Cisco SD-WAN Predeployment Tasks

Revised: August 29, 2021

Setting Up Cisco SD-WAN Specific Configurations in MSX

Configure the following for Cisco SD-WAN setup:

Disabling MSX-Managed Proxy

MSX allows you to connect to the control plane using an MSX-managed proxy, in which case you do not have to add the tenant's IP addresses to the allowed list. This functionality is enabled by default and can be disabled using an API.

To disable this functionality, set the *enableVmanageProxy* metadata to *false* using the *PUT /sdwanservice/v1/featureflag/enable/vmanageproxy* in the **SDWAN Service** API.

For more information on this API, refer the Swagger documentation that can be accessed from **Account Settings > Swagger > SDWAN Microservice > feature-flag-controller** section.

Note Note: Only users with the following permissions can execute the vmanageproxy API.

- Integration Configuration (Manage) permission. This permission can be found under the **Integrations, Settings, and Logs** category.
- SD-WAN Control Plane (View) permission. This permission can be found under the **SD-WAN Service** category.

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.

Procedure

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:

Procedure

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.

Procedure

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.**

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 Site or Device.

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

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:

Procedure

Step 1 Log in to the Cisco MSX Portal.

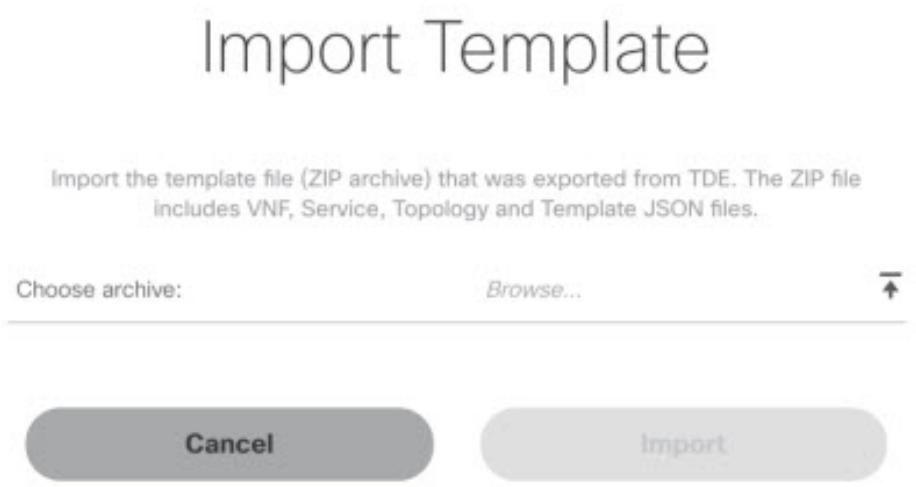
Step 2 In the main menu, choose **Settings > Service Configuration**.

Step 3 Click **SD-Branch** and then click the **Settings > Template Management**. The Manage Template appears.

Step 4 To add a new template:

a) Select Import Template. The Import Template dialog box appears.

Figure 1: Import Template



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**.

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

Step 5 To modify an existing template:

a) 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:

Procedure

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:

