Configuration

Action Parameters - Data Policy

Table 1: Feature History

Feature Name	Release Information	Description
Traffic Redirection to SIG Using Data Policy	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	You can create a data policy where you can selectively define an application list along with other existing match criteria in the data-policy to redirect the application traffic to a Secure Internet Gateway (SIG).
Next Hop Action Enhancement in Data Policies	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature enhances match action conditions in a centralized data policy for parity with the features configured on Cisco vEdge devices. When you are setting up next-hop-loose action, this feature helps to redirect application traffic to an available route when next-hop address is not available.

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or dropped. Then, you can associate parameters with accepted packets.

In the CLI, you configure the action parameters with the **policy data-policy vpn-list sequence action** command.

Each sequence in a centralized data policy can contain one action condition.

In the action, you first specify whether to accept or drop a matching data packet, and whether to count it:

Action Condition	Description
Click **Accept**	Accepts the packet. An accepted packet is eligible to be modified by the additional parameters configured in the action portion of the policy configuration.
Cflowd	Enables cflowd traffic monitoring.
Counter	Counts the accepted or dropped packets. Specifies the name of a counter. Use the **show policy access-lists counters** command on the Cisco vEdge device.
Click **Drop**	Discards the packet. This is the default action.
Log	Logs the packet. Packets are placed into the messages and syslog system logging (syslog) files. To view the packet logs, use the **show app log flows** and **show log** commands.

Action Condition	Description
Redirect DNS	Redirects DNS requests to a particular DNS server. Redirecting requests is optional, but if you do so, you must specify both actions. For an inbound policy, **redirect-dns host** allows the DNS response to be correctly forwarded back to the requesting service VPN. For an outbound policy, specify the IP address of the DNS server. **Note** When you upgrade to releases later than Cisco IOS XE Release 17.7.1a, you must configure redirect DNS through **nat use-vpn 0** to redirect DNS to Direct Internet Interface (DIA). **Note** You can set only local TLOC preferences with redirect-dns as actions on the same sequence, but not remote TLOC.
TCP Optimization	Fine-tune TCP to decrease round-trip latency and improve throurghout for matching TCP traffic.
Secure Internet Gateway	Redirect application traffic to a SIG **Note** Before you apply a data policy for redirecting application traffic to a SIG, you must have configured the SIG tunnels. For more information on configuring Automatic SIG tunnels, see Automatic Tunnels. For more information on configuring Manual SIG tunnels, see Manual Tunnels.

Then, for a packet that is accepted, the following parameters can be configured:

Action Condition	Description
Cflowd	Enables cflowd traffic monitoring.
NAT Pool or **NAT VPN**	Enables NAT functionality, so that traffic can be redirected directly to the internet or other external destination.
DSCP	DSCP value. The range is 0 through 63.
Forwarding Class	Name of the forwarding class.
Local TLOC	Enables sending packets to one of the TLOCs that matches the color and encapsulation. The available colors are: 3g, biz-internet, blue, bronze, custom1,custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red and silver. The encapsulation options are: **ipsec** and **gre**. By default, if the TLOC is not available, traffic is forwarded using an alternate TLOC. To drop traffic if a TLOC is unavailable, include the **restrict** option. By default, encapsulation is **ipsec**.

Action Condition	Description
Next Hop	Sets the next hop IP address to which the packet should be forwarded. **Note** Starting from Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1, the **Use Default Route when Next Hop is not available** field is available next to the **Next Hop** action parameter. This option is available only when the sequence type is **Traffic Engineering** or **Custom**, and the protocol is either **IPv4** or **IPv6**, but not both.
Policer	Applies a policer. Specifies the name of policer configured with the **policy policer** command.
Service	Specifies a service to redirect traffic to before delivering the traffic to its destination. The TLOC address or list of TLOCs identifies the remote TLOCs to which the traffic should be redirected to reach the service. In the case of multiple TLOCs, the traffic is load-balanced among them. The VPN identifier is where the service is located. Standard services: **FW**, **IDS**, **IDP** Custom services: **netsvc1**, **netsvc2**,**netsvc3**, **netsvc4** TLOC list is configured with a **policy lists tloc-list** list. Configure the services themselves on the Cisco vEdge devices that are collocated with the service devices, using the **vpn service** command.
TLOC	Direct traffic to a remote TLOC that matches the IP address, color, and encapsulation of one of the TLOCs in the list. If a preference value is configured for the matching TLOC, that value is assigned to the traffic.
Click **Accept**, then action **VPN**.	Set the VPN that the packet is part of. The range is 0 through 65530.

Note Data policies are applicable on locally generated packets, including routing protocol packets, when the match conditions are generic.

Example configuration:

```
sequence 21
   match
    source-ip 10.0.0.0/8
   action accept
```

In such situations, it may be necessary to add a sequence in the data policy to escape the routing protocol packets. For example to skip OSPF, use the following configuration:

```
sequence 20
   match
    source-ip 10.0.0.0/8
    protocol  89
   action accept
sequence 21
   match
    source-ip 10.0.0.0/8
   action accept
```

The following table describes the IPv4 and IPv6 actions.

Table 2:

IPv4 Actions	IPv6 Actions
drop, dscp, next-hop (from-service only)/vpn, count, forwarding class, policer (only in interface ACL), App-route SLA (only)	N/A
App-route preferred color, app-route sla strict, cflowd, nat, redirect-dns	N/A
N/A	drop, dscp, next-hop/vpn, count, forwarding class, policer (only in interface ACL) App-route SLA (only), App-route preferred color, app-route sla strict
policer (DataPolicy), tcp-optimization, fec-always,	policer (DataPolicy)
tloc, tloc-list (set tloc, set tloc-list)	tloc, tloc-list (set tloc, set tloc-list)
App-Route backup-preferred color, local-tloc, local-tloc-list	App-Route backup-preferred color, local-tloc, local-tloc-list

Access the Software Upgrade Workflow

Table 3: Feature History

Feature Name	Release Information	Description
Software Upgrade Workflow	Cisco IOS XE Release 17.8.1a Cisco vManage Release 20.8.1 Cisco SD-WAN Release 20.8.1	You can now upgrade software images on edge devices using the **Workflows** menu in Cisco vManage.
Schedule the Software Upgrade Workflow	Cisco IOS XE Release 17.9.1a Cisco vManage Release 20.9.1 Cisco SD-WAN Release 20.9.1	Upgrade the software of Cisco edge devices using a **scheduler** which helps in scheduling the upgrade process at your convenience.
Software Upgrade Workflow Support for Additional Platforms	Cisco vManage Release 20.9.1	Added support for Cisco Enterprise NFV Infrastructure Software (NFVIS) and Cisco Catalyst Cellular Gateways.

Before You Begin

To check if there is an in-progress software upgrade workflow:

From the Cisco vManage toolbar, click the **Task-list** icon. Cisco vManage displays a list of all running tasks along with the total number of successes and failures.

Access the Software Upgrade Workflow

1. In the Cisco vManage menu, click **Workflows** > **Workflow Library**.

Note In the Cisco vManage Release 20.8.1, the **Workflow Library** is titled **Launch Workflows**.

2. Start a new software upgrade workflow: **Library** > **Software Upgrade**.

   OR

   Alternatively, resume an in-progress software upgrade workflow: **In-progress** > **Software Upgrade**.

3. Follow the on-screen instructions to start a new software upgrade workflow.

Note Click **Exit** to exit from an in-progress software upgrade workflow. You can resume the in-progress workflow at your convenience.

Note In a multi-node cluster setup, if the control connection switches to a different node during a device upgrade from Cisco vManage, the upgrade may be impacted due to NetConf session timeout. The device then establishes control connection to a different node. You need to re-trigger the upgrade activity.

Verify the Status of the Software Upgrade Workflow

To check the software upgrade workflow status:

1. From the Cisco vManage toolbar, click the **Task-list** icon.

   Cisco vManage displays a list of all running tasks along with the total number of successes and failures.

2. Click the + icon to view the details of a task.

   Cisco vManage opens a pane displaying the status of the task and details of the device on which the task was performed.

Add a Cisco vManage Server to a Cluster

Table 4: Feature History

Feature Name	Release Information	Description
Cisco vManage Persona-based Cluster Configuration	Cisco IOS XE Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	You can add Cisco vManage servers to a cluster by identifying servers based on personas. A persona defines what services run on a server.

The following sections provide information about adding a Cisco vManage server to a cluster in various Cisco vManage releases.

Add a Cisco vManage Server to a Cluster for Releases Before Cisco vManage Release 20.6.1

To add a new Cisco vManage server to a cluster for releases before Cisco vManage Release 20.6.1, perform the following steps on the primary Cisco vManage server.

Before you begin, ensure that the default IP address of the Cisco vManage server has been changed to an out-of-band IP address as described in Configure the Cluster IP Address of a Cisco vManage Server, on page 25.

1. From the Cisco vManage menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.

2. Click **Add vManage**.

   The **Edit vManage** window opens.

3. In the **vManage IP Address** field, select an IP address to assign to the Cisco vManage server.

4. Enter the username and password for logging in to the Cisco vManage server.

5. Enter the IP address of the Cisco vManage server that you are adding to the cluster.

6. Specify the username and password for the new Cisco vManage server.

7. Select the services to be run on the Cisco vManage server. You can select from the services listed below. Note that the **Application Server** field is not editable. The Cisco vManage Application Server is the local Cisco vManage HTTP web server.

   - Statistics Database: Stores statistics from all the Cisco SD-WAN devices in the network.
   - Configuration Database: Stores all the device and feature templates and configurations for all the Cisco SD-WAN devices in the network.
   - Messaging Server: Distributes messages and shares state among all the Cisco vManage cluster members.

8. Click **Add**.

   The Cisco vManage server that you just added reboots before joining the cluster.

Note

- In a cluster, we recommend that you run at least three instances of each service.
- When you add the first two compute or compute+data nodes to the cluster, the host node's application-server is unavailable. The following message is displayed on the host node's GUI, before the application-server shuts down in the host node: `\Node added to the cluster. The operation may take up to 30 minutes and may cause application-server to restart in between. Once the application server is back online, the post cluster operation progress can be viewed under tasks pop-up\.`

Add a Cisco vManage Server to a Cluster for Cisco vManage Release 20.6.1 and Later Releases

From Cisco vManage Release 20.6.1, a cluster supports any of the following deployments of nodes:

- Three Compute+Data nodes
- Three Compute+Data nodes and three Data nodes

Note DATA nodes should be added only after 3 node cluster with CONFIG+DATA is added.

- Three Compute nodes and three Data nodes (supported only in an upgrade from an existing deployment)

If you require a different combination of nodes, contact your Cisco representative.

To add a Cisco vManage server to a cluster from Cisco vManage Release 20.6.1, perform the following steps.

Perform this procedure on a Compute+Data node or a Compute node. Performing this procedure on a Data node is not supported because a Data node does not run all the services that are required for the addition.

Do not add a server that was a member of the cluster and then removed from the cluster. If you need to add that server to the cluster, bring up a new VM on that server to be used as the node to add.

Before you begin, ensure that the default IP address of the Cisco vManage server has been changed to an out-of-band IP address, as described in Configure the Cluster IP Address of a Cisco vManage Server, on page 25.

1. From the Cisco vManage menu, choose **Administration** > **Cluster Management**.

   The **Cluster Management page** window appears. The table on this window shows the Cisco vManage servers that are in the cluster.

2. Click **Add vManage**.

   The **Add vManage** dialog box opens.

   Note If the **Edit vManage** dialog box opens, configure an out-of-band IP address for the server, as described in Configure the Cluster IP Address of a Cisco vManage Server, on page 25, and then repeat this procedure for adding a server.

3. In the **Add vManage** dialog box, perform the following actions:

   a. Click the **Node Persona** option (**Compute+Data**, **Compute**, or **Data**) that corresponds to the persona that has been configured for the server.

      You can determine the persona of a server by logging in to the server and looking at the persona display on the **Administration** > **Cluster Management** window. If you choose an incorrect persona, a message displays the persona that you should choose.

   b. From the **vManage IP Address** drop-down list, choose the IP address of the server to be added to the cluster.

   c. In the **Username** field, enter the user name for logging in to the server.

   d. In the **Password** field, enter the password for logging in to the server.

   e. (Optional) Click **Enable SD-AVC** if you want Cisco Software-Defined Application Visibility and Control (SD-AVC) to run on the server.

      Cisco SD-AVC is a component of Cisco Application Visibility and Control (AVC). It can be enabled on one Cisco vManage server. The server on which it is enabled must have the Compute+Data or the Compute persona. Cisco SD-AVC cannot be enabled on a server that has the Data persona.

      If you enabled Cisco SD-AVC for this server when you changed its IP address, the **Enable SD-AVC** check box is checked by default.

   f. Click **Add**.

   g. To confirm, click **OK**.

      The dialog box indicates that the services will restart, and that the existing metadata and other information that is not required when the server joins the cluster will be deleted from the server.

      When you click **OK**, the system starts the server add operation. The **Cluster Management** window displays the tasks that the system performs as it adds the server.

      As part of this operation, the system checks the compatibility of the server that you are adding. This check ensures that the server has sufficient disk space, and that the persona that you specified matches the persona of the node.

After the server is added, the system performs a cluster sync operation, which rebalances the services in the cluster. Then the Cisco vManage servers in the cluster restart.

Add Cisco vBond Orchestrator to the Overlay Network

After you create a minimal configuration for Cisco vBond Orchestrator, you must add it to overlay network by making Cisco vManage aware of Cisco vBond Orchestrator. When you add Cisco vBond Orchestrator, a signed certificate is generated and is used to validate and authenticate the orchestrator.

Add Cisco vBond Orchestrator and Generate Certificate

To add Cisco vBond Orchestrator to the network, automatically generate the CSR, and install the signed certificate:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, from **Add Controller** drop-down, select **vBond**.
3. In the **Add vBond** window:
   a. Enter the vBond management IP address.
   b. Enter the username and password to access Cisco vBond Orchestrator.
   c. Choose the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
   d. Click **Add**.

Cisco vManage generates the CSR, retrieves the generated certificate, and automatically installs it on Cisco vBond Orchestrator. The new controller device is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

Verify Certificate Installation

To verify that the certificate is installed on Cisco vBond Orchestrator:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Choose the new device listed, and check in the Certificate Status column to ensure that the certificate has been installed.

Add Cisco vSmart Controller to the Overlay Network

After you create a minimal configuration for Cisco vSmart Controller, you must add it to an overlay network by making Cisco vManage aware of the controller. When you add Cisco vSmart Controller, a signed certificate is generated and is used to validate and authenticate the controller.

Cisco vManage can support up to 20 Cisco vSmart Controllers in the network.

Add a Cisco vSmart Controller and Generate Certificate

To add a Cisco vSmart Controller to the network, automatically generate the CSR, and install the signed certificate:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and from the **Add Controller** drop-down menu, choose **vSmart**.
3. In the **Add vSmart** window:
   a. Enter the system IP address of Cisco vSmart Controller.
   b. Enter the username and password to access Cisco vSmart Controller.
   c. Choose the protocol to use for control-plane connections. The default is DTLS.
   d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.
   e. Check the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
   f. Click **Add**.

Cisco vManage automatically generates the CSR, retrieves the generated certificate, and installs it on Cisco vSmart Controller. The new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details.

Verify Certificate Installation

To verify that the certificate is installed on a Cisco vSmart Controller:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Choose the new controller listed and check in the Certificate Status column to ensure that the certificate has been installed.

Note If Cisco vSmart Controller and Cisco vBond Orchestrator have the same system IP addresses, they do not appear in Cisco vManage as devices or controllers. The certificate status of Cisco vSmart Controller and Cisco vBond Orchestrator is also not displayed. However, the control connections still successfully comes up.

What's Next

See *Deploy the vEdge Routers*.

Apply Policy to a Zone Pair

Table 5: Feature History

Feature Name	Release Information	Description
Self Zone Policy for Zone-Based Firewalls	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature allows you to define firewall policies for incoming and outgoing traffic between a self zone of an edge router and another zone. When a self zone is configured with another zone, the traffic in this zone pair is filtered as per the applied firewall policy.

Note For IPSEC overlay tunnels in Cisco SD-WAN, if a self zone is chosen as a zone pair, firewall sessions are created for SD-WAN overlay BFD packets if inspect action is configured for UDP.

However, for GRE overlay tunnels, if you chose a self zone as a zone pair with the inspect action of protocol 47, firewall sessions are created only for TCP, UDP, ICMP packets; but not BFD packets.

Warning Control connections may be impacted when you configure drop action from self-zone to VPN0 and vice versa. This applies for DTLS/TLS, BFD packets, and IPsec overlay tunnel.

Note On a Cisco vEdge device, packets to and from the management interface under VPN 512 do not go through the firewall module.

To apply policy to a zone pair:

1. Create security policy using Cisco vManage. For information see, Start the Security Policy Configuration Wizard.
2. Click **Apply Zone-Pairs**.
3. In the **Source Zone** field, choose the zone that is the source of the data packets.
4. In the **Destination Zone** field, choose the zone that is the destination of the data packets.

   Note You can choose self zone for either a source zone or a destination zone, not both.

5. Click the plus (+) icon to create a zone pair.
6. Click **Save**.
7. At the bottom of the page, click **Save Firewall Policy** to save the policy.

8. To edit or delete a firewall policy, click the **...**, and choose the desired option.
9. Click **Next** to configure the next security block in the wizard. If you do want to configure other security features in this policy, click **Next** until the Policy Summary page is displayed.

Note When you upgrade to Cisco SD-WAN Release 20.3.3 and later releases from any previous release, traffic to and from a service VPN IPSEC interface is considered to be in the service VPN ZBFW zone and not a VPN0 zone. This could result in the traffic getting blackholed, if you allow traffic flow only between service VPN and VPN0 and not the intra service VPN.

You have to make changes to your ZBFW rules to accommodate this new behavior, so that the traffic flow in your system is not impacted. To do this, you have to modify your intra area zone pair to allow the required traffic. For instance, if you have a policy which has the same source and destination zones, you have to ensure the zone-policy allows the required traffic.

Attach and Detach a Device Template

To configure a device on the network, you attach a device template to the device. You can attach only one device template to a device, so the template—whether you created it by consolidating individual feature templates or by entering a CLI text-style configuration—must contain the complete configuration for the device. You cannot mix and match feature templates and CLI-style configurations.

On Cisco Cisco vEdge devices in the overlay network, you can perform the same operations, in parallel, from one or more vManage servers. You can perform the following template operations in parallel:

- Attach a device template to devices
- Detach a device template from a device
- Change the variable values for a device template that has devices attached to it

For template operations, the following rules apply:

- When a device template is already attached to a device, you can modify one of its feature templates. Then when you click **Update** > **Configure Devices**, all other template operations—including attach devices, detach devices, and edit device values—are locked on all vManage servers until the update operation completes. This means that a user on another vManage server cannot perform any template operations until the update completes.
- You can perform the attach and detach device template operations on different devices, from one or more vManage servers, at the same time. However, if any one of these operations is in progress on one vManage server, you cannot edit any feature templates on any of the servers until the attach or detach operation completes.

Note You need to recreate the feature templates as the templates created prior to Cisco vManage Release 20.5 fails when attached to the device.

If the device being configured is present and operational on the network, the configuration is sent to the device immediately and takes effect immediately. If the device has not yet joined the network, the pushing of the configuration to the device is scheduled. When the device joins the network, Cisco vManage pushes the configuration immediately after it learns that the device is present in the network.

