-ping-availability",
 "queryTemplate": "{\"query\": {\"bool\": {\"filter\": [{\"term\": {\"deviceId\": {\"value\": \"{{deviceId}}\"}}, {\"range\": {\"@timestamp\": {\"gte\": \"{{timestamp_gte}}\", \"lte\": \"{{timestamp_lte}}\"}}]}}, \"aggs\": {\"{{statusInterval}}\": {\"date_histogram\": {\"field\": \"@timestamp\", \"interval\": \"{{statusInterval}}\", \"aggs\": {\"status\": {\"bucket_script\": {\"buckets_path\": {\"tot\": \"_count\", \"success\": \"count_success\"}, \"script\": \"def threshold = 0.5; if (params.success / params.tot > threshold) {return 1} else {return 0}\"}}, \"count_success\": {\"sum\": {\"script\": \"return doc['up'].value == true ? 1 : 0\"}}}}, \"size\": 0}}\",
 "indices": [
 "heartbeat-*"
]
 },
 {
 "type": "*",
 "profile": "*",
 "specificType": "*",
 "templateName": "query-snmp-availability",
 "queryTemplate": "{\"query\": {\"bool\": {\"filter\": [{\"term\": {\"deviceId\": {\"value\": \"{{deviceId}}\"}}, {\"range\": {\"@timestamp\": {\"gte\": \"{{timestamp_gte}}\", \"lte\": \"{{timestamp_lte}}\"}}]}}, \"aggs\": {\"{{statusInterval}}\": {\"date_histogram\": {\"field\": \"@timestamp\", \"interval\": \"{{statusInterval}}\", \"aggs\": {\"status\": {\"bucket_script\": {\"buckets_path\": {\"fail\": \"count_fail\", \"tot\": \"_count\"}, \"script\": \"def threshold = 0.5; if ((params.tot - params.fail) / params.tot > threshold)
```

```

 {return 1} else {return 0}\"}}, \count_fail\": {\value_count\": {\field\":
\Failed\"}\}}}, \size\": 0}",
 "indices": [
 "snmpbeat-*"
]
 },
 {
 "type": "CPE",
 "profile": "sdwan",
 "specificType": "MERAKE",
 "templateName": "meraki-device-status",
 "queryTemplate": "{\sort\": [{\timestamp\": {\order\": \desc\}}], \query\":
{\bool\": {\filter\": [{\term\": {\deviceId\": {\value\": \{{deviceId}}\}}],
{\range\": {\timestamp\": {\gte\": \{{timestamp_gte}}\", \lte\":
{\timestamp_lte}}\}}], {\bool\": {\must\": [{\exists\": {\field\":
\DeviceHealth\}}\}}\}}}, \aggs\": {\{{statusInterval}}\": {\date_histogram\": {\field\":
\timestamp\, \interval\": \{{statusInterval}}\", \aggs\": {\status\":
{\bucket_script\": {\buckets_path\": {\total\": _count\, \deviceHealthSum\":
\deviceHealthSum\}, \gap_policy\": \insert_zeros\, \script\": \(params.deviceHealthSum
/ params.total >= 0.5) ? 1 : 0\}}, \deviceHealthSum\": {\sum\": {\script\": \return
doc['DeviceHealth.status'].value == 'offline' ? 0 : doc['DeviceHealth.status'].value ==
'online' ? 1 : 'undefined'\}}\}}}, \size\": 1}",
 "indices": [
 "merakibeat-*"
]
 }
],
 "command": "Get all device health query templates",
 "parms": {},
 "httpStatus": "OK",
 "message": "Get all device health query templates",
 "errors": [],
 "throwable": null
}

```

**Problem:** If meraki-device-status does not exist in the response, it means there were issues in deployment and query templates were not pushed properly.

**Solution:** Use the following API:

#### **POST [api/v2/querytemplates/device](#)**

Response:

```

{
 "type": "CPE",
 "profile": "sdwan",
 "specificType": "MERAKE",
 "templateName": "meraki-device-status",
 "queryTemplate": "{\sort\": [{\timestamp\": {\order\": \desc\}}], \query\":
{\bool\": {\filter\": [{\term\": {\deviceId\": {\value\": \{{deviceId}}\}}],
{\range\": {\timestamp\": {\gte\": \{{timestamp_gte}}\", \lte\":
{\timestamp_lte}}\}}], {\bool\": {\must\": [{\exists\": {\field\":
\DeviceHealth\}}\}}\}}}, \aggs\": {\{{statusInterval}}\": {\date_histogram\": {\field\":
\timestamp\, \interval\": \{{statusInterval}}\", \aggs\": {\status\":
{\bucket_script\": {\buckets_path\": {\total\": _count\, \deviceHealthSum\":
\deviceHealthSum\}, \gap_policy\": \insert_zeros\, \script\": \(params.deviceHealthSum
/ params.total >= 0.5) ? 1 : 0\}}, \deviceHealthSum\": {\sum\": {\script\": \return
doc['DeviceHealth.status'].value == 'offline' ? 0 : doc['DeviceHealth.status'].value ==
'online' ? 1 : 'undefined'\}}\}}}, \size\": 1}",
 "indices": [
 "merakibeat-*"
]
}

```

## Checking Device Status for a Specific Service ID

Use the following end point to get the statuses of the devices for a specific service ID:

**GET /api/v1/status/service/{serviceId}/devices**

Response:

```
{
 "statusData": [{
 "id": "<Device ID 1>",
 "locationId": null,
 "name": "127.0.0.1",
 "operationalState": "up",
 "parentId": null,
 "topLevelServiceId": "<Service ID>",
 "type": "CPE"
 },
 {
 "id": "<Device ID 2>",
 "locationId": null,
 "name": "127.0.0.1",
 "operationalState": "up",
 "parentId": null,
 "topLevelServiceId": "<Service ID>",
 "type": "CPE"
 },
 {
 "id": "<Device ID 3>",
 "locationId": null,
 "name": "127.0.0.1",
 "operationalState": "down",
 "parentId": null,
 "topLevelServiceId": "<Service ID>",
 "type": "CPE"
 }
]
}
```

Problem: Device ID is returned empty, which indicates issue in metric collection.

Solution: In this case, run the following query for each device on Elastic Search:

```
{
 "query": {
 "bool": {
 "filter": [
 {
 "term": {
 "deviceId": {
 "value": "{{deviceId}}"
 }
 }
 },
 {
 "range": {
 "@timestamp": {
 "gte": "{{timestamp_gte}}",
 "lte": "{{timestamp_lte}}"
 }
 }
 }
],
 "must": [
 {

```