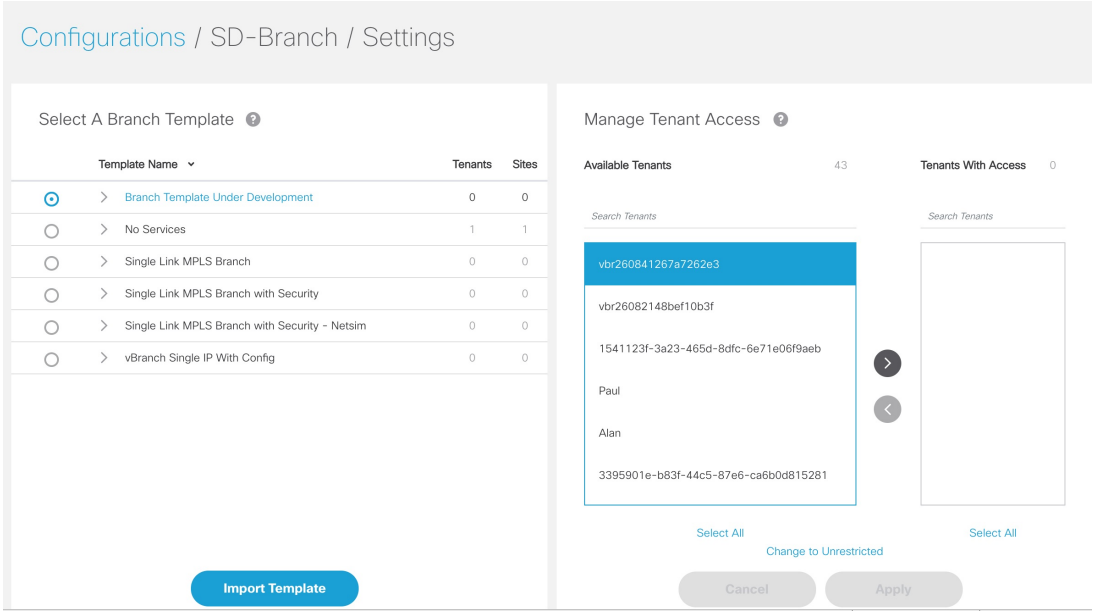
Procedure

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 2: SD-Branch Settings



Step 4 To assign the template to a tenant:

a) Click the template that you want to assign to the tenant.

b) Select the template version.

c) To display the template version, click >.

d) 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.**
e) Click >.The tenant record(s) moves to the Tenant With Access list.
f) Click **Apply**.

Step 5 To remove access to a template:

a) Click the template that for which modify the access.
b) 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**.
c) 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.

d) Click **Apply**.

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 1: Attributes Used in Creating SD-WAN Control Plane in OpenStack

Key Options of OS orchestrator	Explanation
Provider Network	• 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	• 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. **Note** • 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.
Multi-Tenant	• 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. **Note** Change the "projectName" and "projectID" values in the add vim payload to reflect the Tenant/Project space that is to be configured.
Enterprise Certificate Authentication (CA)	• 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. **Note** To select this option, include ‘createCA: true' in the create control plane payload.

Key Options of OS orchestrator	Explanation
Default Symantec/Cisco CA	• 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'. **Note** • 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 2: Tasks involved in Creating SD-WAN Control Plane

Request Type	API	Description
Create VIM	`POST /osorch/v1/vims`	• 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.

Request Type	API	Description

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"`
		• Receives request to delete VIM, initiates the cleanup activity, and finally deletes the VIM.
		Note To delete VIM, enter the vimID. The vimID is returned as a response for creating the VIM.

Create CP	`POST /osorch/v1/cps`	• 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`
		• Receives request to delete the control plane, this initiates the OpenStack cleanup activity. Finally deletes the control plane.
		Note To delete CP, enter the cpID. The cpID is returned from the create CP response.

Get the Create/Delete job status	`GET/osorch/v1/jobs/{jobID}` **Note** The jobID is the response from this API or "GET /osorch/v1/cps" to check the job status.	• This API is used to check the create/delete transaction status.
Get all Templates	`GET /osorch/v1/templates`	• 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}`	• Displays the content of a specific template. • You can edit the content of the specific template.
Change the Template	`POST /osorch/v1/template`	• 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 SD-WAN control plane service on AWS:

Procedure

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click **Service Catalog > SD-WAN > Continue to Offers**.

Step 3 Select the tenant from the drop-down.

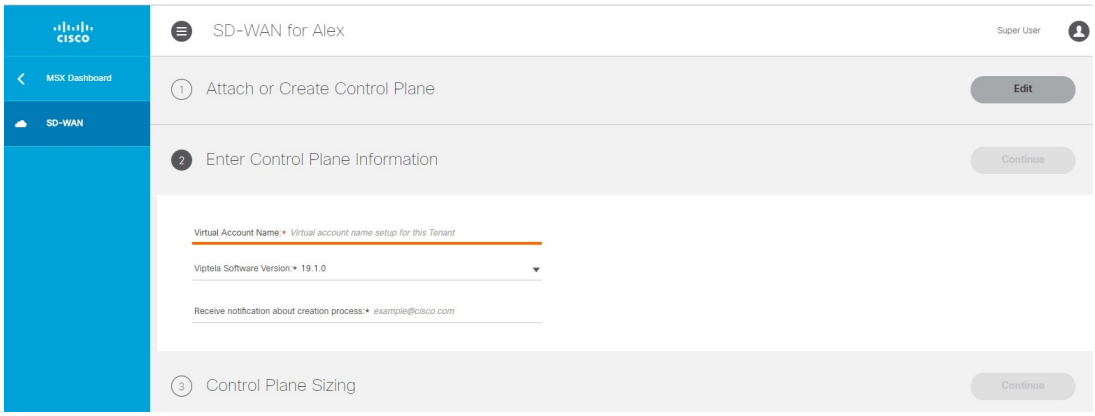
Step 4 Click **Get Started**.