Attach a Device Template to Devices

You can attach the same templates to multiple devices, and you can do so simultaneously, in a single operation.

To attach a device template to one or more devices:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** and select the desired template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Attach Devices**. The **Attach Devices** dialog box opens with the **Select Devices** tab selected
4. In the **Available Devices** column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.
5. Click the arrow pointing right to move the device to the **Selected Devices** column on the right.
6. Click **Attach**.
7. If the template contains variables, enter the missing variable values for each device you selected in one of the following ways:
   - Enter the values manually for each device either in the table column or by clicking **...** and **Edit Device Template**. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
   - Click **Import File** to upload a CSV file that lists all the variables and defines each variable's value for each device.
8. Click **Update**
9. Click **Next**.

   If any devices have the same system IP address, a dialog box appears or an error message is displayed when you click **Next**. Modify the system IP addresses so that there are no duplicates, and click **Save**. Then click **Next** again.
10. In the left pane, select the device, to preview the configuration that is ready to be pushed to the device. The right pane displays the device's configuration and the **Config Preview** tab is selected. Click the **Config Diff** tab to view the differences between this configuration and the configuration currently running on the device, if applicable. Click the **Back** button to edit the variable values entered in the previous screen.
11. If you are attaching a Cisco vEdge device, click **Configure Device Rollback Timer** to configure the time interval at which the device rolls back to its previous configuration if the router loses its control connection to the overlay network. **The Configure Device Rollback Time** dialog box is displayed.

a. From the **Devices** drop-down list, select a device.

b. To enable the rollback timer, in the **Set Rollback slider**, drag the slider to the left to enable the rollback timer. When you do this, the slider changes in color from gray to green.

c. To disable the rollback timer, click the **Enable Rollback** slider. When you disable the timer, the Password field dialog box opens. Enter the password that you used to log in to the vManage NMS.

d. In the **Device Rollback Time slider**, drag the slider to the desired value. The default time is 5 minutes. You can configure a time from 6 to 15 minutes.

e. To exclude a device from the rollback timer setting, click **Add Exception** and select the devices to exclude.

f. The table at the bottom of the **Configure Device Rollback Time** dialog box lists all the devices to which you are attaching the template and their rollback time. To delete a configured rollback time, click the **Trash** icon from the device name.

g. Click **Save**.

12. Click **Configure Devices** to push the configuration to the devices. The **Status** column displays whether the configuration was successfully pushed. Click the right angle bracket to display details of the push operation.

Export a Variables Spreadsheet in CSV Format for a Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** and select the desired template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Export CSV**.

Configure Basic System Parameters

Use the System template for all Cisco SD-WAN devices.

To configure system-wide parameters using Cisco vManage templates:

1. Create a **System** feature template to configure system parameters.
2. Create an **NTP** feature template to configure NTP servers and authentication.
3. Configure the organization name and Cisco vBond Orchestrator IP address on the Cisco vManage. These settings are appended to the device templates when the templates are pushed to devices.

Create System Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.

2. Click **Device Templates**, and click **Create Template**.

> **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. To create a custom template for System, select the **Factory_Default_System_Template** and click **Create Template**.

   The System template form is displayed. This form contains fields for naming the template, and fields for defining the System parameters.
6. In **Template Name**, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
7. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down to the left of the parameter field and select one of the following:

Table 6:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco SD-WAN device to a device template. When you click **Device Specific**, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco SD-WAN device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Basic System-Wide Configuration

To set up system-wide functionality on a Cisco SD-WAN device, select the **Basic Configuration** tab and then configure the following parameters. Parameters marked with an asterisk are required.

Table 7:

Parameter Field	Description
Site ID* (on routers, vManage instances, and vSmart controllers)	Enter the identifier of the site in the Cisco SD-WAN overlay network domain in which the device resides, such as a branch, campus, or data center. The site ID must be the same for all Cisco SD-WAN devices that reside in the same site.*Range:* 1 through 4294967295 (2^{32} – 1)
System IP*	Enter the system IP address for the Cisco SD-WAN device, in decimal four-part dotted notation. The system IP address provides a fixed location of the device in the overlay network and is a component of the device's TLOC address. It is used as the device's loopback address in the transport VPN (VPN 0). You cannot use this same address for another interface in VPN 0.
Timezone*	Select the timezone to use on the device.
Hostname	Enter a name for the Cisco SD-WAN device. It can be up to 32 characters.
Location	Enter a description of the location of the device. It can be up to 128 characters.
Device Groups	Enter the names of one or more groups to which the device belongs, separated by commas.
Controller Groups	List the Cisco vSmart Controller groups to which the router belongs.
Description	Enter any additional descriptive information about the device.
Console Baud Rate	Select the baud rate of the console connection on the router. *Values:* 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps). *Default:* 115200 bps
Maximum OMP Sessions	Set the maximum number of OMP sessions that a router can establish to a Cisco vSmart Controller. *Range*: 0 through 100. *Default:* 2
Dedicated Core for TCP Optimization (optional, on vEdge 1000 and 2000 routers only)	Click **On** to carve out a separate CPU core to use for performing TCP optimization.

To save the feature template, click **Save**.

CLI equivalent:

```
 system
clock timezone timezone
 console-baud-rate rate
controller-group-list numbers
description text
device-groups group-name
host-name string
location string
max-omp-sessions  number
site-id site-id
```

```
system-ip ip-address
tcp-optimization-enabled
```

To configure the DNS name or IP address of the Cisco vBond Orchestrator in your overlay network, go to **Administration** > **Settings** screen and click **vBond**.

Configure the GPS Location

To configure a device location, select the **GPS** tab and configure the following parameters. This location is used to place the device on the Cisco vManage network map. Setting the location also allows Cisco vManage to send a notification if the device is moved to another location.

Table 8:

Parameter Field	Description
Latitude	Enter the latitude of the device, in the format *decimal-degrees*.
Longitude	Enter the longitude of the device, in the format *decimal-degrees*.

To save the feature template, click **Save**.

CLI equivalent:

```
 system  gps-location  (latitude decimal-degrees | longitude decimal-degrees)
```

Configure Interface Trackers for NAT Direct Internet Access

Table 9: Feature History

Feature Name	Release Information	Description
Support for Interface Status Tracking on Cisco vEdge Devices	Cisco vManage Release 17.2.2	This feature supports interface tracking on Cisco vEdge devices.
Dual Endpoint Support for Interface Status Tracking on Cisco vEdge Devices	Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature allows you to configure tracker groups with dual endpoints using the **Cisco System** template and associate each template group to an interface. The dual endpoints provide redundancy for tracking the status of transport interfaces to avoid false negatives.

The DIA tracker helps determine if the internet or external network becomes unavailable. This feature is useful when NAT is enabled on a transport interface in VPN 0 to allow data traffic from the router to exit directly to the internet.

If the internet or external network becomes unavailable, the router continues to forward traffic based on the NAT route in the service VPN. Traffic that is forwarded to the internet gets dropped. To prevent the internet-bound traffic from being dropped, configure the DIA tracker on the edge router to track the status of the transport interface. The tracker periodically probes the interface IP address of the end point of the tunnel interface to determine the status of the transport interface. The tracker determines the status of the internet and returns the data to the attach points that are associated with the tracker.

When the tracker is configured on the transport interface, the interface IP address is used as a source IP address for probe packets.

IP SLA monitors the status of probes and measures the round trip time of these probe packets and compares the values with the configured latency in the probe. When the latency exceeds the configured threshold value, the tracker considers the network as unavailable.

If the tracker determines that the local internet is unavailable, the router withdraws the NAT route and reroutes the traffic based on the local routing configuration to overlay.

The local router continues to periodically check the status of the path to the interface. When it detects that the path is functioning again, the router reinstalls the NAT route to the internet.

Starting Cisco SD-WAN Release 20.6.1 you can configure a tracker group with dual endpoints on Cisco vEdge devices (using two trackers) and associate this tracker group to an interface. Dual endpoints help in avoiding false negatives that might be introduced regarding unavailability of the internal or external network.

Restrictions for Configuring Tracker Groups for Dual Endpoints

A tracker group with dual endpoints can only be configured on the following types of interfaces:

- Ethernet Interfaces
- Subinterfaces
- PPPoE Interfaces

Configure NAT DIA Tracker

To track the status of transport interfaces that connect to the internet (Network Address Translation Direct Internet Access (NAT DIA)), click **Tracker** > **Add New Tracker** and configure the following parameters:

Table 10:

Parameter Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters. You can configure up to eight trackers.
Tracker Type	Choose an interface, static route, or a tracker group. Starting Cisco SD-WAN Release 20.6.1 you can configure a tracker group with dual endpoints on Cisco vEdge devices and associate this tracker group to an interface. Choose **Tracker** type as **Interface** for NAT DIA and dual endpoint tracker configuration.
Tracker Type: Tracker Elements	This field is displayed only if you chose **Tracker Type** as a tracker-group. Add the existing interface tracker names (separated by a space). When you add this tracker to the template, the tracker group is associated with these individual trackers and you can then associate the tracker group to an interface.

Parameter Field	Description
Tracker Type: Tracker Boolean	This field is displayed only if you chose **Tracker Type** as a tracker-group. Select **AND** or **OR** explicitly. An **OR** operation ensures that the transport interface status is reported as active if either one of the associated trackers of the tracker group report that the interface is active. If you select the **AND** operation, the transport interface status is reported as active if both the associated trackers of the tracker group report that the interface is active.
Threshold	How long to wait for the probe to return a response before declaring that the transport interface is down. *Range:* 100 through 1000 milliseconds. *Default:* 300 milliseconds.
Interval	How often probes are sent to determine the status of the transport interface. *Range:* 10 through 600 seconds. *Default:* 60 seconds (1 minute)
Multiplier	Number of times to resend probes before declaring that the transport interface is down. *Range:* 1 through 10. *Default:* 3
End Point Type: IP Address	IP address of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface. **Note** In Cisco SD-WAN Release 20.5.1 and later releases, if the tracker receives an HTTP response status code, which is less than 400, the endpoint is reachable. Prior to Cisco SD-WAN Release 20.5.1, the endpoint is reachable if the tracker receives an HTTP response status code of 200.
End Point Type: DNS Name	DNS name of the end point of the tunnel interface. This is the destination in the internet to which the router sends probes to determine the status of the transport interface.

To save a tracker, click **Add**.

To save the feature template, click **Save**.

Configure NAT DIA Tracker Using the CLI

Configure NAT DIA tracker

```
system
   tracker tracker-name
   endpoint-dns-name dns-name
   endpoint-ip ip-address
   interval seconds
   multiplier number
   threshold milliseconds
```

Configure tracker group and assign it to an interface

Note You can configure only one endpoint per tracker.

```
system
 tracker nat-tracker1
  endpoint-ip 10.1.1.1
 !
 tracker nat-tracker2
  endpoint-ip 10.2.2.2
 !
 tracker nat-tracker3
  tracker-type tracker-group
  boolean or
  tracker-elements nat-tracker1 nat-tracker2
  !
 !
vpn 0
 interface ge0/1
  nat
  tracker nat-tracker3
  !
 !
```

Verify dual endpoints configuration

```
vEdge1# show running-config system | begin tracker

 tracker nat-tracker1
  endpoint-ip 10.1.1.1
 !
 tracker nat-tracker2
  endpoint-ip 10.2.2.2
 !
 tracker nat-tracker3
  boolean          or
  tracker-type     tracker-group
  tracker-elements nat-tracker1 nat-tracker2
 !

vEdge1# show tracker tracker-group

                                                             TRACKER  TRACKER
                                               TRACKER       ELEMENT  ELEMENT
VPN  INTERFACE  TRACKER NAME  BOOLEAN  STATUS  ELEMENT NAME  STATUS   RTT
-------------------------------------------------------------------------------
0    ge0_1      nat-tracker3  or       DOWN    nat-tracker1  DOWN     Timeout
                                               nat-tracker2  DOWN     Timeout
```

Apply Tracker to an Interface

To apply a tracker to an interface, configure it in the **VPN Interface Cellular**, **VPN Interface Ethernet**, **VPN Interface NAT Pool**, or **VPN Interface PPP** configuration templates. You can apply only one tracker to an interface.

A tracker group with dual endpoints can only be configured on the following types of interfaces:

- Ethernet Interfaces
- Subinterfaces

- PPPoE Interfaces

Monitor NAT DIA Endpoint Tracker Configuration

1. From the Cisco vManage menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices.
3. Click **Real Time**.
4. From the **Device Options** drop-down list, choose **Dual Endpoint Tracker Info**.

Configure Advanced Options

To configure additional system parameters, click **Advanced**:

Table 11:

Parameter Name	**Description**
Control Session Policer Rate	Specify a maximum rate of DTLS control session traffic, to police the flow of control traffic. *Range:* 1 through 65535 pps. *Default:* 300 pps
MTU of DTLS Tunnel	Specify the MTU size to use on the DTLS tunnels that send control traffic between Cisco SD-WAN devices. *Range:* 500 through 2000 bytes. *Default:* 1024 bytes
Port Hopping	Click **On** to enable port hopping, or click **Off** to disable it. When a Cisco SD-WAN device is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other Cisco SD-WAN devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. To disable port hopping on an individual TLOC (tunnel interface), use the VPN Interface Ethernet configuration template. *Default:* Enabled (on routers); disabled (on Cisco vManage devices and Cisco vSmart Controllers).
Port Offset	Enter a number by which to offset the base port number. Configure this option when multiple Cisco SD-WAN devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections. *Values:* 0 through 19
DNS Cache Timeout	Specify when to time out the Cisco vBond Orchestrator addresses that have been cached by the device. *Range:* 1 through 30 minutes. *Default:* 30 minutes
Track Transport	Click **On** to regularly check whether the DTLS connection between the device and a Cisco vBond Orchestrator is up. Click **Off** to disable checking. By default, transport checking is enabled.
Local vBond (only on routers acting as vBond orchestrators)	Click **On** to configure the router to act as a Cisco vBond Orchestrator. Then specify the DNS name for the Cisco vBond Orchestrator or its IP address, in decimal four-part dotted notation.

Parameter Name	Description
Track Interface	Set the tag string to include in routes associated with a network that is connected to a non-operational interface. *Range:* 1 through 4294967295
Multicast Buffer	Specify the percentage of interface bandwidth that multicast traffic can use. *Range:* 5% through 100% *Default:* 20%
USB Controller (on vEdge 1000 and 2000 series routers only)	Click **On** to enable or click **Off** to disable the USB controller, which drives the external USB ports. If you enable the USB controller, the vEdge router reboots when you attach the device template to the device. *Default:* Disabled
Gateway Tracking	Click **On** to enable or click **Off** to Disable tracking of default gateway. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the device's route table. *Default:* Enabled
Host Policer Rate (on vEdge routers only)	Specify the maximum rate at which a policer delivers packets to the control plane. *Range:* 1000 through 20000 pps. *Default:* 5000 pps
ICMP Error Rate (on vEdge routers only)	Specify how many ICMP error messages a policer can generate or receive. *Range:* 1 through 200 pps *Default:* 100 pps
Allow Same-Site Tunnel (on vEdge routers only)	Click **On** to allow tunnels to be formed between vEdge routers in the same site. Note that no BFD sessions are established between the two collocated vEdge routers. *Default:* Off
Route Consistency Check (on vEdge routers only)	Click **On** to check whether the IPv4 routes in the device's route and forwarding table are consistent.
Collect Admin Tech on Reboot	Click **On** to collect admin-tech information when the device reboots.
Idle Timeout	Set how long the CLI is inactive on a device before the user is logged out. If a user is connected to the device via an SSH connection, the SSH connection is closed after this time expires. *Range:* 0 through 300 seconds. *Default:* CLI session does not time out.
Eco-Friendly Mode (on vEdge Cloud routers only)	Click **On** to configure a Cloud router not to use its CPU minimally or not at all when the router is not processing any packets.

To save the feature template, click **Save**.

CLI equivalent:

```
system
   admin-tech-on-failure  allow-same-site-tunnels
   control-session-pps rate eco-friendly-mode
   host-policer-pps rate

   icmp-error-pps rate

   idle-timeout seconds multicast-buffer-percent percentage

   port-hop  port-offset number route-consistency-check
   system-tunnel-mtu bytes timer
    dns-cache-timeout minutes track-default-gateway
    track-interface-tag number

   track-transport  upgrade-confirm minutes [no] usb-controller (on Cisco vEdge 1000 and
Cisco vEdge2000 routers only)
   vbond  (dns-name | ip-address) local (on Cisco vEdge routers acting as Cisco vBond
controllers)
```

Release Information

Introduced in Cisco vManage in Release 15.2. In Releases 15.3.8 and 15.4.3, add Track Interface field. In Release 17.1.0, add Route Consistency Check and Collect Admin Tech on Reboot fields. In Release 17.2.0, add support for CLI idle timeout and eco-friendly mode. In Release 17.2.2, add support for interface status tracking.

Configure the Cluster IP Address of a Cisco vManage Server

When you start Cisco vManage for the first time, the default IP address of the Cisco vManage server is shown as localhost. Before you can add a new Cisco vManage server to a cluster, you must change the localhost address of the primary Cisco vManage server to an out-of-band IP address. (From Cisco vManage Release 20.6.1, the primary Cisco vManage server has the Compute+Data persona.) Servers in the cluster use this out-of-band IP address to communicate with each other.

If you need to change the out-of-band IP address in the future, contact your Cisco support representative.

Cluster interconnection between Cisco vManage servers requires that each of the servers be assigned a static IP address. We recommend that you do not use DHCP to assign IP addresses to Cisco vManage servers that are to be a part of a cluster. Configure the IP address on a nontunnel interface in VPN 0.

Before you configure the cluster IP address of a Cisco vManage server, ensure that out-of-band IP addresses have been configured on VPN0 for its server interfaces. This configuration typically is done when the server is provisioned. The port type for an out-of-band IP address must be **service** for the IP address to be available for assigning to a Cisco vManage server.

Configure the IP Address for Releases Before Cisco vManage Release 20.6.1

Configure the IP address of a Cisco vManage server before you add the server to the cluster. To do so for releases before Cisco vManage Release 20.6.1, follow these steps:

1. From the Cisco vManage menu, choose **Administration** > **Cluster Management** and click **Service Configuration**.
2. Click **Add vManage**.

   The **Edit vManage** dialog box opens.
3. From the **vManage IP Address** drop-down list, choose an IP address to assign to the Cisco vManage server.
4. Enter the user name and password for logging in to the Cisco vManage server.
5. Click **Update**.

The Cisco vManage server reboots and displays the **Cluster Management** window.

Configure the IP Address for Cisco vManage Release 20.6.1 and Later Releases

Configure the IP address of a Cisco vManage server before you add the server to the cluster. To do so from Cisco vManage Release 20.6.1, perform the following steps.

Perform this procedure on the primary Cisco vManage server (which has the Compute+Data persona).

1. From the Cisco vManage menu, choose **Administration** > **Cluster Management**.

   The **Cluster Management** window is displayed. The table on this window lists the Cisco vManage servers that are in the cluster.

2. Click **...** adjacent to the Cisco vManage server to configure and click **Edit**.

   The **Edit vManage** dialog box is displayed.