```

 "exists": {
 "field": "DeviceHealth"
 }
]
 }
],
 "sort": [
 {
 "@timestamp": {
 "order": "desc"
 }
 }
],
 "size": 1,
 "aggs": {
 "{{statusInterval}}": {
 "date_histogram": {
 "field": "@timestamp",
 "interval": "{{statusInterval}}"
 },
 "aggs": {
 "deviceHealthSum": {
 "sum": {
 "script": "return doc['DeviceHealth.status'].value == 'offline' ? 0 :
doc['DeviceHealth.status'].value == 'online' ? 1 : 'undefined'"
 }
 },
 "status": {
 "bucket_script": {
 "buckets_path": {
 "deviceHealthSum": "deviceHealthSum",
 "total": "_count"
 },
 "gap_policy": "insert_zeros",
 "script": "(params.deviceHealthSum / params.total >= 0.5) ? 1 0"
 }
 }
 }
 }
 }
} :[..

```

In the above query, provide the values for the following:

- timestamp\_gte
- timestamp\_lte
- statusInterval

Response:

```

"": {
 "": 1
}
0 Down
1 Up

```

## Checking Device Connections

Use the following endpoint to get all device connections:

**GET /manage/api/v2/devices/connections**

**Response:**

```
{
 "success": true,
 "command": "getAllDeviceConnections",
 "params": {
 "serviceInstanceId": null
 },
 "message": "getAllDeviceConnections succeeded",
 "responseObject": [
 {
 "deviceInstanceId": "<Device ID1>",
 "serviceInstanceId": "<Service ID1>",
 "tenantId": null,
 "name": null,
 "profile": "sdwan",
 "type": "CPE",
 "specificType": "MERAKI",
 "category": "CPE",
 "hostName": null,
 "ipAddress": "127.0.0.1",
 "serialKey": "<Device Serial Key>",
 "createdOn": "2020-02-18T10:33:44.849412",
 "createdBy": "operatorapi181027585e8c87a9",
 "modifiedOn": "2020-02-18T10:33:44.849412",
 "modifiedBy": "operatorapi181027585e8c87a9"
 },
 {
 "deviceInstanceId": "<Device ID2>",
 "serviceInstanceId": "Service ID2",
 "tenantId": null,
 "name": "aw9DpjAZShwiRwUrNbuMZtji",
 "profile": "vbranch",
 "type": "CPE",
 "specificType": "ENCS",
 "category": "CPE",
 "hostName": "aw9DpjAZShwiRwUrNbuMZtji",
 "ipAddress": "127.0.0.1",
 "serialKey": "<Device Serial Key>",
 "createdOn": "2020-02-18T10:34:17.223363",
 "createdBy": "system",
 "modifiedOn": "2020-02-18T10:34:17.223363",
 "modifiedBy": "system"
 }
],
 "httpStatus": "OK"
}
```

Make sure the device connection has been created for the device with the serial number.

Problem: Device connections are not returned in the response.

Solution: Create a device connection using the following API :

**POST /api/v2/devices/connections**

**Response:**