Step 5 From the SD-WAN Service screen, click **Add Control Plane** to add a control plane for the customer.

Step 6 Select Create Control Plane to create a new control plane for the tenant.

Step 7 Enter the following details in the **Control Plane Information** section:

Figure 3: Control Plane Information Fields While Creating Control Plane on AWS



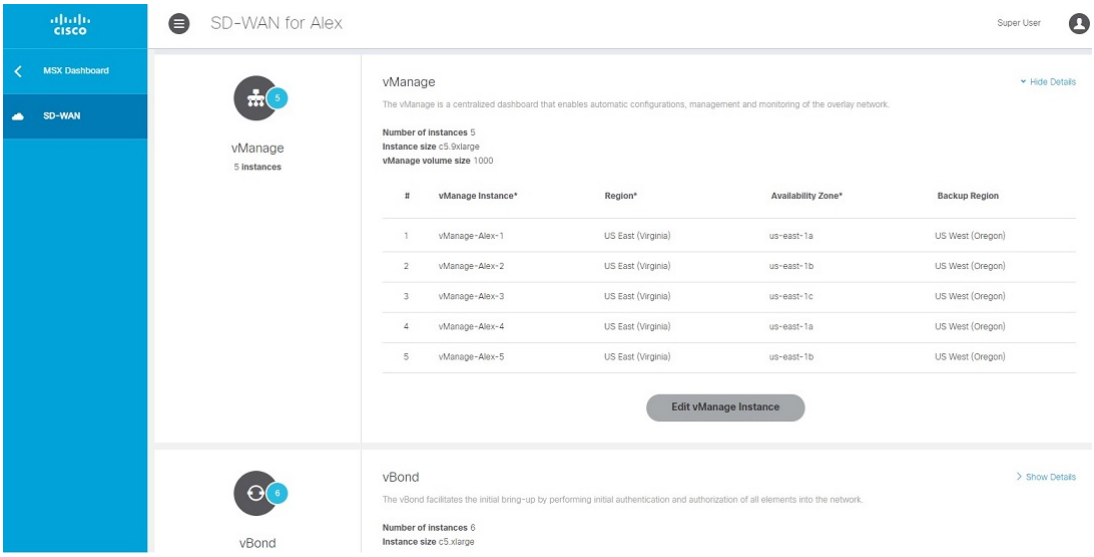
- Enter the Virtual Account Name: The service provider creates a Virtual Account (VA) to manage the licenses and assets of the tenant.
- Select a Cisco SD-WAN Software version from the list of version available. For example: 19.2,19.1,18.4.1, and 18.4.0.
- Enter your Cisco email address, to receive an information about the creation process and an approved Certificate Signing Request (CSR) message.

Note These control plane fields appear only if the SD-WAN Orchestrator (vOrch) Settings has been added for your SD-WAN setup. For more information, see Configuring Cisco SD-WAN Orchestrator Settings.

Step 8 In the Control Plane Sizing 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 be possible.

Figure 4: Recommended Number of Instances



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 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 the **Edit** button in vManage, vSmart, and vBond section. You can also edit the recommended number of instances, 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 will be displayed 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.

What to do next

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.

Attaching Control Plane

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

Procedure

Step 1 Log in to the Cisco MSX Portal.

Step 2 In the main menu, click **Service Catalog**.

Step 3 Click **SD-WAN**.

Step 4 Select the tenant from the drop-down.

Step 5 Click **Get Started**.

Step 6 From the **SD-WAN Service** screen, click **Add Control Plane** to add a control plane for the customer.

Step 7 Select **Attach Control Plane** 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
- Only alphanumeric characters are allowed in the username field.
- All alphanumeric characters are supported in the password field, except Space .
- Organization name cannot contain (),<>?{}[]`\"

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

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

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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