3. In the **Edit vManage** dialog box, perform the following actions.

Note You cannot change the persona of a server. So the Node Persona options are disabled.

   a. From the **vManage IP Address** drop-down list, choose an out-of-band static IP address to assign to the server.

   b. In the **Username** field, enter the user name for logging in to the server.

   c. In the **Password** field, enter the password for logging in to the server.

   d. (Optional) Click **Enable SD-AVC** if you want Cisco Software-Defined Application Visibility and Control (SD-AVC) to run on the server.

      Cisco SD-AVC is a component of Cisco Application Visibility and Control (AVC). It can be enabled on only one Cisco vManage server. The server on which it is enabled must have the Compute+Data or the Compute persona. Cisco SD-AVC cannot be enabled on a server that has the Data persona.

Note If Cisco vManage is set up as a cluster and the cluster crashes as a result of a reboot or upgrade, the connection to the edge device is reset and the custom app ceases to function.

To resolve this and to resume operation, redefine the custom application name with a new, unique name. For more information to define custom applications, see the Define Custom Applications Using Cisco vManage chapter of the *Cisco SD-WAN Policies Configuration Guide*.

   e. Click **Update**.

      The server reboots and displays the **Cluster Management** window.

Change Configuration Modes

A device can be in either of these configuration modes:

- vManage mode–A template is attached to the device and you cannot change the configuration on the device by using the CLI.

- CLI mode – No template is attached to the device and the device can be configured locally by using the CLI.

When you attach a template to a device from vManage, it puts the device in vManage mode. You can change the device back to CLI mode if needed to make local changes to its configuration.

To toggle a router from vManage mode to CLI mode:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List**, and select a device.
3. Click the **Change Mode** drop-down list and select **CLI mode**.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

To toggle a controller device from vManage mode to CLI mode:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and select a device.
3. Click the **Change Mode** drop-down list.
4. Select **CLI mode** and then select the device type. The **Change Mode - CLI** window opens.
5. From the **vManage mode** pane, select the device and click the right arrow to move the device to the **CLI mode** pane.
6. Click **Update to CLI Mode**.

An SSH window opens. To log in to the device, enter a username and password. You can then issue CLI commands to configure or monitor the device.

Clone Service Groups

Table 12: Feature History

Feature Name	Release Information	Description
Clone Service Groups in Cisco vManage	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	You can easily create copies of service groups, download, and upload service group configuration properties using Cisco vManage.

When you clone or create copies of service chains, remember the following:

- Cisco vManage copies all configuration information of a service group to a cloned service group regardless of whether the cloned service group is attached to a cluster.
- Verify the CSV file and ensure that configuration information has a matching service group name during CSV file upload. Otherwise, an unmatched service group name can result in an error message during CSV file upload.

- To get an updated list of service group configuration values, always download service group configuration properties from the service group design view.

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud OnRamp for Colocation**

Step 2 Click **Service Group**.
The service group configuration page appears and all the service groups are displayed.

Step 3 For the desired service group, click **...** and choose **Clone Service Group**.

A clone of the original service group appears in the service group design view. Note the following points:

- By default, the cloned service group name and VM names are suffixed with a unique string.
- To view any VM configuration, click a VM in service chains.
- Cisco vManage marks the service chains that require configuration as **Unconfigured**, next to the edit button of the service chain.

Step 4 Modify the service group name, if required. Provide a description for the service group.

Step 5 To configure a service chain, use one of the following methods:

- Click the edit button for a service chain, enter the values, and then click **Save**.
- Download the configuration values from a CSV file, modify the values, upload the file, and then click **Save**. See Steps 6, 7, 8 on how to download, modify, and upload a CSV file.

The cloned service group appears on the service group configuration page. You can now download the updated service group configuration values.

Step 6 To download the cloned service group configuration values, do one of the following:

Note The download and upload of a CSV file is supported for creating, editing, and cloning of the service groups that aren't attached to a cluster.

- On the service group configuration page, click a cloned service group, click **More Actions** to the right of the service group, and choose **Download Properties (CSV)**.
- In the service group design view, click **Download CSV** in the upper right corner of the screen.

Cisco vManage downloads all configuration values of the service group to an Excel file in CSV format. The CSV file can consist of multiple service groups and each row represents configuration values for one service group. To add more rows to the CSV file, copy service group configuration values from existing CSV files and paste them in this file.

For example, ServiceGroup1_Clone1 that has two service chains with one VM in each of the service chains is represented in a single row.

Note In the Excel file, the headers and their representation in the service chain design view is as follows:

- sc1/name represents the name of the first service chain.
- sc1/vm1/name represents the name of the first VNF in the first service chain.
- sc2/name represents the name of the second service chain.
- sc2/vm2/name represents the name of the second VNF in the second service chain.

Step 7 To modify service group configuration values, do one of the following:

- To modify the service group configuration in the design view, click a cloned service group from the service group configuration page.

  Click any VM in service chains to modify the configuration values, and then click **Save**.

- To modify the service group configuration using the downloaded Excel file, enter the configuration values in the Excel file manually. Save the Excel file in CSV format.

Step 8 To upload a CSV file that includes all the configuration values of a service group, click a service group in the service group configuration page, and then click **Upload CSV** from the right corner of the screen.

Click **Browse** to choose a CSV file, and then click **Upload**.

You can view the updated values displayed for the service group configuration.

Note You can use the same CSV file to add configuration values for multiple service groups. But, you can update configuration values for a specific service group only, when uploading a CSV file using Cisco vManage.

Step 9 To know the representation of service group configuration properties in the CSV file and Cisco vManage design view, click a service group from the service group configuration page.

Click **Show Mapping Names**.

A text appears next to all the VMs in the service chains. Cisco vManage displays this text after mapping it with the configuration properties in the CSV file.

Cisco SD-WAN Multitenancy

Enable Multitenancy on Cisco vManage

Prerequisites

Do not migrate an existing single-tenant Cisco vManage into multitenant mode, even if you invalidate or delete all devices from the existing Cisco vManage. Instead, download and install a new software image of Cisco vManage Release 20.6.1 or a later release.

Note After you enable multitenancy on Cisco vManage, you cannot migrate it back to single tenant mode.

1. Launch Cisco vManage using the URL `https://vmanage-ip-address:port`. Log in as the provider **admin** user.
2. From the Cisco vManage menu, choose **Administration** > **Settings**.
3. In the **Tenancy Mode** bar, click the **Edit**.
4. In the **Tenancy** field, click **Multitenant**.
5. In the **Domain** field, enter the domain name of the service provider (for example, managed-sp.com).
6. Enter a **Cluster Id** (for example, cluster-1 or 123456).

7. Click **Save**.
8. Click **Proceed** to confirm that you want to change the tenancy mode.

   Cisco vManage reboots in multitenant mode and when a provider user logs in to Cisco vManage, the provider dashboard appears.

Note The **Domain** and **Cluster Id** values created in steps 5 and 6 serve as the Provider FQDN. Ensure these values conform to current DNS naming conventions. You can not modify these values after the configuration is saved. To change these values, a new Cisco vManage cluster need to be deployed. For more details on Provider and Tenant DNS requirements, see step 3.d in Add a New Tenant.

Add Cisco vSmart Controller to Cisco SD-WAN Multitenant Deployment

1. Log in to Cisco vManage as the provider **admin** user.
2. From the Cisco vManage menu, choose **Configuration** > **Devices**.
3. Click **Controllers**.
4. Click **Add Controller** and click **vSmart**.
5. In the **Add vSmart** dialog box, do the following:
   a. In the **vSmart Management IP Address** field, enter the system IP address of the Cisco vSmart Controller.
   b. Enter the **Username** and **Password** required to access the Cisco vSmart Controller.
   c. Select the protocol to use for control-plane connections. The default is **DTLS**.

      If you select **TLS**, enter the port number to use for TLS connections. The default is 23456.
   d. Check the **Generate CSR** check box for Cisco vManage to create a Certificate Signing Request.
   e. Click **Add**.
6. From the Cisco vManage menu, choose **Configuration** > **Certificates**.

   For the newly added Cisco vSmart Controller, the **Operation Status** reads **CSR Generated**.
   a. For the newly added Cisco vSmart Controller, click **More Options** icon and click **View CSR**.
   b. Submit the CSR to the Certificate Authority (CA) and obtain a signed certificate.
7. From the Cisco vManage menu, choose **Configuration** > **Certificates**.
8. Click **Install Certificate**.
9. In the **Install Certificate** dialog box, paste the **Certificate Text** or click **Select a file** upload the certificate file. Click **Install**.

   Cisco vManage installs the certificate on the Cisco vSmart Controller. Cisco vManage also sends the serial number of the certificate to other controllers.

On the **Configuration** > **Certificates** page, the **Operation Status** for the newly added Cisco vSmart Controller reads as **vBond Updated**.

On the **Configuration** > **Devices** page, the new controller is listed in the Controller table with the controller type, hostname of the controller, IP address, site ID, and other details. The **Mode** is set to **CLI**.

10. Change the mode of the newly added Cisco vSmart Controller to **vManage** by attaching a template to the device.

a. From the Cisco vManage menu, choose **Configuration** > **Templates**.

b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

c. Find the template to be attached to the Cisco vSmart Controller.

d. Click **...**, and click **Attach Devices**.

e. In the **Attach Devices** dialog box, move the new controller to the **Selected Device** list and click **Attach**.

f. Verify the **Config Preview** and click **Configure Devices**.

Cisco vManage pushes the configuration from the template to the new controller.

In the **Configuration** > **Devices** page, the **Mode** for the Cisco vSmart Controller shows **vManage**. The new Cisco vSmart Controller is ready to be used in your mutitenant deployment.

Add a New Tenant

Table 13: Feature History

Feature Name	Release Information	Description
Tenant Device Forecasting	Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	While adding a new tenant to the multitenant Cisco SD-WAN deployment, a service provider can forecast the number of WAN edge devices that the tenant may deploy in their overlay network. Cisco vManage enforces this forecast limit. If the tenant tries to add devices beyond this limit, Cisco vManage responds with an appropriate error message and the device addition fails.

Prerequisites

- At least two Cisco vSmart Controllers must be operational and in the `vManage` mode before you can add new tenants.

  A Cisco vSmart Controller enters the `vManage` mode when you push a template onto the controller from Cisco vManage. A Cisco vSmart Controller in the `CLI` mode cannot serve multiple tenants.

- Each pair of Cisco vSmart Controllers can serve a maximum of 24 tenants and a maximum of 1000 tenant devices. Ensure that there at least two Cisco vSmart Controllers that can serve a new tenant. If no pair of Cisco vSmart Controllers in the deployment can serve a new tenant, add two Cisco vSmart Controllers and change their mode to `vManage`.

- If you add a second tenant immediately after adding a tenant, Cisco vManage adds them sequentially, and not in parallel.

- Each tenant must have a unique Virtual Account (VA) on **Plug and Play Connect** on Cisco Software Central. The tenant VA should belong to the same Smart Account (SA) as the provider VA.

- For an on-premises deployment, create a Cisco vBond Orchestrator controller profile for the tenant on **Plug and Play Connect**. The fields in the following table are mandatory.

  Table 14: Controller Profile Fields

Field	Description/Value
Profile Name	Enter a name for the controller profile.
Multi-Tenancy	From the drop-down list, select **Yes**.
SP Organization Name	Enter the provider organization name.
Organization Name	Enter the tenant organization name in the format `<SP Org Name>-<Tenant Org Name>`. **Note** The organization name can be up to 64 characters.
Primary Controller	Enter the host details for the primary Cisco vBond Orchestrator.

  For a cloud deployment, the Cisco vBond Orchestrator controller profile is created automatically as part of the tenant creation process.

1. Log in to Cisco vManage as the provider **admin** user.
2. From the Cisco vManage menu, choose **Administration** > **Tenant Management**.
3. Click **Add Tenant**. In the **Add Tenant** dialog box:
   a. Enter a name for the tenant.

      For a cloud deployment, the tenant name should be same as the tenant VA name on **Plug and Play Connect**.

   b. Enter a description of the tenant.

      The description can be up to 256 characters and can contain only alphanumeric characters.

c. Enter the name of the organization.

The organization name is case-sensitive. Each tenant or customer must have a unique organization name.

Enter the organization name in the following format:

```
<SP Org Name>-<Tenant Org Name>
```

For example, if the provider organization name is 'multitenancy' and the tenant organization name is 'Customer1', while adding the tenant, enter the organization name as **multitenancy-Customer1**.

Note The organization name can be up to 64 characters.

d. In the **URL Subdomain Name** field, enter the fully qualified sub-domain name of the tenant.

- The sub-domain name must include the domain name of the service provider. For example, for the managed-sp.com service provider, a valid domain name can be customer1.managed-sp.com.

Note The service provider name is shared amongst all tenants. Hence, ensure that the URL naming convention follows the same domain name convention that was provided while enabling multitenancy from **Administration** > **Settings** > **Tenancy Mode**.

- For an on-premises deployment, add the fully qualified sub-domain name of the tenant to the DNS. Map the fully qualified sub-domain name to the IP addresses of the three Cisco vManage instances in the Cisco vManage cluster.
  - **Provider Level**: Create DNS A record and map it to the IP addresses of the Cisco vManage instances running in the Cisco vManage cluster. The A record is derived from the domain and Cluster ID that was created in steps 5 and 6 in Enable Multitenancy on Cisco vManage. For example, if domain is **sdwan.cisco.com** and Cluster ID is **vmanage123**, then A record will need to be configured as **vmanage123.sdwan.cisco.com**.

Note If you fail to update DNS entries, it will result in authentication errors when logging in to Cisco vManage. Validate DNS is configured correctly by executing **nslookup vmanage123.sdwan.cisco.com**.

  - **Tenant Level**: Create DNS CNAME records for each tenant created and map them to the FQDN created at the Provider Level. For example, if domain is **sdwan.cisco.com** and tenant name is **customer1** the CNAME record will need to be configured as **customer1.sdwan.cisco.com**.

Note Cluster ID is not required for CNAME record. Validate DNS is configured correctly by executing **nslookup customer1.sdwan.cisco.com**.

For a cloud deployment, the fully qualified sub-domain name of the tenant is automatically added to the DNS as part of the tenant creation process. After you add a tenant, it could take up to an hour before the fully qualified sub-domain name of the tenant can be resolved by the DNS.

e. In the **Number of Devices** field, enter the number of WAN edge devices that the tenant can deploy.

   If the tenant tries to add WAN edge devices beyond this number, Cisco vManage reports an error and the device addition fails.

f. Click **Save**.

   The **Create Tenant** screen appears, and the **Status** of the tenant creation reads **In progress**. To view status messages related to the creation of a tenant, click the > button to the left of the status.

   Cisco vManage does the following:

   - creates the tenant
   - assigns two Cisco vSmart Controllers to serve the tenant and pushes a CLI template to these controllers to configure tenant information
   - sends the tenant and Cisco vSmart Controller information to Cisco vBond Orchestrators.

What to do next:

After the **Status** column changes to **Success**, you can view the tenant information on the **Administration** > **Tenant Management** page.

Modify Tenant Information

1. Log in to Cisco vManage as the provider **admin** user.
2. From the Cisco vManage menu, choose **Administration** > **Tenant Management**.
3. In the left pane, click the name of the tenant.

   The tenant information is displayed in a pane on the right.
4. To modify tenant data, do as follows:

   a. In the right pane, click the pencil icon.

   b. In the **Edit Tenant** dialog box, you can modify the following:

      - **Description**: The description can be up to 256 characters and can contain only alphanumeric characters.
      - **Forecasted Device**: The number of WAN edge devices that the tenant can deploy.

        A tenant can add a maximum of 1000 devices.

Note

This option is available from Cisco SD-WAN Release 20.6.2, Cisco vManage Release 20.6.2.

If you increase the number of devices that a tenant can deploy, you must add the required number of device licenses to the tenant virtual account on **Plug and Play Connect** on Cisco Software Central.

Before you increase the number of devices that a tenant can deploy, ensure that the Cisco vSmart Controller pair assigned to the tenant can support this increased number. A pair of Cisco vSmart Controllers can support a maximum of 24 tenants and 1000 devices across all these tenants.

- **URL Subdomain Name**: Modify the fully qualified sub-domain name of the tenant.

c. Click **Save**

Delete a Tenant

Before you delete a tenant, delete all tenant WAN edge devices. See Delete a WAN Edge Device from a Tenant Network.

1. Log in to Cisco vManage as the provider **admin** user.
2. From the Cisco vManage menu, choose **Administration** > **Tenant Management**.
3. In the left pane, click the name of the tenant.

   The tenant information is displayed in a pane on the right.
4. To delete the tenant, do as follows:
   a. In the right pane, click the trash icon.
   b. In the **Delete Tenant** dialog box, enter the provider **admin** password and click **Save**.

View OMP Statistics per Tenant on a Cisco vSmart Controller

1. Log in to Cisco vManage as the provider **admin** user.
2. From the Cisco vManage menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor** > **Network**.
3. In the table of devices, click on the hostname of a Cisco vSmart Controller.
4. In the left pane, click **Real Time**.
5. In the **Device Options** field, enter `OMP` and select the OMP statistics you wish to view.
6. In the **Select Filters** dialog box, click **Show Filters**.
7. Enter the **Tenant Name** and click **Search**.

Cisco vManage displays the selected OMP statistics for the particular tenant.

View Tenants Associated with a Cisco vSmart Controller

1. Log in to Cisco vManage as the provider **admin** user.
2. Click a **vSmart** connection number to display a table with detailed information about each connection.

   Cisco vManage displays a table that provides a summary of the Cisco vSmart Controllers and their connections.
3. For a Cisco vSmart Controller, click **...** and click **Tenant List**.

   Cisco vManage displays a summary of tenants associated with the Cisco vSmart Controller.

Manage Tenant WAN Edge Devices

Add a WAN Edge Device to a Tenant Network

Note If you are adding a WAN edge device that you had previously invalidated and deleted from an overlay network, you must reset the device software after adding the device. To reset the software on a Cisco vEdge device, use the command **request platform software reset**.

1. Log in to Cisco vManage.

   If you're a provider user, log in as the **admin**. In the provider dashboard, choose a tenant from the drop-down list to enter the provider-as-tenant view.

   If you're a tenant user, log in as the **tenantadmin**.
2. Upload the device serial number file to Cisco vManage.
3. Validate the device and send details to controllers.
4. Create a configuration template for the device and attach the device to the template.

   While configuring the device, configure the service provider organization name and the tenant organization name as in the following example:

   ```
   sp-organization-name multitenancy
   organization-name multitenancy-Customer1
   ```

   Note Enter the `organization-name` in the format `<SP Org Name>-<Tenant Org Name>`.
5. Bootstrap the device using bootstrap configuration generated through Cisco vManage or manually create the initial configuration on the device.
6. If you are using Enterprise Certificates to authenticate the device, download the CSR from Cisco vManage and get the CSR signed by the Enterprise CA. Install the certificate on Cisco vManage.

Delete a WAN Edge Device from a Tenant Network

1. Log in to Cisco vManage.

   If you're a provider user, log in as the **admin**. In the provider dashboard, choose a tenant from the drop-down list to enter the provider-as-tenant view.

   If you're a tenant user, log in as the **tenantadmin**.