```
{
 "": "CPE",category
```

```
"": "CPE-<UUID>",deviceInstanceId
"": null,hostName
"": "127.0.0.1",ipAddress
"": null,name
"": " ",profilesDwan
"": "<Serial_Key>",serialKey
"": "<Service_instance_ID>",serviceInstanceId
"": " MERAKI",specificType
"": " CPE"type
}
```

The above endpoint response returns an entry for the device instance ID.







## APPENDIX **C**

# Applications Available with Cisco MSX SD-WAN

---

Cisco MSX allows you to set the application relevance for the applications in Cisco SD-WAN and Meraki SD-WAN managed sites. For more information, see [Cisco MSX SD-WAN and Meraki Out-of-the box Applications Addendum](#).





## APPENDIX **D**

# Out-of-the-Box Cisco SD-WAN Device Templates Available Within MSX

Cisco MSX provides out-of-the-box device templates. The details of these templates are provided in the figures below. You can export these templates to your tenants vManage and use them as is or modify them as per your requirements.

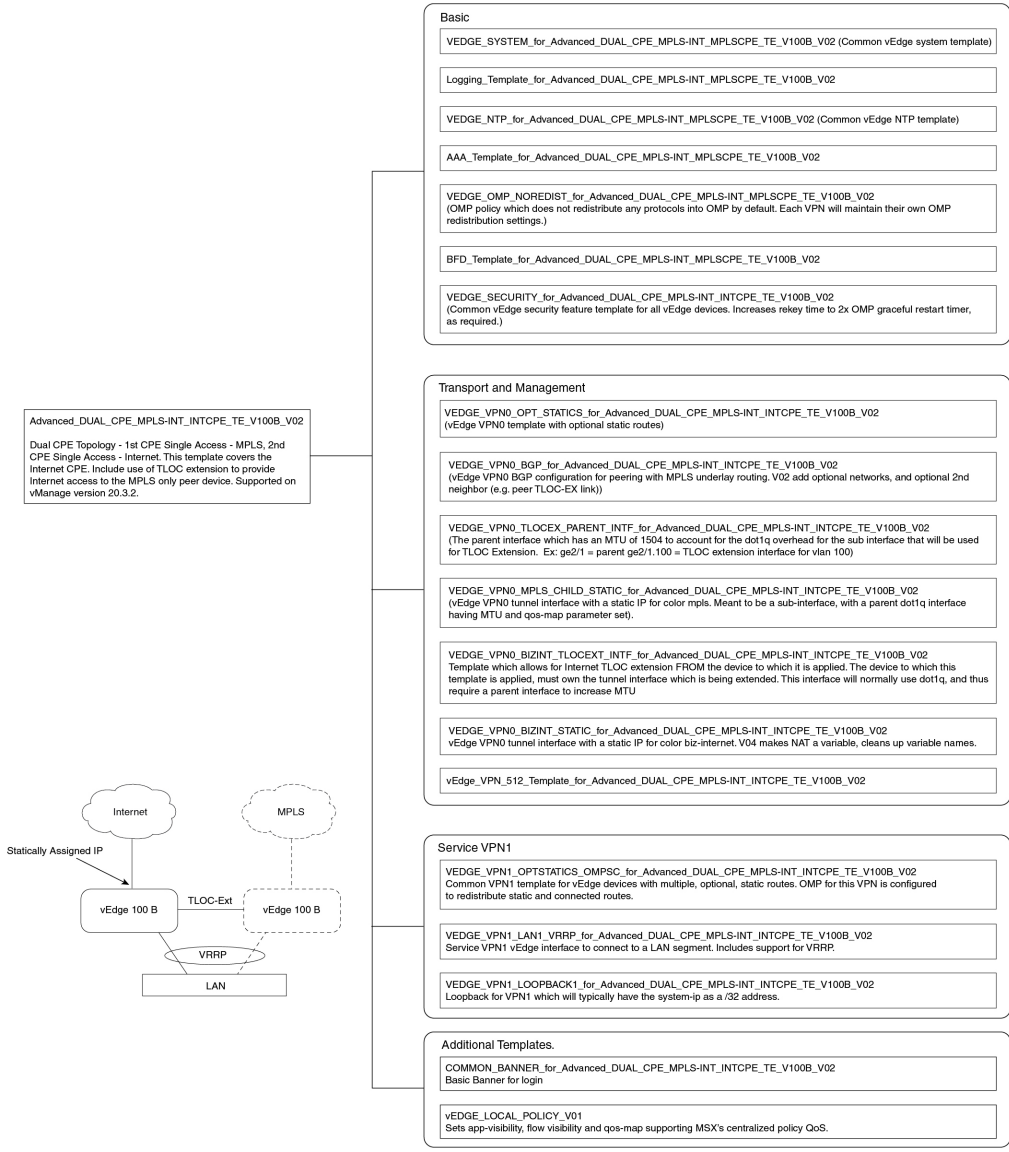