2. Detach the device from any configuration templates.

3. Delete a WAN Edge Router.

Flexible Tenant Placement on Multitenant Cisco vSmart Controllers

Table 15: Feature History

Feature Name	Release Information	Description
Flexible Tenant Placement on Multitenant Cisco vSmart Controllers	Cisco vManage Release 20.9.1	With this feature, while onboarding a tenant to a multitenant deployment, you can choose the pair of multitenant Cisco vSmart Controllers that serve the tenant. After onboarding a tenant, you can migrate the tenant to a different pair of multitenant Cisco vSmart Controllers, if necessary.

Assign Cisco vSmart Controllers to Tenants During Onboarding

Prerequisites

- At least two Cisco vSmart Controllers must be operational and in the vManage mode before you can add new tenants.

  A Cisco vSmart Controller enters the **vManage** mode when you push a template to the controller from Cisco vManage. A Cisco vSmart Controller in the **CLI** mode cannot serve multiple tenants.

- Each pair of Cisco vSmart Controllers can serve a maximum of 24 tenants and a maximum of 1000 tenant devices. Ensure that there are at least two Cisco vSmart Controllers that can serve a new tenant. If no pair of Cisco vSmart Controllers in the deployment can serve a new tenant, add two Cisco vSmart Controllers and change their mode to **vManage**.

- Add up to 16 tenants in a single operation. If you add more than one tenant, during the **Add Tenant** task, Cisco vManage adds the tenants one after another and not in parallel.

  While an **Add Tenant** task is in progress, do not perform a second tenant addition operation. If you do so, the second Add Tenant task fails.

- Each tenant must have a unique Virtual Account (VA) on Plug and Play Connect on Cisco Software Central. The tenant VA should belong to the same Smart Account (SA) as the provider VA.

- For an on-premises deployment, create a Cisco vBond Orchestrator controller profile for the tenant on Plug and Play Connect. The fields in the following table are mandatory.

Field	Description
Profile Name	Enter a name for the controller profile.
Multi-Tenancy	From the drop-down list, select **Yes**.
SP Organization Name	Enter the provider organization name.
Organization Name	Enter the tenant organization name in the format <SP Org Name>-<Tenant Org Name>. The organization name can be up to 64 characters.
Primary Controller	Enter the host details for the primary Cisco vBond Orchestrator.

  For a cloud deployment, the Cisco vBond Orchestrator controller profile is created automatically as part of the tenant creation process.

1. Log in to Cisco vManage as the provider **admin** user.
2. From the Cisco vManage menu, choose **Administration** > **Tenant Management**.
3. Click **Add Tenant**.
4. In the **Add Tenant** slide-in pane, click **New Tenant**.
5. Configure the following tenant details:

Field	Description
Name	Enter a name for the tenant. For a cloud deployment, the tenant name should be same as the tenant VA name on Plug and Play Connect.
Description	Enter a description for the tenant. The description can have up to 256 characters and can contain only alphanumeric characters.
Organization Name	Enter the name of the tenant organization. The organization name can have up to 64 characters. The organization name is case-sensitive. Each tenant or customer must have a unique organization name. Enter the organization name in the following format: `<SP Org Name>-<Tenant Org Name>` For example, if the provider organization name is ‘managed-sp’ and the tenant organization name is 'customer1', while adding the tenant, enter the organization name as ‘managed-sp-customer1’.

Field	Description
URL Subdomain	

Field	Description
	Enter the fully qualified subdomain name of the tenant. • The subdomain name must include the domain name of the service provider. For example, for the managed-sp.com service provider, a valid domain name for customer1 is customer1.managed-sp.com. **Note** The service provider name is shared amongst all tenants. Ensure that the URL naming convention follows the same domain name convention that was followed while enabling multitenancy using **Administration** > **Settings** > **Tenancy Mode**. • For an on-premises deployment, add the fully qualified subdomain name of the tenant to the DNS. Map the fully qualified subdomain name to the IP addresses of the three Cisco vManage instances in the Cisco vManage cluster. • Provider DNS: Create a DNS A record and map it to the IP addresses of the Cisco vManage instances running in the Cisco vManage cluster. The A record is derived from the provider's domain name and the cluster ID that was created while enabling multitenancy on Cisco vManage. For example, if the provider's domain name is `sdwan.cisco.com` and the cluster ID is `vmanage123`, configure the A record as `vmanage123.sdwan.cisco.com`. **Note** If you fail to add the DNS A record, you will experience authentication errors when logging in to Cisco vManage. Validate that the DNS is configured correctly by using the **nslookup** command. Example: `nslookup vmanage123.sdwan.cisco.com .` • Tenant DNS: Create DNS CNAME records for each tenant that you created and map them to the provider FQDN. For example, if the provider's domain name is `sdwan.cisco.com` and tenant name is `customer1`, configure the CNAME record as `customer1.sdwan.cisco.com`. Cluster ID is not required in the CNAME record. Validate that the DNS is configured correctly by using the **nslookup** command. Example: `nslookup customer1.sdwan.cisco.com`. • For a cloud deployment, the fully qualified subdomain name of the tenant is automatically added to the DNS as part of the tenant creation process. After you add a tenant, it could take up to an hour before the fully qualified subdomain name of

Field	Description
	the tenant can be resolved by the DNS.
Forecasted Devices	Enter the number of WAN edge devices that the tenant can add to the overlay. If the tenant tries to add WAN edge devices beyond this number, Cisco vManage reports an error and the device addition fails.

Field	Description
Select two vSmarts	

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td></td><td>
<ul>
<li>Automatic tenant placement: Ensure that the <b>Select two vSmarts</b> field has the value <b>Autoplacement</b>. This is the default configuration.</li>
<li>Flexible tenant placement:
<ol type="a">
<li>Click the <b>Select two vSmarts</b> drop-down list.
Cisco vManage lists the hostnames of the available Cisco vSmart Controllers. For each Cisco vSmart Controller, Cisco vManage shows whether the controller is reachable and reports the following utilization details:
<table>
<tr><td>Tenant hosting capacity</td><td>Each Cisco vSmart Controller can serve a maximum of 24 tenants. Tenant hosting capacity represents the number of tenants to which the Cisco vSmart Controller is assigned in the form of a percentage. This value indicates whether you can assign another tenant to this controller.</td></tr>
<tr><td>Used device capacity</td><td>Each Cisco vSmart Controller can support a maximum of 1000 tenant WAN edge devices. Used device capacity represents the number of tenant WAN edge devices connected to the Cisco vSmart Controller in the form of a percentage of the maximum capacity (1000 WAN edge devices). This value indicates whether the Cisco vSmart Controller can support the number of devices forecast for the tenant that you are onboarding.</td></tr>
<tr><td>Memory utilized</td><td>This value represents memory consumption as a percentage.</td></tr>
<tr><td>CPU utilized</td><td>This value represents CPU usage as a percentage.</td></tr>
</table>
</li>
<li>Select two Cisco vSmart Controllers to assign to the</li>
</ol>
</li>
</ul>
</td></tr>
</table>

Field	Description
	tenant based on the utilization details. To select a Cisco vSmart Controller, check the check box adjacent to its hostname.

6. To save the tenant configuration, click **Save**.
7. To add another tenant, repeat Step 4 to Step 6.
8. To onboard tenants to the deployment, click **Add**.

Cisco vManage initiates the Create Tenant Bulk task to onboard the tenants.

As part of this task, Cisco vManage performs the following activities:

- creates the tenant
- assigns two Cisco vSmart Controllers to serve the tenant and pushes a CLI template to these controllers to configure tenant information
- sends the tenant and Cisco vSmart Controller information to Cisco vBond Orchestrators

When the task is successfully completed, you can view the tenant information, including the Cisco vSmart Controllers assigned to the tenant, on the **Administration** > **Tenant Management** page.

Update Cisco vSmart Controllers Placement For a Tenant

You can migrate a tenant to a different pair of Cisco vSmart Controllers from the controllers that are currently assigned to the tenant. For instance, if you need to increase the tenant WAN edge device forecast and the controllers assigned to the tenant cannot connect to these revised number of tenant WAN edge devices, you can migrate the tenant to a pair of controllers that can accommodate the revised forecast.

If you wish to migrate a tenant to different pair of Cisco vSmart Controllers, you must change the Cisco vSmart Controllers that are assigned to the tenant one at a time. Doing so ensures that one of the Cisco vSmart Controllers is available to the tenant WAN edge devices during the migration and prevents disruptions in traffic.

1. Log in to Cisco vManage as the provider **admin** user.
2. From the Cisco vManage menu, choose **Administration** > **Tenant Management**.
3. For the tenant you wish to migrate to a different controller, click **…** adjacent to the tenant organization name.
4. Click **Update vSmart Placement**.
5. In the **Update vSmart Placement** slide-in pane, configure the following:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>Source vSmart (currently applied)</b></td><td>
<ol type="a">
<li>Click the <b>Source vSmart (currently applied)</b> drop-down list.
Cisco vManage lists the hostnames of the Cisco vSmart Controllers assigned to the tenant. For each Cisco vSmart Controller, Cisco vManage shows whether the controller is reachable and reports the following utilization details:
<table>
<tr><td>Tenant hosting capacity</td><td>Each Cisco vSmart Controller can serve a maximum of 24 tenants. Tenant hosting capacity represents the number of tenants to which the Cisco vSmart Controller is assigned in the form of a percentage. This value indicates whether you can assign another tenant to this controller.</td></tr>
<tr><td>Used device capacity</td><td>Each Cisco vSmart Controller can support a maximum of 1000 tenant WAN edge devices. Used device capacity represents the number of tenant WAN edge devices connected to the Cisco vSmart Controller in the form of a percentage of the maximum capacity (1000 devices). This value indicates whether the Cisco vSmart Controller can support the number of devices forecast for the tenant that you are onboarding.</td></tr>
<tr><td>Memory utilized</td><td>This value represents memory consumption as a percentage.</td></tr>
<tr><td>CPU utilized</td><td>This value represents CPU usage as a percentage.</td></tr>
</table>
</li>
<li>Check the check box adjacent to the hostname of one of the Cisco vSmart Controllers assigned to the tenant.</li>
</ol>
</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td><b>Destination vSmart</b></td><td>
<b>a.</b> Click the <b>Destination vSmart</b> drop-down list.
Cisco vManage lists the hostnames of the available Cisco vSmart Controllers that are not assigned to the tenant. For each Cisco vSmart Controller, Cisco vManage shows whether the controller is reachable and reports the following utilization details:
<table>
<tr><td>Tenant hosting capacity</td><td>Each Cisco vSmart Controller can serve a maximum of 24 tenants. Tenant hosting capacity represents the number of tenants to which the Cisco vSmart Controller is assigned in the form of a percentage. This value indicates whether you can assign another tenant to this controller.</td></tr>
<tr><td>Used device capacity</td><td>Each Cisco vSmart Controller can support a maximum of 1000 tenant WAN edge devices. Used device capacity represents the number of tenant WAN edge devices connected to the Cisco vSmart Controller in the form of a percentage of the maximum capacity (1000 devices). This value indicates whether the Cisco vSmart Controller can support the number of devices forecast for the tenant that you are onboarding.</td></tr>
<tr><td>Memory utilized</td><td>This value represents memory consumption as a percentage.</td></tr>
<tr><td>CPU utilized</td><td>This value represents CPU usage as a percentage.</td></tr>
</table>
<b>b.</b> Check the check box adjacent to the hostname of the Cisco vSmart Controller you want to assign to the tenant.
If you select a Cisco vSmart Controller that does not have the required capacity to serve the tenant devices, the update operation fails.
</td></tr>
</table>

6. Click **Update**.

7. To change the other Cisco vSmart Controller that is assigned to the tenant, repeat Step 3 to Step 6.

Cisco vManage initiates the Tenant vSmart Update task to assign the selected Cisco vSmart Controller to the tenant, migrating the tenant details from the Cisco vSmart Controller that was previously assigned. When the task is successfully completed, you can view the tenant information, including the Cisco vSmart Controllers assigned to the tenant, on the **Administration** > **Tenant Management** page.

Configure Application Probe Class through vManage

Table 16: Feature History

Feature Name	Release Information	Description
Per-Class Application-Aware Routing	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This release supports Per-class application-aware routing to Cisco SD-WAN. You can configure Application Probe Class using Cisco vManage.

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. In **Centralized Policy**, click **Add Policy**. The **Create Groups of Interest** page appears.
3. Choose the list type **App Probe Class** from the left navigation panel to create your groups of interest.
4. Click **New App Probe Class**.
5. Enter the probe class name in the **Probe Class Name** field.
6. Choose the required forwarding class from the **Forwarding Class** drop-down list.

   If there are no forwarding classes, then create a class from the **Class Map** list page under the **Localized Policy Lists** in the **Custom Options** menu.

   To create a forwarding class:

   a. In the **Custom Options** drop-down, choose **Lists** from the Localized Policy options.

   b. In the Define Lists window, choose the list type **Class Map** from the left navigation panel.

   c. Click **New Class List** to create a new list.

   d. Enter **Class** and choose the **Queue** from the drop-down list.

   e. Click **Save**.

7. In the **Entries** pane, choose the appropriate color from the **Color** drop-down list and enter the **DSCP** value.

   Click **+** sign, to add more entries as required.

8. Click **Save**.

Configure Authorization and Accounting

Table 17: Feature History

Feature Name	Release Information	Description
Authorization and Accounting	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	You can configure authorization, which authorizes commands that a user enter on a device before the commands can be executed, and accounting, which generates a record of commands that a user executes on a device.

Navigating to the Template Screen and Naming the Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and click **Create Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. From the **Create Template** drop-down list, select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you are creating the template.
5. Select **Basic Information**.
6. To create a custom template for AAA, select Factory_Default_AAA_Template and click **Create Template**. The AAA template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining AAA parameters.
7. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
8. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the **Scope** drop-down list to the left of the parameter field and select one of the following:

Table 18:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco vEdge device to a device template . When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco vEdge device to a device template. For more information, see Create a Template Variables Spreadsheet . To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configuring Authorization

You can configure authorization, which causes the device to authorize commands that users enter on a device before the commands can be executed.

Configuring authorization involves creating one or more tasks. A task consists of a set of operational commands and a set of configuration commands. Operational commands are show commands and exec commands. Configuration commands are the XPath of configuration commands.

You define the default user authorization action for each command type. The default action can be accept or deny. You also can define user authorization accept or deny actions for individual commands or for XPath strings within a command type. In this way, you can override the default action for specific commands as needed.

A task is mapped to a user group, so all users in the user group are granted the authorizations that the command sets in the task define.

To configure authorization, choose the **Authorization** tab, click **+ New Task**, and configure the following parameters:

Table 19:

Parameter Name	Description
Name	Enter a unique name for the task

Parameter Name	Description
+ Add Oper	Click to add a set of operational commands. In the Add Oper window that pops up: **1.** From the **Default action** drop-down list, choose the default authorization action for operational commands. Choose **accept** to grant user authorization by default, or choose **deny** to prevent user authorization by default. **2.** To designate specific operational commands for which user authorization is granted or denied authorization, click **+ Add Oper** to expand the Add Oper area. In the **Oper** field that displays, click **accept** to grant user authorization for a command, or click **deny** to prevent user authorization for a command, and enter the command in the **CLI** field. Then click **Add** in the Add Oper area. Do not include quotes or a command prompt when entering a command. For example, **config terminal** is a valid entry, but **"config terminal"** is not valid. Repeat this Step 2 as needed to designate other commands. The actions that you specify here override the default action. In this way, you can designate specific commands that are not authorized when the default action is accept, and designate specific commands that are authorized when the default action is deny. To remove a specific command, click the trash icon on the right side of its line in the table at the bottom of the Add Oper window. **3.** Click **Add** at the bottom right of the Add Oper window.
+ Add Config	Click to add a set of XPath strings for configuration commands. In the Add Config window that pops up: **1.** From the **Default action** drop-down list, choose the default authorization action for configuration commands. Choose **accept** to grant user authorization by default, or choose **deny** to prevent user authorization by default. **2.** To designate specific configuration command XPath strings for which user is granted or denied authorization **Click + Add Config** to expand the Add Config area. In the **Config** field that displays, click **accept** to grant user authorization for an XPath, or click **deny** to prevent user authorization for an XPath, and enter the XPath string in the **CLI** field. Then click **Add** in the Add Config area. To display the XPath for a device, enter the **`show running-config | display xpath`** command on the device. Do not include quotes or a command prompt when entering an XPath string. Repeat this Step 2 as needed to designate other XPath strings. The actions that you specify here override the default action. In this way, you can designate specific XPath strings that are not authorized when the default action is accept, and designate specific XPath strings that are authorized when the default action is deny. To remove a specific command, click the trash icon on the right side of its line in the table at the bottom of the Add Config window. **3.** Click **Add** at the bottom right of the Add Config window.

To remove a task, click the trash icon on the right side of the task line.

After you create a tasks, perform these actions:

- Create or update a user group. Use the Custom feature type to associate one or more tasks with the user group by assigning read, write, or both privileges to each task. See Configure Local Access for Users and User Groups.

Note A user group can be associated with either a predefined task or with user-defined tasks. Associating a user group with a combination of both predefined and user-defined tasks is not supported.

- Add users to the user group. These users then receive the authorization for operational and configuration commands that the tasks that are associated with the user group define. See Configure Local Access for Users and User Groups.

  If a user is attached to multiple user groups, the user receives the authorization access that is configured for the last user group that was created.

CLI equivalent:

```
system aaa
   accounting
   task name
     config
       default-action {accept | deny}
       accept "xpath"
       deny "xpath"
     oper-exec
       default-action {accept | deny}
       accept "command"
       deny ""command-id
   usergroup group-name
     task authorization-task {read | write}
```

Configuring Accounting

You can configure accounting, which causes a TACACS+ server to generate a record of commands that a user executes on a device.

Note Accounting does not generate a record of CLI commands for Cisco vManage template configuration.

Prerequisites

- The TACACS+ server must be configured with a secret key on the **TACACS** tab
- The TACACS+ server must be configured as first in the authentication order on the **Authentication** tab

To configure accounting, choose the **Accounting** tab and configure the following parameter:

Table 20:

Parameter Name	Description
Enable/disable user accounting	Click **On** to enable the accounting feature. Click **Off** to disable this feature.

CLI equivalent:

```
system  aaa
   accounting
```

Configure Automatic Bandwidth Detection

Table 21: Feature History

Feature Name	Release Information	Description
Day 0 WAN Interface Automatic Bandwidth Detection	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	You can enable a device to automatically determine the bandwidth for WAN interfaces in VPN0 during day 0 onboarding by performing a speed test using an iPerf3 server.

You can configure the Cisco VPN Interface Ethernet template to cause a device to automatically detect the bandwidth for WAN interfaces in VPN0 during its day 0 onboarding. If you configure a template in this way, a Cisco IOS XE SD-WAN device attempts to determine the bandwidth for WAN interfaces in VPN0 after completing the PnP process.

Automated bandwidth detection can provide more accurate day 0 bandwidth configuration than manual configuration because there is limited user traffic that can affect results.

A device determines the bandwidth by performing a speed test using an iPerf3 server. iPerf3 is a third-party tool that provides active measurements of bandwidth on IP networks. For more information, see the Iperf.fr website.

If a device has a connection to the internet, the device uses a public iPerf3 server for automatic bandwidth detection, unless you specify a private iPerf3 server. If a device has a connection to a private circuit and no internet connection, you must specify a private iPerf3 server for automatic bandwidth detection.