**Note** After the upgrade, the Cisco MSX SD-WAN out-of-the-box device templates assigned to your tenants will continue to work. However, if you are assigning templates to the tenants, use the new out-of-the-box templates (template names with V02 or V03 or V04). If you assign old templates, the system will show an error indicating that these are outdated OOB templates.

**Figure 49: Out-of-the-Box Device Templates**

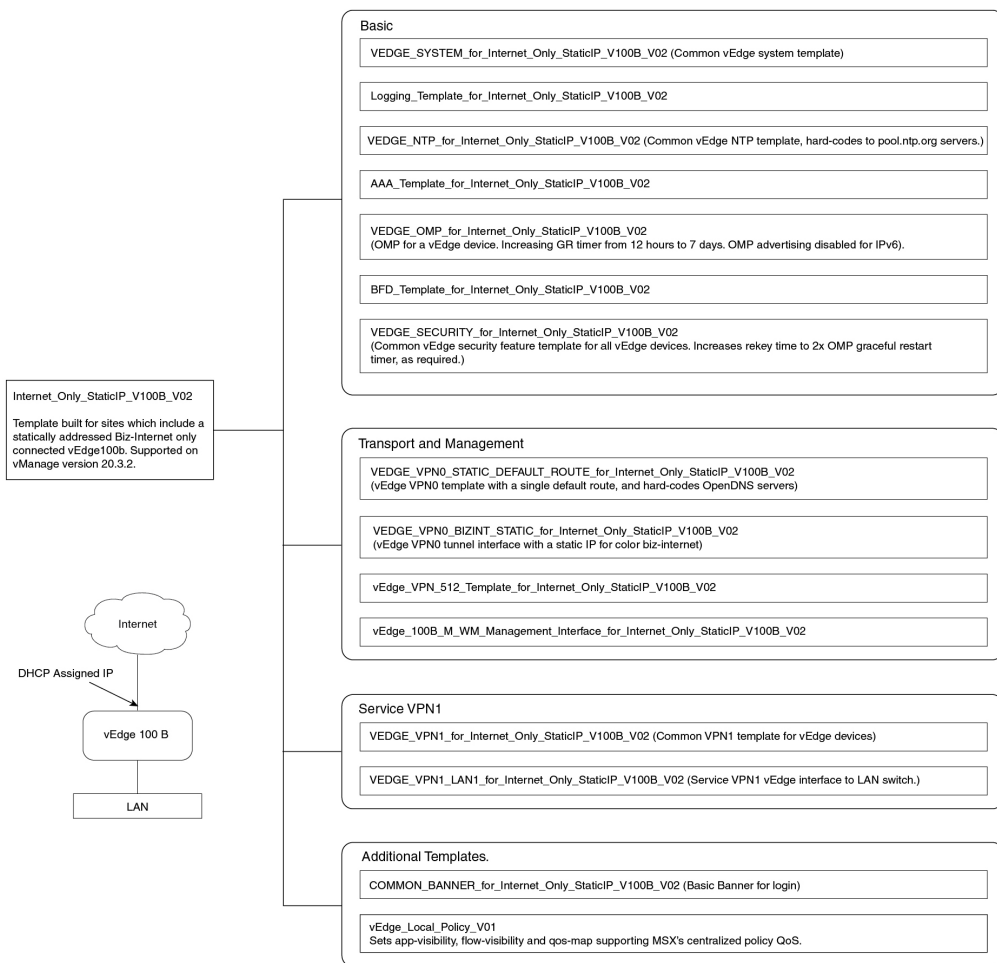
| SD-WAN Template Management |                                                | TYPE ^                       | ... |
|----------------------------|------------------------------------------------|------------------------------|-----|
| <input type="checkbox"/>   | Internet_Only_StaticIP_V100B_V02               | Cisco SD-WAN Device Template | ... |
| <input type="checkbox"/>   | Internet_MPLS_dot1q_VEC_V02                    | Cisco SD-WAN Device Template | ... |
| <input type="checkbox"/>   | Internet_MPLS_dot1q_VEC_SinglePMode_V02        | Cisco SD-WAN Device Template | ... |
| <input type="checkbox"/>   | Advanced_DUAL_CPE_MPLS-INT_INTCPE_TE_V100B_V02 | Cisco SD-WAN Device Template | ... |
| <input type="checkbox"/>   | Advanced_SINGLE_CPE_INT_MPLS_DOT1Q_ASR1KX_V03  | Cisco SD-WAN Device Template | ... |
| <input type="checkbox"/>   | Advanced_SINGLE_CPE_INT_MPLS_DOT1Q_ASR1KX_V02  | Cisco SD-WAN Device Template | ... |

**Figure 50: Advanced Dual CPE MPLS INT INTCPPE**



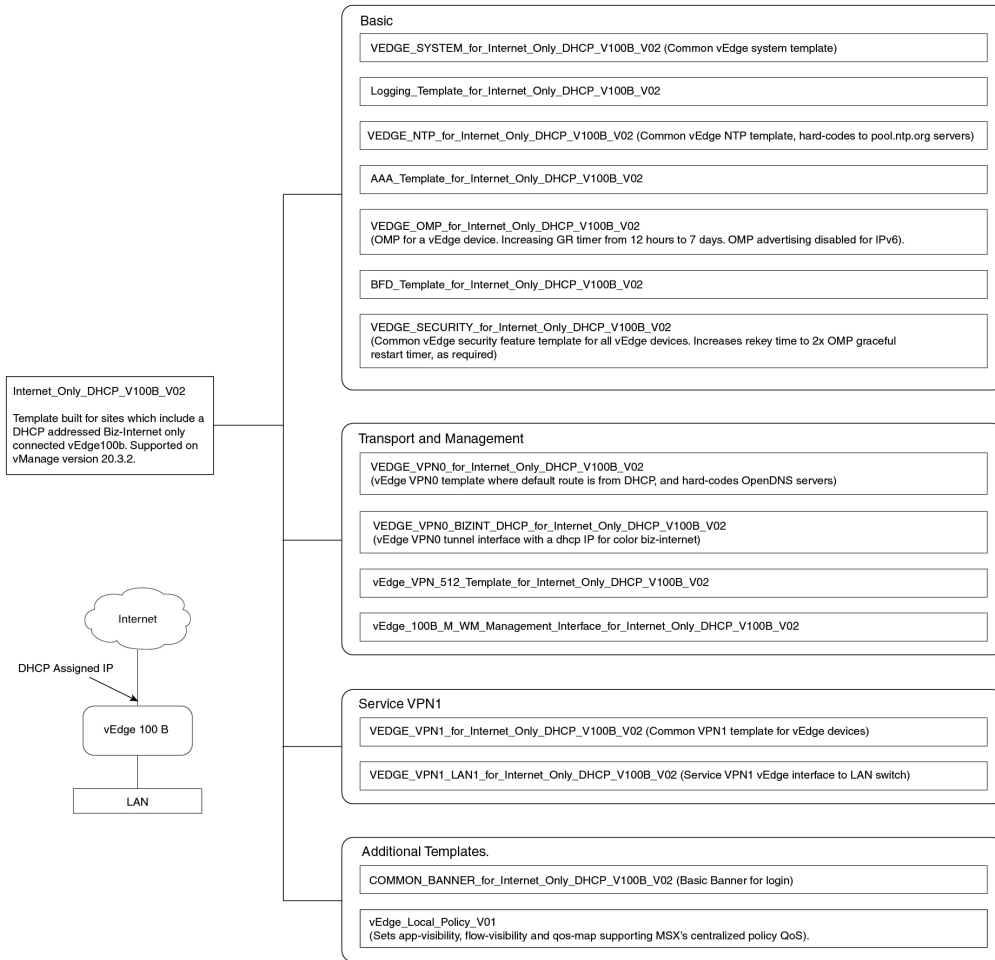
557162

**Figure 51: Internet Only StaticIP**



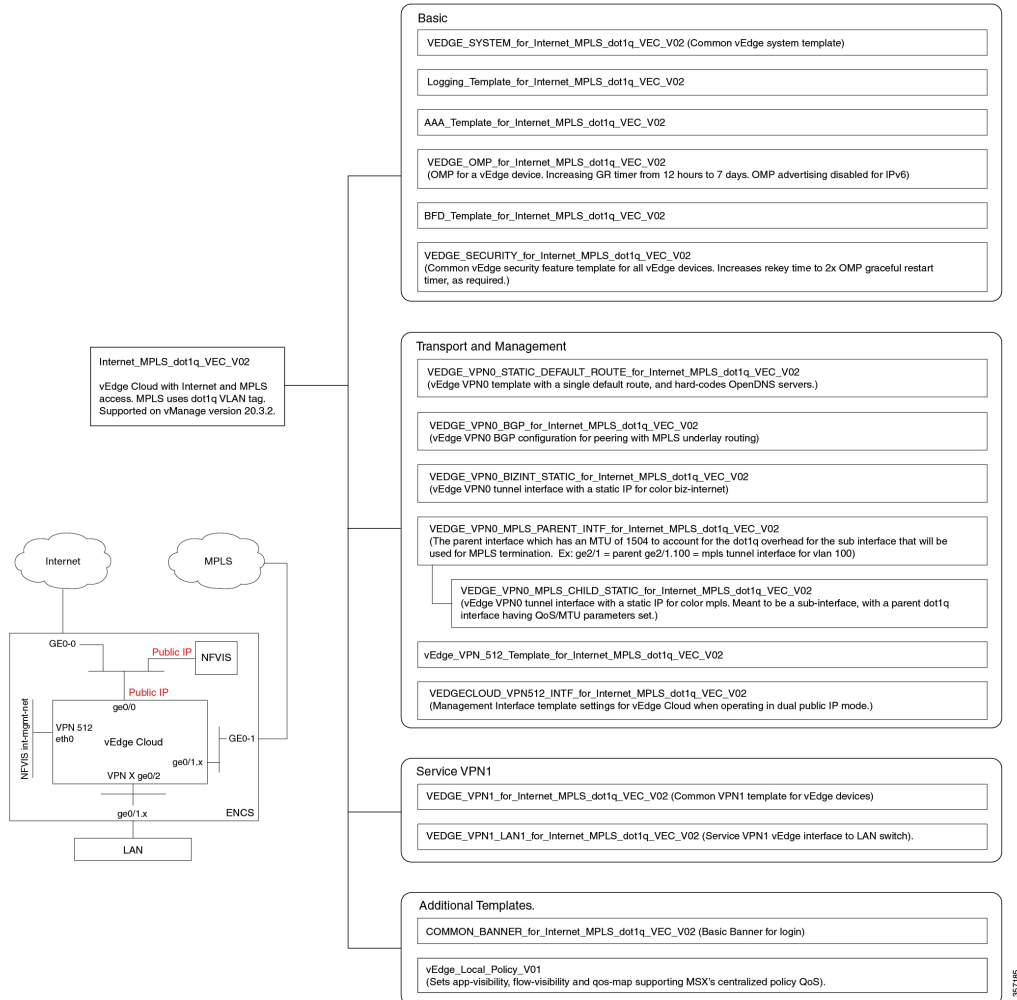
957/103

**Figure 52: Internet Only DHCP**

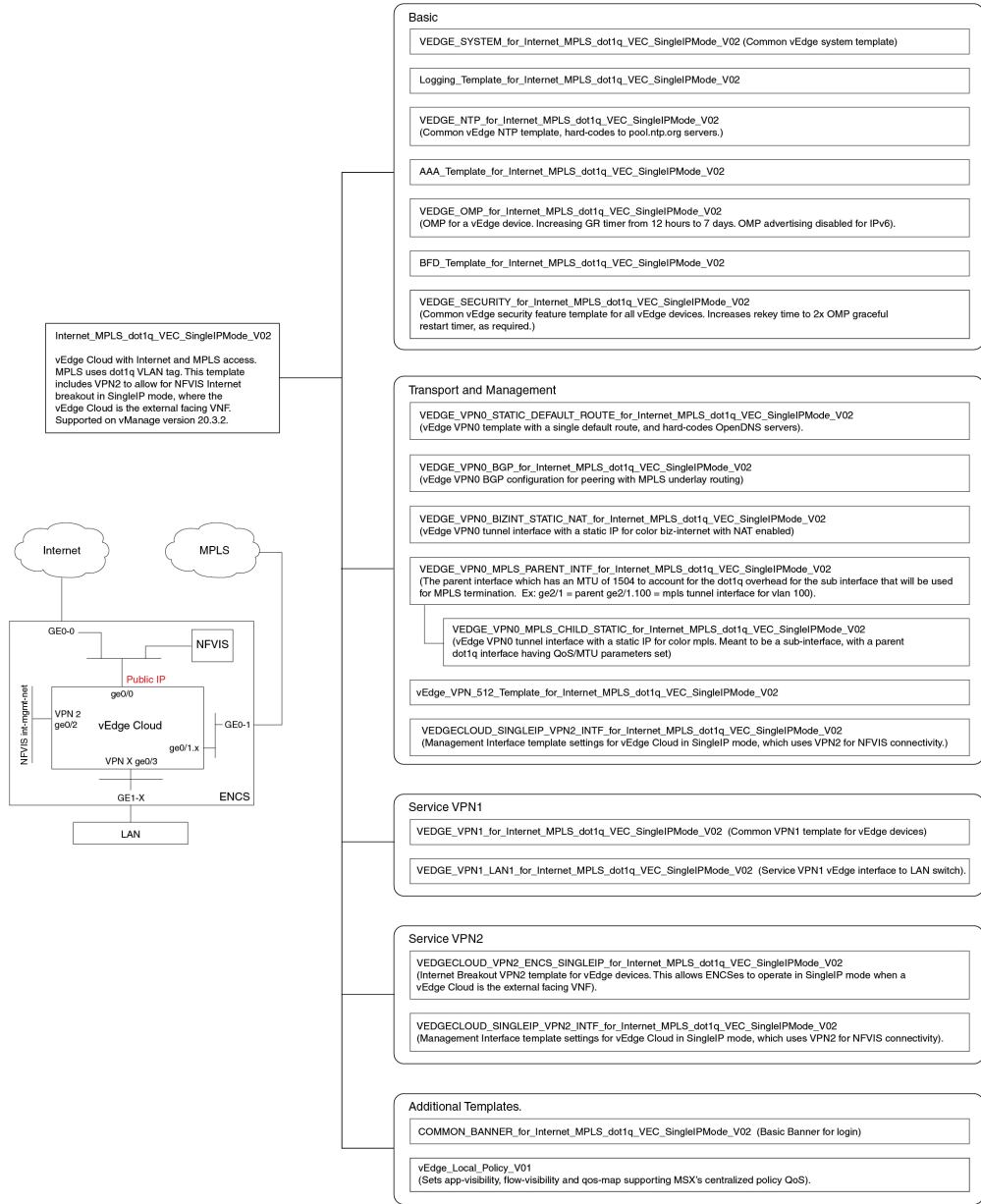


587184

**Figure 53: Internet MPLS**



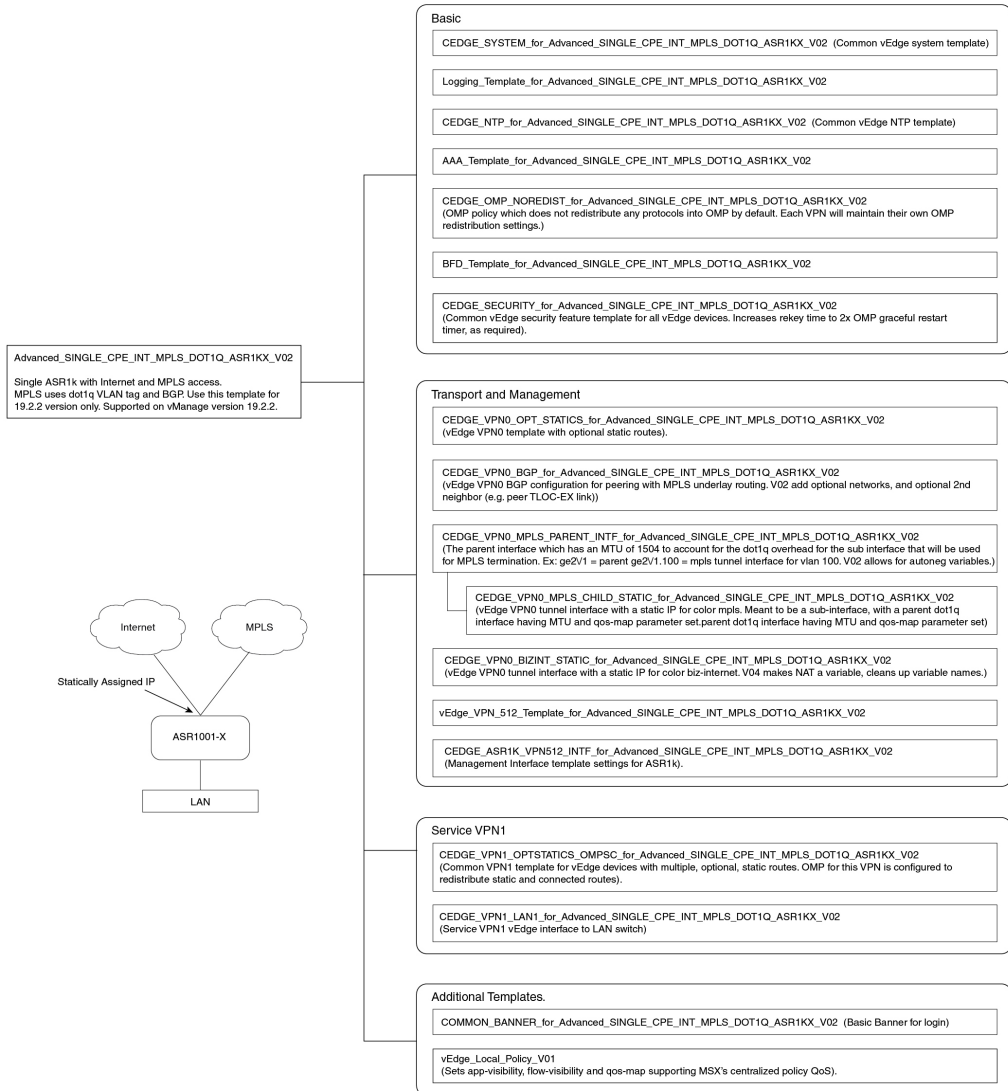
**Figure 54: Internet MPLS VEC Single IP Mode**



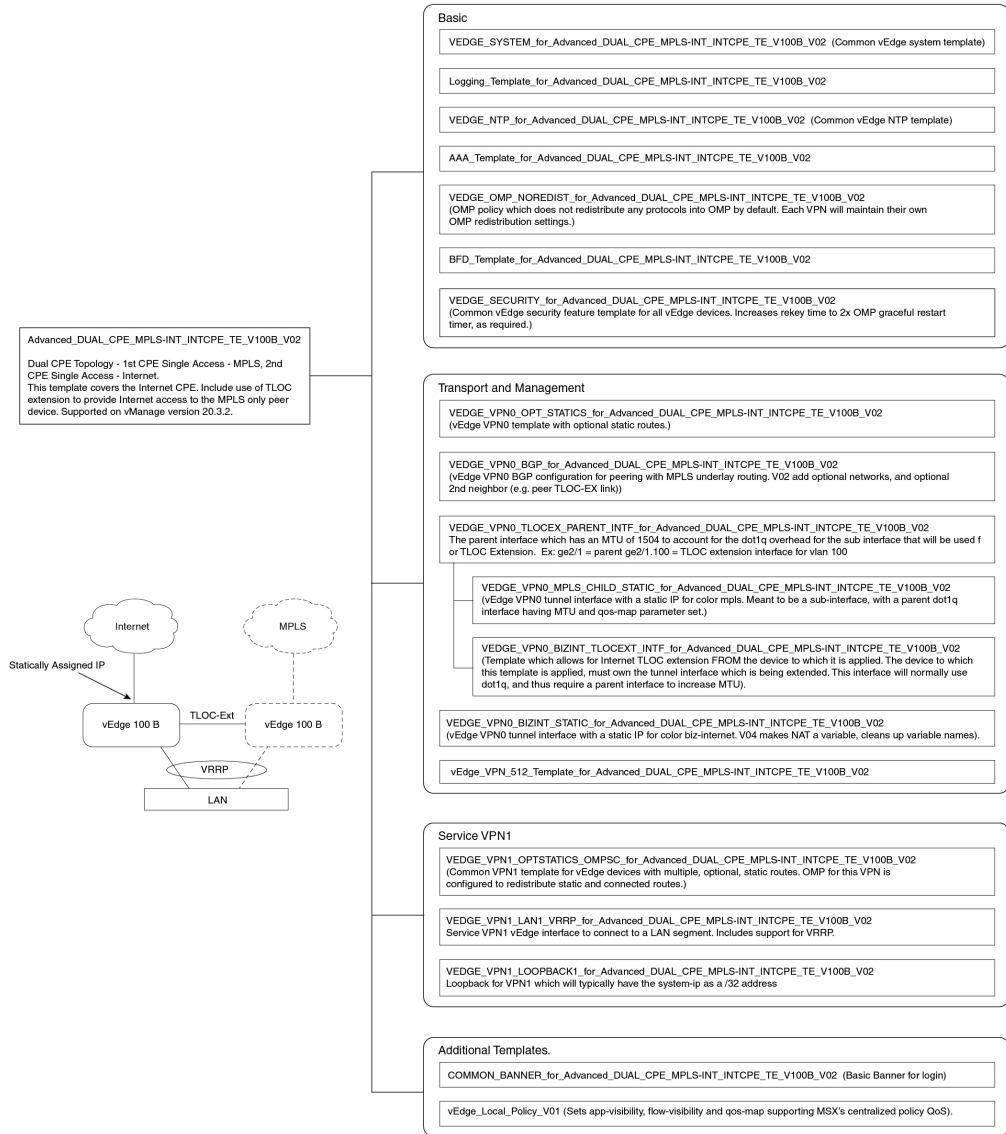
357186



**Figure 55: Advanced Single CPE INT MPLS DOT1Q ASR1KX**

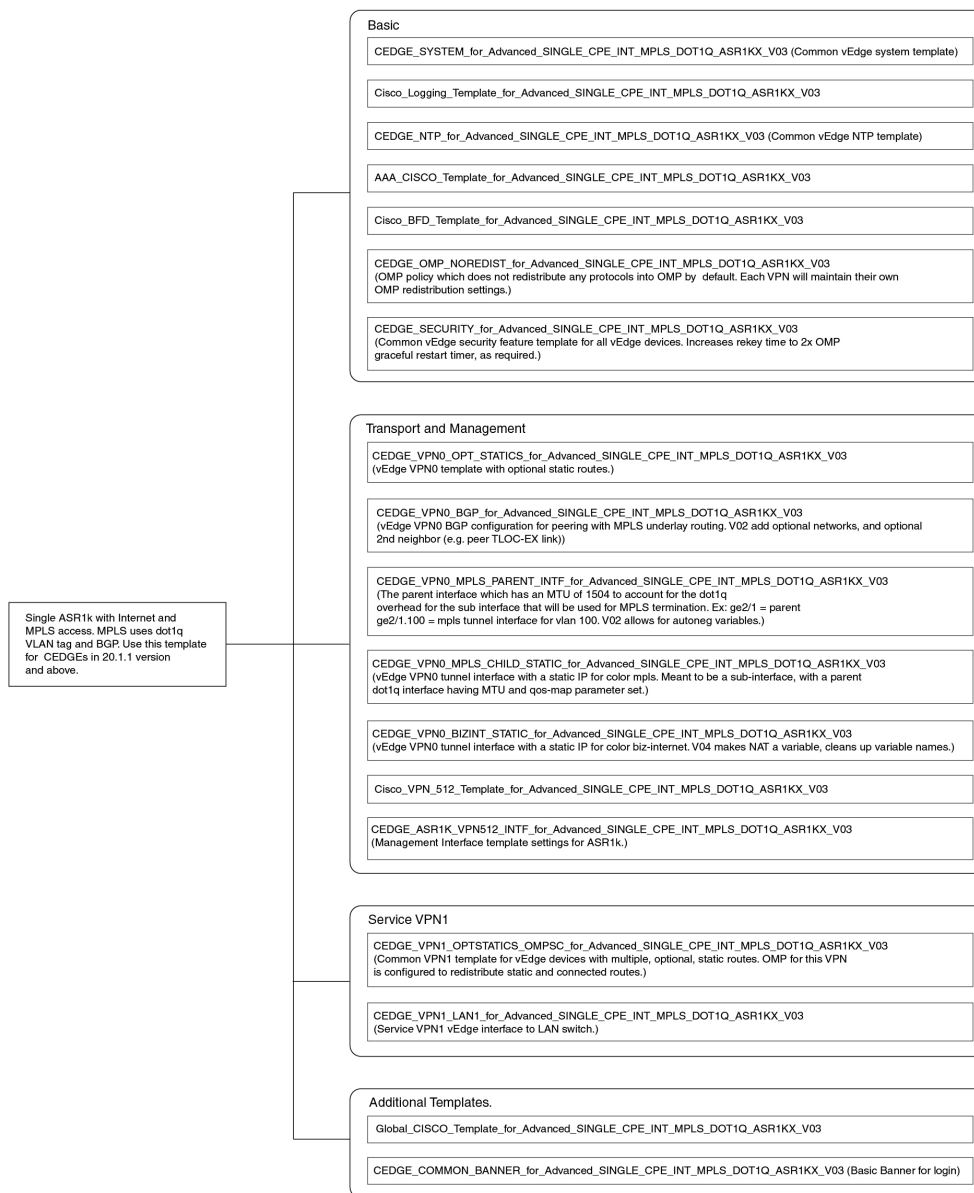


**Figure 56: Actual Dual CPE MPLS-INTCPE\_TE**



957108

Figure 57: Advanced\_SINGLE\_CPE\_INT\_MPLS\_DOT1Q\_ASR1KX\_V03



587180

**Figure 58: Advanced\_SINGLE\_CPE\_INT\_MPLS\_DOT1Q\_ASR1KX\_V04**



357181



## APPENDIX **E**

# Sample Payloads for Creating Cisco SD-WAN Control Plane on Openstack

This section contains the sample JSON configuration files for adding VIM and control plane payloads in the provider and tenant network. The authentication certificate is a part of the control plane deployment activity in vManage and sample JSON files are given for both enterprise and symantec certificate based on the network.

- [Adding VIM Payload in Provider Network](#) , on page 149
- [Adding VIM Payload in Tenant Network](#), on page 150
- [Adding Control Plane Payload with Enterprise Certificate in Provider Network](#), on page 151
- [Adding Control Plane Payload with Symantec Certificate in Provider Network](#), on page 152
- [Adding Control Plane Payload with Enterprise Certificate in Tenant Network](#), on page 153
- [Adding Control Plane Payload with Symantec Certificate on Tenant Network](#), on page 154

## Adding VIM Payload in Provider Network

This is the sample JSON file for adding VIM payload in the provider network.

Note:

- Ensure that the names used in "dtlsNetName"(VPN0) and "mgmtNetName"(VPN512) are from the provider network, that is already created in the OpenStack cloud.
- The VPN512 network should be reachable from MSX for the deployment of the control plane.
- The VPN0 network should be reachable from vEdge for the deployment of vEdge on the deployed control plane.

### Provider Network.json