We recommend that you specify a private iPerf3 server. If a private iPerf3 server is not specified, the device pings a system defined set of public iPerf3 servers and selects for the speed test the public server with the minimum hops value or, if all servers have the same minimum hops value, the server with the minimum latency value. If the speed test fails, the device selects another public server from the list. The device continues to select other public iPerf3 servers until the speed test is successful or until it has tried all servers. Therefore, a speed test on a public iPerf3 server can use a server that is far away, resulting in a larger latency than the minimum.

The set of system defined public iPerf3 servers includes the following:

- iperf.scottlinux.com
- iperf.he.net

- bouygues.iperf.fr
- ping.online.net
- iperf.biznetnetworks.com

The following settings on the Cisco vManage VPN Interface Ethernet template control bandwidth detection. These settings are supported for WAN interfaces in VPN0 only.

- **Auto Detect Bandwidth**—When enabled, the device detects the bandwidth.
- **Iperf Server**—To use a private iPerf3 server for automatic bandwidth detection, enter the IPv4 address of the private server. To use a public iPerf3 server for automatic bandwidth detection, leave this field blank.

  The private iPerf3 server should run on port 5201, which is the default iPerf3 port.

In addition, automatic bandwidth detection requires that the allow-service all command be configured for the tunnel interface. See “VPN, Interface, and Tunnel Configuration for WAN and LAN interfaces.”

The device writes the results of a speed test to the auto_speedtest.json file in its bootflash directory. It also displays the results in the **Auto Upstream Bandwidth (bps)** and **Auto Downstream Bandwidth (Mbps)** areas on the **Monitor** > **Devices** > **Interface** page of Cisco vManage.

If a device does not receive a response from an iPerf3 server, an error is recorded in the auto_speedtest.json file and displays on the **Monitor** > **Devices** > **Interface** page of Cisco vManage.

Note In Cisco vManage Release 20.6.x and earlier releases, the speed test results are displayed on the **Monitor** > **Network** > **Interface** page.

CLI Equivalent

`auto-bandwidth-detect`

`iperf-server` *ipv4-address*

There also is a no auto-bandwidth-detect form of this command.

Example

```
Device# show sdwan running-config sdwan
sdwan
 interface GigabitEthernet0/0/0
  tunnel-interface
   encapsulation gre
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
  auto-bandwidth-detect
  iperf-server 192.0.2.255
 exit
 appqoe
  no tcpopt enable
  no dreopt enable
```

Configure Backup Server Settings

Table 22: Feature History

Feature Name	Release Information	Description
RMA Support for Cisco CSP Devices	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	You can configure the **Backup** information to enter storage server settings and backup intervals.

Points to Consider

- If you don't use an NFS server, Cisco vManage can’t successfully create backup copies of a CSP device for future RMA requirements.
- The NFS server mount location and configurations are same for all the CSP devices in a cluster.
- Don't consider an existing device in a cluster as the replacement CSP device.

Note If a replacement CSP device isn’t available, wait until the device appears in Cisco vManage.

- Don't attach further service chains to a cluster after you identify that a CSP device in the cluster is faulty.
- The backup operation on a CSP device creates backup files containing NFVIS configuration and VMs (if VMs are provisioned on the CSP device). You can use the following information for reference.
  - An automated backup file is generated and is in the format:

    serial_number + "_" + time_stamp + ".bkup"

    For example,

    `WZP22180EW2_2020_06_24T18_07_00.bkup`
  - An internal state model is maintained that specifies the status of the overall backup operation and internal states of each backup component:
    - NFVIS: A configuration backup of the CSP device as an xml file, config.xml.
    - VM_Images: All VNF tar.gz packages in `data/intdatastore/uploads` which are listed individually.
    - VM_Images_Flavors: The VM images such as, img_flvr.img.bkup.

    - Individual tar backups of the VNFs: The files such as, vmbkp.

  - The backup.manifest file contains information of files in the backup package and their checksum for verification during restore operation.

To create backup copies of all CSP devices in a cluster, perform the following steps:

1. On the **Cluster Topology** window, click **Add** next to **Backup**.

   To edit backup server settings, on the **Cluster Topology** window, click **Edit** next to **Backup**

   In the **Backup** configuration window, enter information about the following fields:

   - Mount Name—Enter the name of the NFS mount after mounting an NFS location.
   - Storage Space—Enter the disk space in GB.
   - Server IP: Enter the IP address of the NFS server.
   - Server Path: Enter the folder path of the NFS server such as, `/data/colobackup`
   - Backup: Click **Backup** to enable it.
   - Time: Set a time for scheduling the backup operation.
   - Interval: Choose from the options to schedule a periodic backup process.
     - Daily: The first backup is created a day after the backup configuration is saved on the device, and everyday thereafter.
     - Weekly: The first backup is created seven days after the backup configuration is saved on the device, and every week thereafter.
     - Once: The backup copy is created on a chosen day and it's valid for the entire lifetime of a cluster. You can choose a future calendar date.

2. Click **Save**.

3. To view the status of the previous five backup operations, use the **show hostaction backup status** command. To know about the backup status configuration command, see Backup and Restore NFVIS and VM Configurations. To use this command:

   a. In Cisco vManage, click the **Tools** > **SSH Terminal** screen to start an SSH session with Cisco vManage.

   b. Choose the CSP device.

   c. Enter the username and password for the CSP device and click **Enter** to log in to the CSP device and run the **show hostaction backup status** command.

Restore CSP Device

You can perform the restore operation only by using the CLI on the CSP device that you're restoring.

1. Use the **mount nfs-mount storage** command to mount NFS:

   For more information, see Network File System Support.

Note To access the backup file, the configuration for mounting an NFS file system should match the faulty device. You can view this information from other healthy CSP devices as the NFS mount location and configurations are same for all the CSP devices. To view and capture the information, you can do one of the following:

- In the **Cluster Topology** window, click **Add** next to **Backup**.
- Use the **show running-config** command to view the active configuration that is running on a CSP device.

mount nfs-mount storage { *mount-name* | **server_ip** *server_ip* | **server_path** *server_path* | **storage_space_total_gb** *storage_space_total_gb* | **storage_type** *storage_type* }

For example, `mount nfs-mount storage nfsfs/ server_ip 172.19.199.199 server_path /data/colobackup/ storage_space_total_gb 100.0 storagetype nfs`

2. Restore the backup information on a replacement CSP device using the **hostaction restore** command:

   For example,

```
hostaction restore except-connectivity file-path
nfs:nfsfs/WZP22180EW2_2020_06_24T18_07_00.bkup
```

Note Specify the except-connectivity parameter to retain the connectivity with the NFS server mounted in Step 2.

3. Use the **show hostaction backup status** command to view the status of the previous five backup images and their operational status.

   Also, you can view the backup images from the notifications available on the Cisco vManage **Monitor** > **Logs** > **Events** page.

Note In Cisco vManage Release 20.6.x and earlier releases, you can view the backup images from the notifications available on the Cisco vManage **Monitor** > **Events** page.

4. Use the **show hostaction restore-status** command on the CSP device to view the status of the overall restore process and each component such as system, image and flavors, VM and so on.
5. To fix any failure after viewing the status, perform a factory default reset of the device.

Note The factory default reset sets the device to default configuration. Therefore, before performing the restore operation from Steps 1-4 on the replacement device, verify that all the restore operation prerequisites are met.

To know more about how to configure the restore operation on CSP devices, see Backup and Restore NFVIS and VM Configurations.

Configure or Cancel vManage Server Maintenance Window

You can set or cancel the start and end times and the duration of the maintenance window for the vManage server.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. From **Maintenance Window**, click **Edit**.

   To cancel the maintenance window, click **Cancel**.
3. Click the **Start date and time** drop-down list, and select the date and time when the **Maintenance Window** will start.
4. Click the **End date and time** drop-down list, and select the date and time when the **Maintenance Window** will end.
5. Click **Save**. The start and end times and the duration of the maintenance window are displayed in the **Maintenance Window** bar.

Two days before the start of the window, the Cisco vManage Dashboard displays a maintenance window alert notification.

Configure a Cellular Gateway

Table 23: Feature History

Feature Name	Release Information	Feature Description
Cellular Gateway Configuration	Cisco vManage Release 20.4.1	You can configure a supported cellular gateway as an IP pass-through device from the Templates tab.

You can configure a supported cellular gateway as an IP pass-through device. By positioning the configured device in an area in your facility that has a strong LTE signal, the signal can be extended over an Ethernet connection to a routing infrastructure in a location with a weaker LTE signal.

To configure a cellular gateway in Cisco vManage:

1. Create a device template for the **Cisco Cellular Gateway CG418-E** device.

   See "Create a Device Template from Feature Templates" in *Systems and Interfaces Configuration Guide*.

   After you enter a description for the feature template:

   a. From the Cisco vManage menu, choose **Configuration** > **Templates**.

   b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

c. From the **Create Template** drop-down list choose **From Feature Template**.

d. From the **Device Model** drop-down list select the type of device for which you are creating the template.

e. Choose **Cellular Gateway** > **Cellular Gateway Platform** > **Create Template**. Then configure the Cellular Gateway Platform feature template as shown in the following table.

Table 24: Cellular Gateway Platform Template Parameters

Parameter Name	Description
Basic Configuration Tab	
Time Zone	Choose the time zone to use for the device. The device uses this time zone for clock synchronization when NTP is configured.
Management Interface	Enter the IPv4 address of the management interface for accessing the device.
Admin-Password	Enter the admin user password for logging in to the device by using an SSH client or a console port.
NTP-Servers	Configure one or more NTP servers to which the device synchronizes its clock.
Cellular Configuration Tab	
IP-Src-Violation	Choose **v4 only**, **v6 only**, or **v4 and v6** to enable the IP source violation feature for the corresponding IP address types. Choose **None** if you do not want to enable this feature.
Auto-SIM	Choose **On** to enable the auto-SIM feature. When this feature is enabled, the device automatically detects the service provider to which SIMs in the device belong and automatically loads the appropriate firmware for that provider.
Primary SIM Slot	Choose the slot that contains the primary SIM card for the device. If the device loses service to this slot, it fails over to the secondary slot.
Failover-Timer (minutes)	Enter the number of minutes that the device waits before trying to communicate with the primary SIM slot after the device detects loss of service to this slot.

Parameter Name	Description
Max-Retry	Enter the number of consecutive unsuccessful attempts by the device to communicate with the primary SIM before failing over to the secondary slot

f. Choose **Cellular Gateway** > **Cellular Gateway Profile** and choose **Create Template** from the Cellular Gateway Profile drop-down list. Then configure the Cellular Gateway Profile feature template as shown in the following table.

Table 25: Cellular Gateway Profile Template Parameters

Parameter Name	Description
Basic Configuration Tab	
SIM	Choose a SIM slot and configure the following options to create a profile for the SIM in that slot. This profile indicates to the service provider which of its cellular networks the SIM should attach to. • Profile ID: Enter a unique ID for the profile • Access Point Name: Enter the name of the access point for this profile • Packet Data Network Type: Choose the type of network for data services for this profile (**IPv4**, **IPv6**, or **IPv4v6**) • Authentication: Choose the authentication method that this profile uses for data, and enter the user name and password for this method in the Profile Username and Profile Password fields that display You can configure one profile for each SIM slot in the device.
Add Profile	Click to add an access point name (APN) profile that the cellular device uses to attach to a cellular network. You can add up to 16 profiles.
Profile ID	Enter a unique identifier for the profile. Valid values: Integers 1 through 16.
Access Point Name	Enter a name to identify the cellular access point.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network (**IPv4**, **IPv6**, or **IPv46**).

Parameter Name	Description
Authentication	Choose the authentication method that is used to attach to the cellular access point (**none**, **pap**, **chap**, **pap_chap**).
Profile Username	If you choose an authentication method other than **none**, enter the user name to use for authentication when attaching to the cellular access point.
Password	If you choose an authentication method other than **none**, enter the password to use for authentication when attaching to the cellular access point.
Add	Click to add the profile your are configuring.
Advanced Configuration Tab	
Attach Profile	Choose the profile that the device uses to connect to the cellular network.
Cellular 1/1 Profile	Choose the profile that the device uses for data connectivity over the cellular network.

2. Attach the device template to the device.

   See "Attach and Detach a Device Template" in *Systems and Interfaces Configuration Guide*.

Configure Cellular Profile

Use the Cellular Profile feature template to configure the profiles used by cellular modems on devices.

To configure a cellular profile using Cisco vManage templates:

1. Create a Cellular Profile template to configure the profiles used by the cellular modem, as described in this section.
2. Create a VPN-Interface-Cellular feature template to configure cellular module parameters.
3. Create a VPN feature template to configure VPN parameters. .

Create a Cellular Profile Feature Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Under **Device Templates**, click **Create Template** and choose **From Feature Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. From the **Device Model** drop-down list, choose the device for which you are creating the template.

4. Click **Cellular**.
5. In the **Cellular** area, click **Cellular Profile**.
6. In the **Cellular Profile** field, choose **Create Template** from the drop-down list.

   The Cellular-Profile template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining Cellular-Profile parameters.

Minimum Cellular Profile Configuration

The following table describes the parameters that are required to specify the cellular profile on the cellular modem of a device. Click **Save** after you enter the values for the template.

Parameter Name	Description
Template Name	Enter the template name. It can contain only alphanumeric characters.
Description (Template)	Enter a description for the template. It can contain only alphanumeric characters.
Interface name	Enter the name of the cellular interface, which must be cellular0.
Profile ID	Enter the identification number of the profile to be used on the device. You use this profile identification number when you configure for the cellular interface in the VPN-Interface-Cellular template. Range: 1 through 15.

CLI Equivalent

```
cellular cellular0
  profile number
```

Modify Cellular Profile Parameters

You can modify paramters of a profile if your service provider requires you to do so. For example, if you procure a data plan with static IP addresses, you might need to modify the APN field in the profile.

Parameter Name	Description
Access Point Name	Enter the name of the gateway between the service provider network and the public Internet. The name can contain up to 32 characters.
Authentication	Choose the authentication method used for the connection to the cellular network. It can be CHAP, None, PAP, or PAP/CHAP.
IP Address	Enter the static IP address assigned to the cellular interface. This field is used when the service provider requires that a static IP address be preconfigured before attaching to the network.

Parameter Name	Description
Profile Name	Enter a name to identify the cellular profile. The name can contain up to 14 characters.
Packet Data Network Type	Choose the packet data network (PDN) type of the cellular network. It can be IPv4, IPv6, or IPv46.
Profile Username	Enter the username to use when making cellular connections for web services. It can be 1 to 32 characters. It can contain any alphanumeric characters, including spaces.
Profile Password	Enter the user password to use when making cellular connections for web services. The password is case-sensitive and can be clear text, or an AES encrypted key.
Primary DNS Address	Enter the IP addresses of the primary DNS servers in the service provider network, in decimal four-part dotted notation.
Secondary DNS Address	Enter the IP addresses of the secondary DNS servers in the service provider network, in decimal four-part dotted notation.

Configure Certificate Revocation

Table 26: Feature History

Feature Name	Release Information	Feature Description
Certificate Revocation	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	You can revoke enterprise certificates from devices based on a certificate revocation list that Cisco vManage obtains from a root certificate authority.

Before You Begin

Make a note of the URL of the root CA CRL.

Procedure

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. In the **Administration Settings** window, click **Edit** next to **Certificate Revocation List**.

   The certificate revocation options appear.
3. Click **Enabled**.

4. In the **CRL Server URL** field, enter the URL of the CRL that you created on your secure server.
5. In the **Retrieval Interval** field, enter the interval, in hours, at which Cisco vManage retrieves the CRL from your secure server and revokes the certificates that the CRL designates.

   Enter a value from 1 to 24. The default retrieval interval is 1 hour.
6. Click **Save**.

   Cisco vManage immediately retrieves the CRL and revokes the certificates that the CRL designates. From then on, Cisco vManage retrieves the CRL according to the retrieval interval period that you specified.

Configure Certificate Settings

New controller devices in the overlay network—Cisco vManage instances, Cisco vBond Orchestrators, and Cisco vSmart Controllers—are authenticated using signed certificates. From Cisco vManage, you can automatically generate the certificate signing requests (CSRs), retrieve the generated certificates, and install them on all controller devices when they are added to the network.

Note All controller devices must have a certificate installed on them to be able to join the overlay network.

To automate the certificate generation and installation process, configure the name of your organization and certificate authorization settings before adding the controller devices to the network.

For more information on configuring certificate settings, see Certificates.

Configure Cisco SD-WAN Multi-Region Fabric

Table 27: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric (also Hierarchical SD-WAN)	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	You can use Cisco vManage to enable and configure Multi-Region Fabric, which provides the ability to divide the architecture of the Cisco SD-WAN overlay network into multiple regional networks that operate distinctly from one another.
Re-Origination Dampening	Cisco IOS XE Release 17.9.1a	In networks experiencing instability, TLOCs and bidirectional forwarding detection (BFD) tunnels may alternate repeatedly between being available and unavailable. This causes the overlay management protocol (OMP) to repeatedly withdraw and re-originate routes. This churn adversely affects Cisco vSmart controller performance. Adding a delay before re-originating routes that have gone down repeatedly prevents excessive churn, and prevents this type of network instability from diminishing Cisco vSmart controller performance.

Enable Multi-Region Fabric

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. In the **Multi-Region Fabric** area, enable Multi-Region Fabric.

Note In Cisco vManage Releases 20.7.x and 20.8.x, this area was labeled **Hierarchical SDWAN**.

Assign a Role and Region to a Device Using Cisco vManage

Before You Begin

- Plan the Multi-Region Fabric architecture, and decide on the roles (edge router or border router) and regions for each device in the network.
- This procedure uses a feature template to assign a role. For full information about configuring devices using templates, see Configure Devices.
- For information about the number of interfaces that are supported for each device, see the scale limitations in Restrictions for Multi-Region Fabric.
- From Cisco vManage Release 20.9.1, use Network Hierarchy and Resource Management to create the region that you will use in the following procedure. Creating the region includes assigning a region ID to the region. For information about creating a region, see the Network Hierarchy and Resource Management chapter in the *Cisco SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x*.

Assign a Role and Region to a Device

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Select the device type to display the templates available for the device.
5. Click the **System** template.
6. In the **Template Name** field, enter a name for the template.
7. In the **Basic Configuration** section, configure the following fields:

Field	Description
Region ID	Choose a value between 1 and 63 for a region. **Note** From Cisco vManage Release 20.9.1, enter the number of the region that you created for the device using Network Hierarchy and Resource Management, as described in Before You Begin. **Note** By default, all interfaces on the device use the region configured here. For a border router, configure one or more TLOC interfaces to connect to the core region. Other TLOC interfaces on the border router use the region configured here. See Assign Border Router TLOCs to the Core Region Using Cisco vManage.
Role	Choose **Edge Router** or **Border Router**. **Note** Only Cisco IOS XE SD-WAN devices can have the **Border Router** role.

8. For a border router, enable the device to function in the core region.

   a. From the Cisco vManage menu, choose **Configuration** > **Templates**.

   b. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

   c. Click **Add Template**.

   d. Select the device type to display the templates available for the device.

   e. Click the **Cisco VPN Interface Ethernet** template.

   f. In the **Tunnel** section, in the **Tunnel Interface** field, click **On** to enable tunnels.

   g. In the **Enable Core Region** field, click **On** to enable connections to the core region.