```
#Provider
{
 "tenantID": "TestTenant",
 "vim":
 {
 "type": "openstack",
 "openstack":
 {
 "username": "username",
 "password": "password",
```

```

"authURL": "URL",
"projectName": "admin",
"projectID": Project ID,
"domainName": "Default",
"region": "RegionOne",
"extNetName": "external",
"networkType": "provider",
"network":
{
"dtlsNetName": "Vnf-outside",
"mgmtNetName": "external"
}
}
}
}

```

## Adding VIM Payload in Tenant Network

This is the sample JSON file for adding VIM payload in tenant network.

Note:

- Ensure that the names used in "dtlsNetName"(VPN0) and "mgmtNetName"(VPN512) are not repeated on the openstack cloud.
- The subnet used in "dtlsSubnet"(VPN0) and "mgmtSubnet"(VPN512) for the 'create control plane' payload should not be repeated on the openstack cloud. You can provide two subnets in this payload.
- The VPN512 network has floating IPs that should be reachable from MSX for the deployment of the control plane.
- The VPN0 network has floating IPs that should be reachable from vEdge for the deployment of vEdge on the deployed control plane.

### Tenant Network.json

```

{
"tenantID": "TestTenant",
"vim": {
"type": "openstack",
"openstack": {
"username": "username",
"password": "password",
"authURL": "url",
"projectName": "admin",
"projectID": "Project ID",
"domainName": "Default",
"region": "RegionOne",
"extNetName": "external",
"networkType": "tenant",
"network": {
"dtlsNetName": "Test-Dtls",
"mgmtNetName": "Test-Mgmt"
}
}
}
}
}

```

## Adding Control Plane Payload with Enterprise Certificate in Provider Network

This is the sample JSON file for adding control plane payload with enterprise certificate in provider network.

### Provider Network with EnterpriseCA.json