Assign Border Router TLOCs to the Core Region Using Cisco vManage

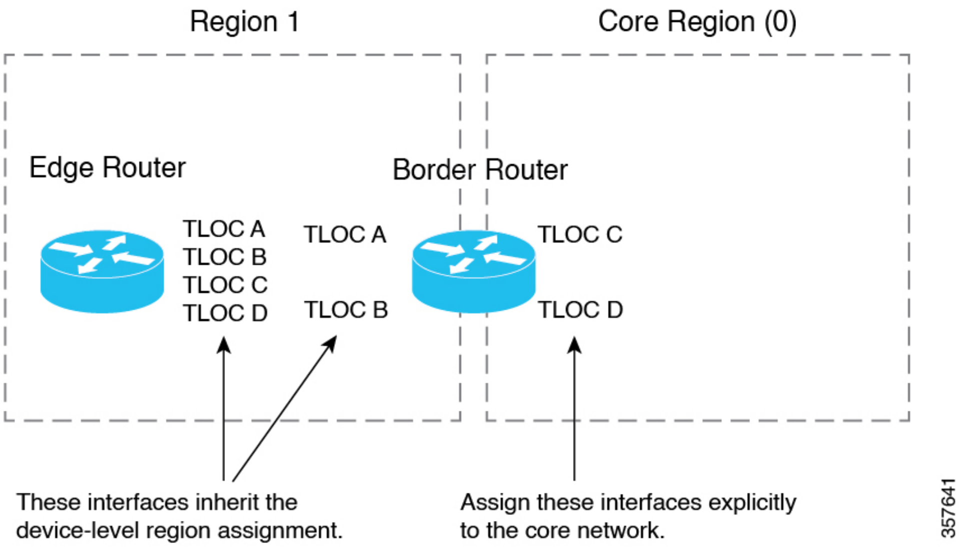
Before You Begin

- Assign the role of border router to the device and assign the device to a region. By default, all interfaces on a device use the region configured for the device. See Assign a Region and Role to a Device Using Cisco vManage.

  For a border router, configure one or more TLOC interfaces to connect to the core region. Other TLOC interfaces on the border router use the region configured for the device.

- This procedure creates a template that assigns interfaces of a specified color to the core region. Before creating the template, configure a color for the interfaces that you want to assign to the core region, or verify that they have a color configured already.

Figure 1: TLOC Interface Region Assignments


Region 1
Core Region (0)
Edge Router
Border Router
TLOC A
TLOC B
TLOC C
TLOC D
TLOC A
TLOC B
TLOC C
TLOC D
These interfaces inherit the device-level region assignment.
Assign these interfaces explicitly to the core network.
357641

Assign Border Router TLOCs to the Core Region

1. Create a Cisco VPN Interface Ethernet template for the TLOC interfaces that you want to connect to the core region.

   a. From the Cisco vManage menu, choose **Configuration** > **Templates**.

   b. Click **Feature Templates**.

   Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

   c. Click **Add Template**.

   d. In the **Template Name** field, provide a template name.

   e. In the **Tunnel** section, in the **Tunnel Interface** field, click **On**.

   f. In the **Color** field, specify a color that identifies the interfaces that you want to assign to the core region.

   g. Click **Advanced Options**.

   h. In the **Settings** section, in the **Enable Core Region** field, click **On**.

   i. In the **Basic Configuration** section, in the **Interface Name** field, enter an interface name.

   j. Click **Save**.

2. Add the Cisco VPN Interface Ethernet template that you created in the previous step to a device template.

a. From the Cisco vManage menu, choose **Configuration** > **Templates**.

b. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.

c. Click **Create Template** and choose **From Feature Template**.

d. In the **Transport & Management VPN** section, locate the **Additional Cisco VPN 0 Templates** list and click **Cisco VPN Interface Ethernet**.

   This adds a new line to the **Transport & Management VPN** section, labelled **Cisco VPN Interface Ethernet**, with a menu for selecting an interface.

e. In the new **Cisco VPN Interface Ethernet** line, click the menu and select the Cisco VPN Interface Ethernet template that you created in an earlier step.

f. Click **Update**.

3. Apply the device template to the border router device.

Assign Regions to a Cisco vSmart Controller Using Cisco vManage

Before You Begin

- Plan the Multi-Region Fabric architecture, and decide on the roles (edge router or border router) and regions for each device in the network. Plan which Cisco vSmart controllers should serve each region.
- This procedure uses a feature template to assign a role. For full information about configuring devices using templates, see Configure Devices.
- For restrictions that apply to Cisco vSmart controllers, see Restrictions for Multi-Region Fabric.

Assign Regions to a Cisco vSmart Controller

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. For the device type, select **vSmart**.
5. Click the **System** template.
6. In the **Template Name** field, enter a name for the template.
7. In the **Basic Configuration** section, in the **Region ID List** field, enter a region or region list.

8. Apply the template to the Cisco vSmart controller.

View OMP Peers Using Cisco vManage

1. From the Cisco vManage menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** at the right of the desired border router and choose **Real Time**.
3. In the left pane, click **Real Time**.
4. In the **Device Options** field, enter **OMP Peers**.

   A table shows peer information, similarly to the **show sdwan omp peers** CLI command. In the output, check the **REGION ID** column, which shows one of the following for each peer.

   - **None**: A Cisco vSmart controller that has not been configured to operate with Multi-Region Fabric. This includes the default region Cisco vSmart controllers configured before migration to Multi-Region Fabric.
   - **0**: Core region Cisco vSmart controllers.
   - *access-region-id*: Access region Cisco vSmart controllers.

Verify Connectivity Between Devices Using Cisco vManage

Use this procedure to trace the route between two devices, such as two edge devices in different regions to verify connectivity between the devices.

1. From the Cisco vManage menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** adjacent to the desired border router and choose **Real Time**.
3. In the left pane, click **Troubleshooting**.
4. Click **Trace Route**.
5. In the **Destination IP** field, enter an IP address for the endpoint of the route tracing.
6. Click the **VPN** drop-down list and choose the VPN for the route tracing.

Verify That a Border Router is Re-Originating Routes Using Cisco vManage

1. From the Cisco vManage menu, choose **Monitor** > **Devices**.
2. In the table of devices, click **…** adjacent to the desired border router and choose **Real Time**.
3. In the left pane, click **Real Time**.
4. In the **Device Options** field, enter **OMP Received Routes**.

Locate the rows of the table that show 0.0.0.0 in the **Peer** column. These rows correspond to routes from the border router itself. If the border router is re-originating routes, then in those rows, the **Region Path** column shows two numbers for the route, including a 0 for the core region, and the **Status** column shows **BR-R** (border router re-originated).

Use Regions With a Centralized Policy

Create a Region List Using Cisco vManage

Region lists are useful when creating a region match condition for a centralized policy.

Create a Region List

1. In the Cisco vManage menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. Click **Add Policy**.
4. In the list area, click **Region**.
5. Click **New Region List**.
6. Enter the following:
   - **Region List Name**: Name for the new list.
   - **Add Region**: One or more region numbers in the range of 1 to 63, using to the instructions in the field.
7. Click **Add**.

Add a Region Match Condition to a Centralized Policy

After you configure regions for Multi-Region Fabric, you can specify a region or region list as a match condition when configuring centralized route policy.

For complete information about working with centralized policy, see the Centralized Policy section of the Policies Configuration Guide for vEdge Routers.

Add a Region Match Condition to a Centralized Policy

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. Click **Custom Options** and in the **Centralized Policy** section, choose **Topology**.
3. Click **Add Topology** and choose **Custom Control**.
4. Click **Sequence Type** and choose **Route**.
5. Click **Sequence Rule**.
6. Click **Match**.
7. Click **Region**.
8. In the **Match Conditions** area, enter a region or region list.

   See Create a Region List Using Cisco vManage.

Attach a Centralized Policy to a Region

After you configure regions for Multi-Region Fabric, specify a region or region list when attaching a centralized policy.

For complete information about working with centralized policy, see the Centralized Policy section of the Policies Configuration Guide for vEdge Routers.

Attach a Centralized Policy to a Region

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policy**.
3. In the table, locate the policy to attach. In the row of the policy, click **…** and choose **Edit**.

   For the **Topology**, **Application-Aware Routing**, and **Traffic Data** options, you can choose to add a new site or new region.
4. Click **New Site/Region List**.
5. Click **Region**.
6. Enter a region ID or region list.
7. Proceed with attaching the policy.

Secondary Regions

Table 28: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric: Secondary Regions	Cisco IOS XE Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	Secondary regions provide another facet to the Multi-Region Fabric architecture and enable direct tunnel connections between edge routers in different primary access regions. When you assign an edge router a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions.

Configure a Secondary Region ID for an Edge Router Using Cisco vManage

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco vManage Release 20.8.1

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create a system template for the device.
   - In the table, locate the existing system template for the device. In the row for the template, click **…** and choose **Edit**.

4. In the **Basic Configuration** section, in the **Secondary Region ID** field, enable Global mode and enter the number of the secondary region, in the range 1 to 63.

5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure the Secondary Region Mode for a TLOC Using Cisco vManage

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco vManage Release 20.8.1

Before You Begin

This procedure describes how to configure the secondary region mode for a TLOC using a Cisco VPN Interface Ethernet template. For information about how to use the template in general, including how to specify the interface to which it is applied, see Configure VPN Ethernet Interface in the Cisco SD-WAN Systems and Interfaces Configuration Guide.

Configure the Secondary Region Mode for a TLOC

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates**.

3. Do one of the following:

   - Create a Cisco VPN Interface Ethernet template for the device.

   - In the table, locate the existing Cisco VPN Interface Ethernet template for the device. In the row for the template, click **…** and choose **Edit**.

4. Navigate to the **Tunnel** section, and within that section the **Advanced Options** section.

5. In the **Enable Secondary Region** field, enable Global mode and choose one of the following options:

Option	Description
Only in Secondary Region	Configure the interface to handle only traffic in the secondary region.
Shared Between Primary and Secondary Regions	Configure the interface to handle traffic in the primary and secondary regions.

Note The interface inherits the secondary region assignment configured for the device at the system level.

6. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure a Device to Use Both the Primary-Region Path and Secondary-Region Path Using Cisco vManage

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco vManage Release 20.8.1

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates**.
3. Do one of the following:
    - Create a Cisco OMP template for the device.
    - In the table, locate the existing OMP template for the device. In the row for the template, click **...** and choose **Edit**.
4. Navigate to the **Best Path** section, and in the **Ignore Region-Path Length During Best-Path Algorithm** field, choose **On**.

    When you select **On**, the template automatically selects **Direct-Tunnel Path** and **Hierarchical Path**.

    Note The default value is Off, and by default, OMP gives preference to a direct tunnel path over a hierarchical path because the direct path has fewer hops.

5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Transport Gateways

Table 29: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric: Transport Gateways	Cisco IOS XE Release 17.8.1a Cisco vManage Release 20.8.1	An edge router or border router that has connections to two networks that lack direct connectivity can function as a transport gateway. This is helpful for enabling connectivity between routers that are configured to be within the same access region, but which do not have direct connectivity.

Enable Transport Gateway Functionality on a Router Using Cisco vManage

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco vManage Release 20.8.1

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
    - Create a system template for the device.
    - In the table, locate the existing system template for the device. In the row for the template, click **...** and choose **Edit**.
4. In the **Basic Configuration** section, in the **Transport Gateway** field, choose **On**.
5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure the Transport Gateway Path Preference Using Cisco vManage

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco vManage Release 20.8.1

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
    - Create an OMP template for the device.
    - In the table, locate the existing OMP template for the device. In the row for the template, click **…** and choose **Edit**.
4. In the **Best Path** section, in the **Transport Gateway Path Behavior** field, choose Global mode and choose one of the following options:

Option	Description
Do ECMP Between Direct and Transport Gateway Paths	For devices that can connect through a transport gateway and through direct paths, apply equal-cost multi-path (ECMP) to all available paths.
Prefer Transport Gateway Path	For devices that can connect through a transport gateway, use only the transport gateway paths, even if other paths are available.

5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Router Affinity

Table 30: Feature History

Feature Name	Release Information	Description
Multi-Region Fabric: Router Affinity	Cisco IOS XE Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	Often a router has multiple options to choose for the next hop when routing a flow to its destination. When multiple devices can serve as the next hop for a flow, you can specify the order of preference among the devices by configuring router affinity groups. The result is that a router attempts to use a route to the next-hop device of highest preference first, and if that device is not available, it attempts to use a route to the next-hop device of the next lower preference. Affinity groups enable this functionality without requiring complex control policies.

Feature Name	Release Information	Description
Improved Prioritization of Routes to Peer Devices in the Affinity Group Preference List	Cisco SD-WAN Controllers Release 20.9.x	This feature introduces a change to the order in which Cisco vSmart controllers advertise routes to devices. From this release, when Cisco vSmart controllers advertise routes to a device, they (a) give higher priority to routes to peer devices in the affinity group preference list, and (b) lower priority to routes that may have a higher best path score, but are not routes to a device associated with a preferred affinity group. The effect is to prioritize routes to peer devices in preferred affinity groups.

Configure Router Affinity Groups Using Cisco vManage

Configure an Affinity Group or Affinity Group Preference on a Device, Using Cisco vManage

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco SD-WAN Release 20.8.1, Cisco vManage Release 20.8.1

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.

2. Click **Feature Templates**.

3. Do one of the following:

   - Create a system template for the device.

   - In the table, locate the existing system template for the device. In the row for the template, click **…** and choose **Edit**.

4. To assign an affinity group to a border router, in the **Advanced** section, in the **Affinity Group** field, change the mode to **Global** and enter an affinity group number, in the range 1 to 63.

   If an affinity group has been configured previously on the device, the new value replaces the previous.

5. To configure an affinity group preference order for a border router or an edge router, in the **Advanced** section, in the **Affinity Group Preference** field, change the mode to **Global** and enter a comma-separated list of affinity group numbers. This determines the order of preference for connecting to border routers. The affinity groups are in the range 1 to 63.

   Example: 10, 11, 1, 5

   Note If you configure a Cisco vSmart controller to filter out routes that are not in the affinity group preference list, then the device can only connect to routers in the affinity group. See Configure a Cisco vSmart Controller to Provide Only Paths in the Affinity Preference List, Using Cisco vManage, on page 75.

6. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the devices using the template.

Configure a Cisco vSmart Controller to Provide Only Paths in the Affinity Preference List, Using Cisco vManage

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco SD-WAN Release 20.8.1, Cisco vManage Release 20.8.1

Before You Begin

The last step of this procedure requires logging in to the Cisco vSmart controllers that serve the regions where you are configuring this, to execute a command using the CLI.

Configure a Cisco vSmart Controller to Provide Only Paths in the Affinity Preference List

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.
3. Do one of the following:
   - Create an OMP template for a Cisco vSmart controller.
   - In the table, locate the existing OMP template for the Cisco vSmart controller. In the row for the template, click **...** and choose **Edit**.
4. In the **Best Path** section, in the **Enable Filtering Route Updates Based on Affinity** field, choose **Global** mode and choose **On**.
5. If you are editing an existing template, click **Update** and then **Configure Device** to push the update to the Cisco vSmart controllers using the template.
6. Connect to each Cisco vSmart controller and clear OMP routes to ensure that only the paths in the affinity group preference list are used.

```
vSmart#config terminal
vSmart(config)#omp
vSmart(config-omp)#filter-route outbound affinity-group-preference
vSmart(config-filter-route)#exit
vSmart(config-omp)#exit
vSmart(config)#exit
vSmart#clear omp all
```

Multi-Region Fabric Policy

Table 31: Feature History

Feature Name	Release Information	Description
Match Traffic by Destination: Access Region, Core Region, or Service VPN	Cisco IOS XE Release 17.8.1a Cisco vManage Release 20.8.1	You can apply a policy to traffic whose destination is any one of the following—access region, core region, service VPN. Use this match condition for data policy or application route policy on a border router.

Feature Name	Release Information	Description
Match Routes According to Path Type	Cisco IOS XE Release 17.8.1a Cisco vManage Release 20.8.1	When configuring a control policy for a Multi-Region Fabric architecture, you can match routes according to whether the route uses a hierarchical path, a direct path, or a transport gateway path.
Match Routes by Region and Role in a Control Policy	Cisco IOS XE Release 17.8.1a Cisco SD-WAN Controllers Release 20.8.1	In a control policy, you can match routes according to the region of the device originating the route, or the role (edge router or border router) of the device originating the route.
Match Traffic by Destination Region	Cisco IOS XE Release 17.9.1a Cisco vManage Release 20.9.1	When creating an application route policy or data policy, you can match traffic according to its destination region. The destination may be a device in the same primary region, the same secondary region, or neither of these.
Specify Path Type Preference	Cisco IOS XE Release 17.9.1a Cisco SD-WAN Controllers Release 20.9.1	When configuring a centralized policy, you can create a preferred color group list, which specifies three levels of route preference, called primary, secondary and tertiary. The route preferences are based on TLOC color and, optionally, on the path type—direct tunnel, multi-hop path, or all paths. Path type is relevant to networks using Multi-Region Fabric.

Configure Multi-Region Fabric Policy Using Cisco vManage

Configure a Data Policy or Application Route Policy to Match Traffic-To Using Cisco vManage

Before You Begin

Configure a VPN list to use when applying the policy.

Configure a Data Policy or Application Route Policy to Match Traffic-To

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. Click **Centralized Policies**.
3. Do one of the following:
    - To create a new policy, click **Add Policy**.
    - To edit an existing policy, click **…** in the row of the policy and click **Edit Policy**.
4. Click **Next**.
5. Click **Next**.
6. Click one of the following to create a traffic policy:

- **Application Aware Routing**
- **Traffic Data**

7. Click **Add Policy** and choose **Create New**.

Note To reuse an existing policy, you can choose **Import Existing**.

8. Enter a name and description for the new policy.
9. Click **Sequence Type** and choose **Custom**.
10. Click **Sequence Rule**.
11. Click **Match** (selected by default) and click **Traffic To**.
12. In the **Match Conditions** area, in the **Traffic To** field, choose one of the following:
    - **Access**
    - **Core**
    - **Service**
13. Choose an action for the sequence and complete the configuration of the policy.

    For information about creating traffic policies in general, see Centralized Policy in the Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x.
14. To save the policy, click **Save Application Aware Routing Policy** or **Save Data Policy**, depending on the type of policy that you are creating. A table shows the new policy.
15. Click **Next**.
16. At the **Apply Policies to Sites and VPNs** step, enter the name of the policy to apply.
17. Click one of the following, depending on the type of policy that you are creating and applying:
    - **Application-Aware Routing**
    - **Traffic Data**
18. Click **New Site/Region List and VPN List**.
19. If you are configuring a traffic data policy, choose one of the following options:
    - **From Service**
    - **From Tunnel**
    - **All**
20. Choose one of the following options to configure the sites or Multi-Region Fabric regions to which to apply the policy:
    - **Site List**: Enter a site list.

- **Region**: Enter a Multi-Region Fabric region ID or select a region list.

21. If you are configuring a data policy, do the following:
    a. In the **Select VPN List** field, choose a VPN list.
    b. Click **Add**.

22. Click **Role Mapping for Regions**.

23. For each region ID or region list, in the **Role** column, choose a role of **Edge** or **Border**. If you do not choose a role, Cisco vManage applies the policy to all routers in the region.

Note For policies that match by Traffic-To, choose **Border**. This match condition has no effect on edge routers.

24. Click **Save Policy**. A table shows the new policy. Optionally, to view the details of the policy, in the row of the policy, click **...** and choose **Preview**.

Configure a Control Policy to Match Region and Role Using Cisco vManage

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.

2. Click **Centralized Policies**.

3. Do one of the following:
    - To create a new policy, click **Add Policy**.
    - To edit an existing policy, click **...** in the row of the policy and click **Edit Policy**.

4. Click **Next**.

5. In the **Configure Topology and VPN Membership** step, click **Add Topology** and choose **Custom Control (Route & TLOC)**.

6. Enter a name and description for the new policy.

7. Click **Sequence Rule**.

8. Click **Match** (selected by default) and click **Region**.

9. In the **Match Conditions** area, do one of the following:
    - In the **Region List** field, enter a preconfigured region list name.

    Note You can click the field and choose **New Region List** to define a list.

    - In the **Region ID** field, enter a single region ID.

10. (Optional) To specify a router type within the configured regions, click **Role** and choose **Border** or **Edge**.

11. Choose an action for the sequence and complete the configuration of the policy.

    For information about creating traffic policies in general, see Centralized Policy in the *Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*.

12. To save the policy, click **Save Control Policy**. A table shows the new policy.

13. Click **Next**.

14. At the **Apply Policies to Sites and VPNs** step, enter the name of the policy to apply

15. Click **Topology**.

16. Click **New Site/Region List**.

17. Choose one of the following options to configure the sites or Multi-Region Fabric regions to which to apply the policy:

    - **Site List**: Enter a site list.
    - **Region**: Enter a Multi-Region Fabric region ID or select a region list.

18. Click **Role Mapping for Regions**.

19. For each region ID or region list, in the **Role** column, choose a role of **Edge** or **Border**. If you do not choose a role, Cisco vManage applies the policy to all routers in the region.

Note For policies that match by Traffic-To, choose **Border**. This match condition has no effect on edge routers.

20. Click **Save Policy**. A table shows the new policy. Optionally, to view the details of the policy, in the row of the policy, click **…** and choose **Preview**.

Match Traffic According to the Destination Region Using Cisco vManage

Minimum releases: Cisco IOS XE Release 17.9.1a, Cisco vManage Release 20.9.1

For complete information about configuring an application-aware routing (AAR) policy or traffic data policy, see Configure Centralized Policies Using Cisco vManage in the *Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. The information here only addresses how to use the **Destination Region** match condition.

Use the following procedure for an application-aware policy or a traffic data policy.

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.

2. Choose **Centralized Policy**, which is selected by default.

3. Click **Add Policy**.

4. Optionally, you can click a list type and define a list.

5. Click **Next**.

6. Optionally, add a topology.

7. Click **Next**.

8. Do one of the following:
   - For an AAR policy, click **Application Aware Routing**, which is selected by default.
   - For a traffic data policy, click **Traffic Data**.

9. Click **Add Policy** and select **Create New**.

10. Do one of the following:
    - For an AAR policy, click **Sequence Type** to create a sequence that matches traffic by destination.
    - For a traffic data policy, click **Sequence Type** and choose **Custom** to create a sequence that matches traffic by destination.

11. Click **Sequence Rule** to create a new rule for the sequence.

12. With the **Match** option selected, click **Destination Region** to add this option to the match conditions area of the sequence rule.

13. In the **Match Conditions** area, click the **Destination Region** field and choose one of the following:
    - **Primary**: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using the access-region bidirectional forwarding detection (BFD).
    - **Secondary**: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions.
    - **Other**: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination.

14. Continue to configure the policy as described in Configure Centralized Policies Using Cisco vManage, cited earlier in this section.

Configure the Path Preference for a Preferred Color Group List Using Cisco vManage

Minimum releases: Cisco IOS XE Release 17.9.1a, Cisco vManage Release 20.9.1

For complete information about configuring an application-aware routing (AAR) policy, see Configure Centralized Policies Using Cisco vManage in the *Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. The information here only addresses how to configure a path preference as part of a preferred color group.

1. From the Cisco vManage menu, choose **Configuration** > **Policies**, and choose **Centralized Policy**.
2. Click **Add Policy**.
3. Click **Application List**, which is selected by default.
4. Click **Preferred Color Group**.
5. Click **New Preferred Color Group**.
6. Configure the following fields:

Field	Description
Preferred Color Group Name	Enter a name for the color group.
Primary Colors: **Color Preference**	Click the field and select one or more colors for the primary preference.
Primary Colors: **Path Preference**	Click the drop-down list and choose one of the following for the primary preference: • **Direct Path**: Use only a direct path between the source and the destination devices. **Note** Do not use this option in a non-Multi-Region Fabric network. • **Multi Hop Path**: In a Multi-Region Fabric network, use a multi-hop path, which includes the core region, between the source and destination devices, even if a direct path is available. • **All Paths**: Use any path between the source and destination devices. **Note** This option is equivalent to not configuring path preference at all. If you are applying the policy to a non-Multi-Region Fabric network, use this option.
Secondary Colors: **Color Preference** **Path Preference**	Configure the secondary preference using the same method as for the **Primary Colors** options.
Tertiary Colors: **Color Preference** **Path Preference**	Configure the tertiary preference using the same method as for the **Primary Colors** options.

Use a Preferred Color Group in a Policy

Minimum releases: Cisco IOS XE Release 17.9.1a, Cisco vManage Release 20.9.1

For complete information about configuring policies, see Configure Centralized Policies Using Cisco vManage in the *Cisco SD-WAN Policies Configuration Guide, Cisco IOS XE Release 17.x*. The information here only addresses how to use the **Preferred Color Group** action, which incorporates path preference.

Use the following procedure for an application-aware policy or a traffic data policy.

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.

2. Click **Add Policy**.

3. Choose **Centralized Policy**, which is selected by default.

4. Click **Add Policy**.

5. Optionally, you can click a list type and define a list.

6. Click **Next**.

7. Optionally, add a topology.

8. Click **Next**.

9. Do one of the following:

    - For an AAR policy, click **Application Aware Routing**, which is selected by default.
    - For a traffic data policy, click **Traffic Data**.

10. Click **Add Policy** and select **Create New**.

11. Do one of the following:

    - For an AAR policy, click **Sequence Type** to create a sequence that matches traffic by destination.
    - For a traffic data policy, click **Sequence Type** and choose **Custom** to create a sequence that matches traffic by destination.

12. Click **Sequence Rule** to create a new rule for the sequence.

13. Click **Actions**.

14. For an AAR policy, do the following:

    a. Click **SLA Class List**.

    b. Click the **Preferred Color Group** field and choose a preferred color group.

15. For an traffic control policy, do the following:

    a. Click **Accept**.

    b. Click **Preferred Color Group**.

    c. Click the **Preferred Color Group** field and choose a preferred color group.

Configure Cisco Umbrella Integration

Table 32: Feature History

Feature Name	Release Information	Description
Extended DNS (EDNS) and Local Domain Bypass Support with Cisco Umbrella Integration	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	You can now configure Cisco Umbrella registration, define domain lists, and configure Umbrella DNS policy from the **Configuration** > **Security** screen in Cisco vManage.

Configure Cisco Umbrella Registration

Use this procedure to configure Cisco Umbrella registration globally for all devices. The procedure retrieves the Umbrella registration parameters automatically.

When configuring individual policies, it is also possible to configure Umbrella registration, but it can be managed more flexibly using the following procedure:

1. From the Cisco vManage menu, choose **Configuration** > **Security**.
2. Click **Custom Options** and choose **Umbrella Registration**.
3. In the **Manage Umbrella Registration** dialog box, use one of the following methods to register devices to Umbrella. The registration details are used globally.
   - Cisco Umbrella Registration Key and Secret
     a. Click the **Get Keys** to retrieve Umbrella registration parameters automatically: Organization ID, Registration Key, and Secret.

Note To automatically retrieve registration parameters, Cisco vManage uses the Smart Account credentials to connect to the Umbrella portal. The Smart Account credentials are configured in Cisco vManage under **Administration** > **Settings** > **Smart Account Credentials**.

     b. (Optional) If the Umbrella keys have been rotated and the details that are automatically retrieved are incorrect, enter the details manually.
     c. Click **Save Changes**.

Define Domain Lists

1. From the Cisco vManage menu, choose **Configuration** > **Security**.
2. Click **Custom Options**, and choose **Lists** from the drop-down menu.

3. Choose **Domain** in the left pane.
4. Click **New Domain List** to create a new domain list or click the domain name, and click the pencil icon on the right side for an existing list.
5. Enter the **Domain List Name**, **Add Domain**, and click **Add** to create the list.

Configure Umbrella DNS Policy Using Cisco vManage

1. From the Cisco vManage menu, choose **Configuration** > **Security**.
2. Click **Add Security Policy**.
3. In the **Add Security Policy** wizard, click **Direct Internet Access**.
4. Click **Proceed**.
5. Click **Next** until you reach the **DNS Security** page.
6. From the **Add DNS Security Policy** drop-down list, choose one of the following:
   - **Create New**: A **DNS Security - Policy Rule Configuration** wizard is displated. Continue to Step 7.
   - **Copy from Existing**: Choose a policy from the **Policy** field, enter a policy name, and click **Copy**.
7. If you are creating a new policy using the **Create New** option, the **DNS Security - Policy Rule Configuration** wizard is displayed.
8. Enter a policy name in the **Policy Name** field.
9. The **Umbrella Registration Status** displays the status of the API Token configuration.
10. Click **Manage Umbrella Registration** to add a token, if you have not added one already.
11. Click **Match All VPN** to keep the same configuration for all the available VPNs and continue with Step 13.

    Or click **Custom VPN Configuration** if you need to add target service VPNs to your policy. A Target VPNs window appears, and continue with Step 12.
12. To add target service VPNs, click **Target VPNs** at the top of the window.
13. Click **Save Changes** to add the VPN.
14. From the **Local Domain Bypass List** drop-down list, choose the domain bypass.
15. Click **Advanced** to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.
16. Click **Save DNS Security Policy**.

    The **Configuration > Security** window is displayed, and the DNS policy list table includes the newly created DNS Security Policy.

Configure Umbrella DNS Policy Using Cisco vManage

1. From the Cisco vManage menu, choose **Configuration** > **Security**.

2. Click **Add Security Policy**.
3. In the **Add Security Policy** wizard, click **Direct Internet Access**.
4. Click **Proceed**.
5. Click **Next** until you reach the **DNS Security** page.
6. From the **Add DNS Security Policy** drop-down list, choose one of the following:
    - **Create New**: A **DNS Security - Policy Rule Configuration** wizard is displated. Continue to Step 7.
    - **Copy from Existing**: Choose a policy from the **Policy** field, enter a policy name, and click **Copy**.
7. If you are creating a new policy using the **Create New** option, the **DNS Security - Policy Rule Configuration** wizard is displayed.
8. Enter a policy name in the **Policy Name** field.
9. The **Umbrella Registration Status** displays the status of the API Token configuration.
10. Click **Manage Umbrella Registration** to add a token, if you have not added one already.
11. Click **Match All VPN** to keep the same configuration for all the available VPNs and continue with Step 13.

    Or click **Custom VPN Configuration** if you need to add target service VPNs to your policy. A Target VPNs window appears, and continue with Step 12.
12. To add target service VPNs, click **Target VPNs** at the top of the window.
13. Click **Save Changes** to add the VPN.
14. From the **Local Domain Bypass List** drop-down list, choose the domain bypass.
15. Click **Advanced** to enable or disable the DNSCrypt. By default, the DNSCrypt is enabled.
16. Click **Save DNS Security Policy**.

    The **Configuration > Security** window is displayed, and the DNS policy list table includes the newly created DNS Security Policy.

Attach DNS Umbrella Policy to Device Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and choose **From Feature Template** from the Create Template drop-down menu.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. From the Device Model drop-down menu, choose a device.
4. Click **Additional Templates**. The screen scrolls to the **Additional Templates** section.

5. From the Security Policy drop-down menu, choose the name of the Umbrella DNS Security Policy you configured in the above procedure.

6. Click **Create** to apply the Umbrella policy to a device template.

Configure Default AAR and QoS Policies Using Cisco vManage

Table 33: Feature History

Feature Name	Release Information	Description
Configure Default AAR and QoS Policies	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	You can configure Default AAR and QoS policies.

Follow these steps to configure default AAR, data, and QoS policies using Cisco vManage:

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.

2. Click **Add Default AAR & QoS**.

   The **Process Overview** page is displayed.

3. Click **Next**.

   The **Recommended Settings based on your selection** page is displayed.

4. Based on the requirements of your network, move the applications between the **Business Relevant**, **Default**, and **Business Irrelevant** groups.

   Note When customizing the categorization of applications as Business-relevant, Business-irrelevant, or Default, you can only move individual applications from one category to another. You cannot move an entire group from one category to another.

5. Click **Next**.

   On the **Path Preferences (optional)** page, choose the **Preferred** and **Preferred Backup** transports for each traffic class.

6. Click **Next**.

   The **App Route Policy Service Level Agreement (SLA) Class** page is displayed.

   This page shows the default settings for **Loss**, **Latency**, and **Jitter** values for each traffic class. If necessary, customize **Loss**, **Latency**, and **Jitter** values for each traffic class.

7. Click **Next**.

   The **Enterprise to Service Provider Class Mapping** page is displayed.

   a. Select a service provider class option, based on how you want to customize bandwidth for different queues. For further detials on QoS queues, refer to the section **Mapping of Application Lists to Queues**

b. If necessary, customize the bandwidth percentage values for each queues.

8. Click **Next**.

   The **Define prefixes for the default policies and applications lists** page is displayed.

   For each policy, enter a prefix name and description.

9. Click **Next**.

   The **Summary** page is displayed. On this page, you can view the details for each configuration.

   You can click **Edit** to edit the options that appeared earlier in the workflow. Clicking edit returns you to the relevant page.

10. Click **Configure**.

    Cisco vManage creates the AAR, data, and QoS policies and indicates when the process is complete.

    The following table describes the workflow steps or actions and their respective effects:

Table 34: Workflow Steps and Effects

Workflow Step	Affects the Following
Recommended Settings based on your selection	AAR and data policies
Path Preferences (optional)	AAR policies
App Route Policy Service Level Agreement (SLA) Class: • Loss • Latency • Jitter	AAR policies
Enterprise to Service Provider Class Mapping	Data and QoS policies
Define prefixes for the default policies and applications	AAR, data, QoS policies, forwarding classes, application lists, SLA class lists

11. To view the policy, click **View Your Created Policy**.

Note To apply the default AAR and QoS policies to the devices in the network, create a centralized policy that attaches the AAR and data policies to the required site lists. To apply the QoS policy to the Cisco SD-WAN devices, attach it to a localized policy through device templates.

Mapping of Application Lists to Queues

The following lists show each service provider class option, the queues in each option, and the application lists included in each queue. The application lists are named here as they appear on the Path Preferences page in this workflow.

4 QoS class

- Voice
  - Internetwork control
  - VoIP telephony
- Mission critical
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
  - Multimedia streaming
- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data
- Default
  - Best effort
  - Scavenger

5 QoS class

- Voice
  - Internetwork control
  - VoIP telephony
- Mission critical
  - Broadcast video
  - Multimedia conferencing
  - Real-Time interactive
  - Multimedia streaming
- Business data
  - Signaling
  - Transactional data
  - Network management
  - Bulk data

- General data
    - Scavenger
- Default
    - Best effort

6 QoS class

- Voice
    - Internetwork control
    - VoIP telephony
- Video
    - Broadcast video
    - Multimedia conferencing
    - Real-Time interactive
- Mission Critical
    - Multimedia streaming
- Business data
    - Signaling
    - Transactional data
    - Network management
    - Bulk data
- General data
    - Scavenger
- Default
    - Best effort

8 QoS class

- Voice
    - VoIP telephony
- Net-ctrl-mgmt
    - Internetwork control
- Interactive video

  - Multimedia conferencing
  - Real-Time interactive

- Streaming video
  - Broadcast video
  - Multimedia streaming

- Call signaling
  - Signaling

- Critical data
  - Transactional data
  - Network management
  - Bulk data

- Scavengers
  - Scavenger

- Default
  - Best effort

Configure Cisco SD-WAN Cloud OnRamp for IaaS on AWS

Points to Consider

- Transit VPCs provide the connection between the Cisco overlay network and the cloud-based applications running on host VPCs. You can provision up to four pairs of redundant Cisco SD-WAN cloud devices within each VPC dedicated to function as a transit point for traffic from the branch to host VPCs. The individual Cisco SD-WAN devices of each redundant pair are deployed within a different availability zone in the AWS region of the transit VPC. Multiple Cisco SD-WAN devices provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two Cisco SD-WAN cloud devices, the transport VPN (VPN 0) connects to a branch router, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.

- The Cisco SD-WAN Cloud OnRamp for IaaS workflow uses a public IP address of the second WAN interface to set up the Customer Gateway for mapping (ipsec tunnels) the host VPCs to a transit VPC. To add the public IP address of the WAN interface, configure the VPN interface ethernet template with ge0/0 interface for the devices used in Cisco SD-WAN Cloud OnRamp for IaaS. In vEdge Cloud routers, the tunnel interface is on the ge0/0 interface. .

- Cisco SD-WAN Cloud OnRamp for IaaS supports autoscale for AWS. To use the AWS autoscale feature, ensure that you associate one to four pairs of Cisco SD-WAN cloud devices with a transit VPC.

- Host VPCs are virtual private clouds in which your cloud-based applications reside. When a transit VPC connects to an application or application provider, it's simply connecting to a host VPC.
- All host VPCs can belong to the same AWS account, or each host VPC can belong to a different account. You can map a host that belongs to one AWS account to a transit VPC that belongs to a different account. You configure cloud instances or cloud accounts by using the Cloud OnRamp configuration wizard.

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for IaaS**.

If you're configuring Cisco SD-WAN Cloud OnRamp for IaaS the first time, no cloud instances appear in the screen. A cloud instance corresponds to an AWS account with one or more transit VPCs created within an AWS region.

Step 2 Click **Add New Cloud Instance**.

Step 3 Click the **Amazon Web Services (AWS)** radio button.

Step 4 In the next pop-up window, perform the following:

a) To log in to the cloud server, click **IAM Role** or **Key**. We recommend that you use IAM Role.

b) If you click **IAM Role**, then create an IAM role with Cisco vManage provided **External ID**. Note the displayed external Id from the window and provide the **Role ARN** value that is available when creating an IAM role.

Starting from Cisco SD-WAN Release 20.4.1, to create an IAM role, you must enter the Cisco vManage provided External Id into a policy by using the AWS Management Console. Do the following:

1. Attach an IAM Role to an existing Cisco vManage EC2 instance.

a. See the Creating an IAM role (console) topic of AWS documentation to create a policy. In the AWS **Create policy** wizard, click **JSON** and enter the following JSON policy document.

```
{

"Version": "2012-10-17",

  "Statement": [{

    "Sid": "VisualEditor0",

"Effect": "Allow",

    "Action": "sts:AssumeRole",

"Resource": "*"

    }
]

}
```

b. See the Easily Replace or Attach an IAM Role to an Existing EC2 Instance by Using the EC2 Console blog of AWS Security Blog for information about creating an IAM role and attaching it to the Cisco vManage EC2 instance based on the policy created in Step 1.

Note On the **Attach permissions policy** window, choose the AWS-managed policy that you created in Step 1.