```
{
 "tenantID": "TestTenant",
 "controlPlane": {
 "vimID": "vimID",
 "vmanage": {
 "flavor": "viptela-vmanage-vm",
 "image": "viptela-vmanage-19.1.0-genericx86-64.qcow2",
 "hostname": "TestManage01",
 "systemID": "system ID",
 "day0": "vmanage-fip.j2",
 "vpn0": {
 "publicIP": "IP address",
 "gateway": "IP address",
 "subnetMaskBits": "24"},
 "vpn512": {
 "publicIP": "IP address",
 "gateway": "IP address",
 "subnetMaskBits": "24"
 }
 },
 "vbond": {
 "flavor": "viptela-vbond-vm",
 "image": "viptela-edge-19.1.0-genericx86-64.qcow2",
 "hostname": "TestBond01",
 "systemID": "system ID",
 "day0": "vbond-fip-3.j2",
 "vpn0": {
 "publicIP": "IP address",
 "gateway": "IP address",
 "subnetMaskBits": "24"
 },
 "vpn512": {
 "publicIP": "IP address",
 "gateway": "IP address",
 "subnetMaskBits": "24"
 }
 },
 "vsmart": {
 "flavor": "viptela-vsmart-vm",
 "image": "viptela-smart-19.1.0-genericx86-64.qcow2",
 "hostname": "TestSmart01",
 "systemID": "system ID",
 "day0": "vsmart-fip.j2",
 "vpn0": {
 "publicIP": "IP address",
 "gateway": "IP address",
 "subnetMaskBits": "24"
 },
 "vpn512": {
 "publicIP": "IP address",
 "gateway": "IP address",
 "subnetMaskBits": "24"
 }
 },
 "credentials": {
 "username": "username",
```

```

"password": "password"
},
"org": "vmsoverlay1",
"siteID": "site ID",
"ntpServer": "ntp.esl.cisco.com",
"dnsServer": "dns serverIP address",
"createCA": true
}
}

```

## Adding Control Plane Payload with Symantec Certificate in Provider Network

This is the sample JSON file for adding control plane payload with symantec certificate in provider network.

### Provider Network with Symantec.json

```

{
"tenantID": "TestTenant",
"controlPlane": {
"vimID": "vim ID",
"vmanage": {
"flavor": "viptela-vmanage-vm",
"image": "viptela-vmanage-19.1.0-genericx86-64.qcow2",
"hostname": "TestManage01",
"systemID": "system ID",
"day0": "vmanage-fip-noCA.j2",
"vpn0": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"vbond": {
"flavor": "viptela-vbond-vm",
"image": "viptela-edge-19.1.0-genericx86-64.qcow2",
"hostname": "TestBond01",
"systemID": "system ID",
"day0": "vbond-fip-3-noCA.j2",
"vpn0": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"vsmart": {
"flavor": "viptela-vsmart-vm",
"image": "viptela-smart-19.1.0-genericx86-64.qcow2",
"hostname": "TestSmart01",
"systemID": "system ID",
"day0": "vsmart-fip-noCA.j2",
"vpn0": {

```



```

"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
},
"vpn512": {
"publicIP": "IP address",
"gateway": "IP address",
"subnetMaskBits": "24"
}
},
"credentials": {
"username": "username",
"password": "password"
},
"org": "vmsoverlay1",
"siteID": "site ID",
"ntpServer": "ntp.esl.cisco.com",
"dnsServer": "IP address",
"createCA": false
}
}

```

## Adding Control Plane Payload with Enterprise Certificate in Tenant Network

This is the sample JSON file for adding control plane payload with enterprise certificate in tenant network.

### Tenant Network with EnterpriseCA.json

```

{
"tenantID": "TestTenant",
"controlPlane": {
"vimID": "vim ID",
"vmanage": {
"flavor": "viptela-vmanage-vm",
"image": "viptela-vmanage-19.1.0-genericx86-64.qcow2",
"hostname": "TestManage10",
"systemID": "system ID",
"day0": "vmanage-fip.j2",
"vpn0": {
"subnetMaskBits": "24"
},
"vpn512": {
"subnetMaskBits": "24"
}
},
"vbond": {
"flavor": "viptela-vbond-vm",
"image": "viptela-edge-19.1.0-genericx86-64.qcow2",
"hostname": "TestBond10",
"systemID": "50.0.1.11",
"day0": "vbond-fip-3.j2",
"vpn0": {
"subnetMaskBits": "24"
},
"vpn512": {
"subnetMaskBits": "24"
}
},
"vsmart": {
"flavor": "viptela-vsmart-vm",
"image": "viptela-smart-19.1.0-genericx86-64.qcow2",

```

```

"hostname": "TestSmart10",
"systemID": "system ID",
"day0": "vsmart-fip.j2",
"vpn0": {
 "subnetMaskBits": "24"
},
"vpn512": {
 "subnetMaskBits": "24"
}
},
"credentials": {
 "username": "username",
 "password": "password"
},
"org": "vmsoverlay1",
"siteID": "site ID",
"ntpServer": "ntp.esl.cisco.com",
"dnsServer": "IP address",
"createCA": true,
"dtlsSubnet": "IP address",
"mgmtSubnet": "IP address"
}
}

```

## Adding Control Plane Payload with Symantec Certificate on Tenant Network

This is the sample JSON file for adding control plane payload with symantec certificate on tenant network.

### Tenant Network with Symantec.json

```

{
 "tenantID": "TestTenant",
 "controlPlane": {
 "vimID": "vim ID",
 "vmanage": {
 "flavor": "viptela-vmanage-vm",
 "image": "viptela-vmanage-19.1.0-genericx86-64.qcow2",
 "hostname": "TestManage10",
 "systemID": "system ID",
 "day0": "vmanage-fip-noCA.j2",
 "vpn0": {
 "subnetMaskBits": "24"
 },
 "vpn512": {
 "subnetMaskBits": "24"
 }
 },
 "vbond": {
 "flavor": "viptela-vbond-vm",
 "image": "viptela-edge-19.1.0-genericx86-64.qcow2",
 "hostname": "TestBond10",
 "systemID": "system ID",
 "day0": "vbond-fip-3-noCA.j2",
 "vpn0": {
 "subnetMaskBits": "24"
 },
 "vpn512": {
 "subnetMaskBits": "24"
 }
 },
 "vsmart": {

```

```
"flavor": "viptela-vsmart-vm",
"image": "viptela-smart-19.1.0-genericx86-64.qcow2",
"hostname": "TestSmart10",
"systemID": "system ID",
"day0": "vsmart-fip-noCA.j2",
"vpn0": {
 "subnetMaskBits": "24"
},
"vpn512": {
 "subnetMaskBits": "24"
}
},
"credentials": {
 "username": "username",
 "password": "password"
},
"org": "vmsoverlay1",
"siteID": "site ID",
"ntpServer": "ntp.esl.cisco.com",
"dnsServer": "IP address",
"createCA": false,
"dtlsSubnet": "IP address",
"mgmtSubnet": "IP address"
}
}
```