2. Create an IAM role on an AWS account that you want to use for Cisco SD-WAN Cloud OnRamp for IaaS.

a. See the Creating an IAM role (console) topic of AWS Documentation and create an IAM role by checking **Require external ID** and pasting the external Id that you noted in Step 4(b).

b. See the Modifying a role trust policy (console) topic of AWS Documentation to change who can assume a role.

In the **IAM Roles** window, scroll down and click the role you created in the previous step.

In the **Summary** window, note the **Role ARN**.

Note You can enter this role ARN value when you choose the IAM role in Step 4(b).

c. After modifying the trust relationship, click **JSON** and enter the following JSON document. Save the changes.

Note The account Id in the following JSON document is the Cisco vManage EC2 instance.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::[Account ID from Part 1]:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "[vManage provided External ID]"
       }
      }
    }
  ]
}
```

c) If you click the **Key** radio button:

1. In the **API Key** field, enter your Amazon API key.
2. In the **Secret Key** field, enter the password associated with the API key.
3. From the **Environment** drop-down list, choose **commercial** or **govcloud**.

   By default, commercial environment is selected. You can choose the geographical regions based on the environment specifications.

   Note AWS Government Cloud isn’t supported for vEdge Cloud routers. Therefore, ensure that you don’t choose **govcloud**.

Step 5 Click **Login** to log in to the cloud server.

The cloud instance configuration wizard appears. This wizard consists of three screens that you use to select a region, add a transit VPC, discover host VPCs, and map host VPCs to transit the VPC. A graphic on each wizard screen illustrates the steps in the cloud instance configuration process. The steps that aren’t yet completed are shown in light gray. The current step is highlighted within a blue box. Completed steps are indicated with a green checkmark and are shown in light orange.

Step 6 Select a region:

From the **Choose Region** drop-down list, choose a region where you want to create the transit VPC.

Step 7 Add a transit VPC:

a) In the **Transit VPC Name** field, enter the transit VPC name.

The name can contain 128 alphanumeric characters, hyphens (–), and underscores (_). It can't contain spaces or any other characters.

b) Under **Device Information**, enter information about the transit VPC:

1. In the **WAN Edge Version** drop-down list, choose the software version of the Cisco SD-WAN cloud device to run on the transit VPC.

2. In the **Size of Transit WAN Edge** drop-down list, choose an option to determine the memory and CPUs you can use for each of the Cisco SD-WAN cloud devices that run on the transit VPC. See the Supported Instance Types topic of Cisco Cloud vEdge Routers in the *Cisco SD-WAN Getting Started Guide*.

   Note We recommend that you choose the following size:

   For Cisco Cloud vEdge Routers, choose c4 instance type with four vCPUs, such as c4.xlarge (4 vCPU).

3. In the **Max. Host VPCs per Device Pair** field, select the maximum number of host VPCs that can be mapped to each device pair for the transit VPC. Valid values are 1–32.

4. To set up the transit VPC devices for Direct Internet Access (DIA), click one of the following:

   - **Disabled**: No Internet access.
   - **Enabled via Transport**: Configure or enable NAT for the WAN interface on a device.
   - **Enabled via Umbrella SIG**: Configure Cisco Umbrella to enable secure DIA on a device.

5. In the **Device Pair 1#** field, choose the serial numbers of each device in the pair. To remove a device serial number, click **X** that appears in the field.

   The serial numbers of the devices that appear are associated with a configuration template and supports the Cisco SD-WAN WAN edge version that you selected in Step 1.

6. To add more device pairs, click ⊕.

   To remove a device pair, click ⊖.

   A transit VPC can be associated with one to four device pairs. To enable the autoscale feature on AWS, associate at least two device pairs with the transit VPC.

7. Click **Advanced**, if you wish to enter more specific configuration options:

   a. In the **Transit VPC CIDR** field, enter a custom CIDR that has a network mask in the range of 16–25. If you choose to leave this field empty, the Transit VPC is created with a default CIDR of 10.0.0.0/16. There must be sufficient address space to create six subnets within the CIDR block.

   b. (Optional) In the **SSH PEM Key** drop-down list, choose a PEM key pair to log into an instance. The key pairs are region-specific. See the AWS Documentation for instructions about creating key pairs.

8. To complete the transit VPC configuration, click **Save and Finish**, or optionally to continue with the wizard, click **Proceed to Discovery and Mapping**.

With this cloud instance, a single transit VPC with two Cisco SD-WAN cloud devices has been created. You can configure multiple transit VPCs within a single cloud instance (AWS account within a region). When multiple transit VPCs exist within a cloud instance, you can map host VPCs to any one of the transit VPCs.

9. Discover host VPCs:

  a. In the **Select an account to discover** field, choose the AWS account from which you wish to discover host VPCs.

  Alternatively, to add a new AWS account from which you wish to discover host VPCs, click **New Account**.

  b. Click **Discover Host VPCs**.

  A table appears that display the VPCs, which are available to be mapped to a transit VPC. Only the host VPCs in the selected AWS account and within the same AWS region as the transit VPC appears.

  c. In the table that appears, check one or more hosts to map to the transit VPC.

  To filter the search results, use the Filter option in the search bar and display only host VPCs that match specific search criteria.

  Click the **Refresh** icon to update the table with current information.

  Click the **Show Table Columns** icon to specify which columns to be displayed in the table.

10. Map the host VPCs to a transit VPC:

  a. In the table with all host VPCs, choose the desired host VPCs.

  b. Click **Map VPCs**. The Map Host VPCs pop-up opens.

  c. In the **Transit VPC** drop-down list, choose the transit VPC to map to the host VPCs.

  d. In the **VPN** drop-down list, choose a service VPN in the overlay network in which to place the mapping.

  e. Enable the **Route Propagation** option if Cisco vManage automatically propagates route to the host VPC routes table.

  By default, **Route Propagation** is disabled.

  f. Click **Map VPCs**.

After a few minutes, the **Task View** screen appears, confirming that the host VPC has been mapped to the transit VPC.

Note When configuring the VPN feature template for VPN 0 for the two Cisco SD-WAN cloud devices that form the transit VPC, ensure that the color you assign to the tunnel interface is a public color, and not a private color. The following are the public colors:

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

Configure Cisco SD-WAN Cloud OnRamp for IaaS on Microsoft Azure

In the configuration process, map one or more host VNets to a single transit VNet. When mapping, you're configuring the cloud-based applications that branch users can access.

The mapping process establishes IPsec and BGP connections between the transit VNet and each host VNet. The IPsec tunnel that connects the transit and host VNet runs IKE to provide security for the connection. For Azure, the IPsec tunnel uses IKE version 2. The BGP connection that is established over the secure IPsec tunnel allows the transit and host VNet to exchange routes. The BGP connections or the BGP routes are then re-distributed into OMP within the Cisco SD-WAN cloud devices, which then advertises the OMP routes to the vSmart controllers in the domain. The transit VNet can then direct traffic from the branch to the proper host VNet and to the proper cloud-based application.

During the mapping process, the IPsec tunnels and BGP peering sessions are configured and established automatically. After establishing the mappings, you can view the IPsec and BGP configurations in the VPN Interface IPsec and BGP feature configuration templates, and modify them as necessary.

Points to Consider:

To configure Cisco SD-WAN Cloud OnRamp for IaaS on Azure, create Azure transit VNets, each of which consist of a pair of routers. Then, map the host VNets to transit VNets that exist in the Azure cloud. All VNets reside in the same resource group.

- Transit VNets provide the connection between the overlay network and the cloud-based applications running on the host VNet. Each transit VNet consists of two cloud devices that reside in their own VNet. Two cloud devices provide redundancy for the connection between the overlay network and cloud-based applications. On each of these two cloud devices, the transport VPN (VPN 0) connects to the simulated branch device, and the service-side VPNs (any VPN except for VPN 0 and VPN 512) connect to applications and application providers in the public cloud.
- The Cisco SD-WAN Cloud OnRamp for IaaS workflow uses a public IP address of the second WAN interface to set up the Customer Gateway for mapping (ipsec tunnels) the host VNets to a transit VNet. To add the public IP address of the WAN interface, configure the VPN Interface Ethernet template with ge0/0 interface for the devices used in Cisco SD-WAN Cloud OnRamp for IaaS. In vEdge Cloud routers, the tunnel interface is on the ge0/0 interface.
- Host VNets are virtual private clouds in which your cloud-based applications reside. When a transit VNet connects to an application or application provider, it's simply connecting to a host VNet.

Step 1 From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for IaaS**.

Step 2 Click **Add New Cloud Instance**

Step 3 Click the **Microsoft Azure** radio button.

Step 4 In the next pop-up screen, perform the following:

a) In the **Subscription ID** field, enter the ID of the Microsoft Azure subscription you want to use as part of the Cisco SD-WAN Cloud OnRamp for IaaS workflow.

b) In the **Client ID** field, enter the ID of an existing application or create a new application. To create an application, go to your **Azure Active Directory** > **App Registrations** > **New registration**. See Microsoft Azure documentation for more information on creating an application.

c) In the **Tenant ID** field, enter the ID of your account. To find the tenant ID, go to your Microsoft Azure Active Directory and click **Properties**.

d) In the **Secret Key** key field, enter the password associated with the client ID.

e) In the **Environment** field, choose **commercial** or **GovCloud**.

By default, commercial environment is selected. You can choose the geographical locations based on the environment specifications.

Note Azure Government Cloud isn’t supported for vEdge Cloud routers. Therefore, ensure that you don’t choose the **govcloud** option.

f) Click **Login**.

The cloud instance configuration wizard opens.

The wizard consists of three screens that you use to select a location, add a transit VNet, discover host VNets, and map host VNets to the transit VNet. A graphic on the right side of each wizard screen illustrates the steps in the cloud instance configuration process. The steps not yet completed are shown in light gray. The current step is highlighted within a blue box. All completed steps are indicated with a green checkmark and are shown in light orange.

Step 5 From the **Choose Location** drop-down list, choose a location where you want to create the transit VNet.

The locations available are based on the commercial cloud or GovCloud selection.

Step 6 Add a transit VNet:

a) In the **Transit VNet Name** field, type a name for the transit VNet.

The name can contain 32 alphanumeric characters, hyphens (–), and underscore (_). It can't contain spaces or any other characters.

b) Under **Device Information**, enter information about the transit VNet:

1. In the **WAN Edge Version** drop-down list, choose the software version to run on the transit VNet. The drop-down list includes the published versions of the device software in the Microsoft Azure marketplace.
2. In the **Size of Transit WAN Edge** drop-down list, choose an option to determine the memory and CPUs you can use for each of the Cisco SD-WAN cloud devices that run on the transit VNet. See Supported Instance Types for Cisco Cloud vEdge Routers in the *Cisco SD-WAN Getting Started Guide*.

   Note We recommend that you choose the following size:

3. To set up the transit VNet devices for Direct Internet Access (DIA), click one of the following:
   - **Disabled**: No Internet access.
   - **Enabled via Transport**: Configure or enable NAT for the WAN interface on a device.
   - **Enabled via Umbrella SIG**: Configure Cisco Umbrella to enable secure DIA on a device.
4. In the **Device 1** drop-down list, choose the serial number of the first device.
5. In the **Device 2** drop-down list, choose the serial number of the second device in the device pair.
6. Click **Advanced** if you wish to enter more specific configuration options.
7. In the **Transit VNet CIDR** field, enter a custom CIDR that has a network mask in the range of 16–25. If you leave this field empty, the Transit VNet is created with a default CIDR of 10.0.0.0/16.

c) To complete the transit VNet configuration. click **Save and Finish**, or optionally to continue with the wizard, click **Proceed to Discovery and Mapping**.

Step 7 Map host VNets to transit VNets:

a) In the **Select an account to discover** drop-down list, choose your Azure subscription ID.

Alternatively, to add a new Azure account from which you wish to discover host VNets, click **New Account**.

b) Click **Discover Host VNets**.

c) In the **Select a VNet** drop-down list, choose a desired host VNet.

d) Click **Next**.

e) From the table of host VNets, choose a desired host VNet.

f) Click **Map VNets**. The Map Host VNets pop-up appears.

g) In the **Transit VNet** drop-down list, choose the transit VNet to map to the host VNets.

h) In the **VPN** drop-down list, choose a VPN in the overlay network in which to place the mapping.

i) In the IPSec Tunnel CIDR section, to configure IPSec tunnels to reach the Azure virtual network transit, enter two pairs of interface IP addresses and a pair of loopback IP addresses for each of the Cisco Cloud vEdge Routers. Ensure that the IP addresses are network addresses in the /30 subnet, unique across the overlay network, and they aren’t part of the host VNet CIDR. If they are part of the host VNet CIDR, Microsoft Azure returns an error when attempting to create VPN connections to the transit VNet.

Note The IP addresses aren’t part of the host VNet and Transit VPC CIDR.

Microsoft Azure supports single Virtual Private Gateway (VGW) configuration over IPSec tunnels with redundancy provided over a single tunnel. Therefore, Cisco SD-WAN Cloud OnRamp for IaaS supports two VGWs for redundancy. During a planned maintenance or an unplanned event of a VGW, the IPSec tunnel from the VGW to the cloud devices get disconnected. This loss of connectivity causes the cloud devices lose BGP peering with Cisco vManage over IPSec tunnel. To enable BGP peering with the cloud routers rather than the IP address of the IPSec tunnel, provide the loopback addresses for each cloud device.

Note The loopback option for BGP peering supports single and multiple Virtual Gateways, or Customer Gateway configuration or both on Azure cloud. The loopback option applies only to the new host VNets mapped to transit VNets and not on the existing VNets.

j) In the Azure Information section:

1. In the **BGP ASN** field, enter the ASN that you configure on the Azure Virtual Network Gateway, which is brought up within the host VNet. Use an ASN that isn’t part of an existing configuration on Azure. For acceptable ASN values, refer to Microsoft Azure documentation.
2. In the **Host VNet Gateway Subnet** field, enter a host VNet subnet in which the Virtual Network Gateway can reside. We recommend you use a /28 subnet or higher. Ensure not to provide a subnet that is already created in the VNet.

   Note Ensure that there’s an unused CIDR inside the host VNet CIDR.

k) Click **Map VNets**.

l) Click **Save and Complete**.

Note When configuring the VPN feature template for VPN 0 for the two Cisco SD-WAN cloud devices that form the transit VNet, ensure that the color you assign to the tunnel interface is a public color, and not a private color. Public colors are:

- **3g**
- **biz-internet**
- **blue**
- **bronze**
- **custom1**
- **custom2**
- **custom3**
- **default**
- **gold**
- **green**
- **lte**
- **metro-ethernet**
- **mpls**
- **public-internet**
- **red**
- **silver**

The **Task View** screen appears, confirming that the host VNet has been mapped to the transit VNet successfully.

The creation of VNet Gateway can take up to 45 minutes.

Configure Cloud onRamp for SaaS

Table 35: Feature History

Feature Name	Release Information	Description
New Configuration Workflow for Cloud onRamp for SaaS for Cisco vEdge devices	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	Using Cloud onRamp for SaaS, you can select specific SaaS applications and interfaces, and let Cisco SD-WAN determine the best performing path for each SaaS applications.

Enable Cloud OnRamp for SaaS

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Click **Edit**, next to **Cloud onRamp for SaaS**.
3. In the **Cloud onRamp for SaaS** field, click **Enabled**.
4. Click **Save**.

Configure Applications for Cloud onRamp for SaaS Using Cisco vManage

Table 36: Feature History

Feature Name	Release Information	Description
Service Area Mapping	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	To specify the service area that your Microsoft 365 application belongs to, choose an option from the **Service Area** drop-down list.

1. Open Cloud onRamp for Saas.
   - From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

     or
   - In Cisco vManage, click the cloud icon near the top right and choose **Cloud onRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

   The **Applications and Policy** window displays all SaaS applications.
3. Optionally, you can filter the list of applications by clicking an option in the **App Type** field.
   - **Standard**: Applications included by default for Cloud onRamp for SaaS.
   - **Custom**: User-defined SaaS application lists (see Information About SaaS Application Lists).
4. Enable applications and configure.

Column	Description
Applications	Applications that can be used with Cloud onRamp for SaaS.
Monitoring	**Enabled**: Enables Cloud OnRamp for SaaS to initiate the Quality of Experience probing to find the best path. **Disabled**: Cloud onRamp for SaaS stops the Quality of Experience probing for this application.
VPN	(Cisco vEdge devices) Specify one or more VPNs.

Column	Description
Policy/Cloud SLA	(Cisco IOS XE SD-WAN devices) Select **Enable** to enable Cloud onRamp for SaaS to use the best path for this application. **Note** You can select **Enable** only if there is a centralized policy that includes an application-aware policy has been activated.
	(Cisco IOS XE SD-WAN devices) For Microsoft 365 (M365), select one of the following to specify which types of M365 traffic to include for best path determination: • **Optimize**: Include only M365 traffic categorized by Microsoft as "optimize" – the traffic most sensitive to network performance, latency, and availability. • **Optimize and Allow**: Include only M365 traffic categorized by Microsoft as "Optimize" or "Allow". The "Allow" category of traffic is less sensitive to network performance and latency than the "Optimize" category. • **All**: Include all M365 traffic.
	Starting from Cisco IOS XE Release 17.5.1a, you can choose the service area that your M365 application belongs to. This allows you to apply the policy to only those applications in the specified service area. Microsoft allows the following service area options: • **Common**: M365 Pro Plus, Office in a browser, Azure AD, and other common network endpoints. • **Exchange**: Exchange Online and Exchange Online Protection. • **SharePoint**: SharePoint Online and OneDrive for Business. • **Skype**: Skype for Business and Microsoft Teams. See the Microsoft documentation for information about updates to the service areas.

5. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** window appears, showing the application-aware policy for the current active centralized policy.

   - You can select the application-aware policy and click **Review and Edit** to view the policy details. The match conditions of the policy show the SaaS applications for which monitoring has been enabled.
   - For an existing policy, you cannot edit the site list or VPN list.
   - You can create a new policy for sites that are not included in existing centralized policies. If you create a new policy, you must add a VPN list for the policy.
   - You can delete one or more new sequences that have been added for the SaaS applications, or change the order of the sequences.

6. Click **Save Policy and Next**. This saves the policy to the Cisco vSmart Controller.

Configure Client Sites

To configure Cloud OnRamp for SaaS on client sites that access the internet through gateways, configure Cloud OnRamp for SaaS both on the client sites and on the gateway sites.

Note You cannot configure Cloud OnRamp for SaaS with Point-to-Point Protocol (PPP) interface on the gateway sites.

Client sites in the Cloud onRamp service choose the best gateway site for each application to use for accessing the internet.

1. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**. The **Cloud OnRamp for SaaS** Dashboard appears.
2. Click **Manage Cloud OnRamp for SaaS** and choose **Client Sites**. The page displays the following elements:
    - Attach Sites: Add client sites to Cloud onRamp for SaaS service.
    - Detach Sites: Remove client sites from Cloud onRamp for SaaS service.
    - Client sites table: Display client sites configured for Cloud onRamp for SaaS service.
3. On the **Cloud onRamp for SaaS** > **Manage Sites** window, click **Attach Sites**. The **Attach Sites** dialog box displays all sites in the overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
4. Choose one or more client sites from **Available Sites** and move them to **Selected Sites**.
5. Click **Attach**. The Cisco vManage NMS saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
6. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS** to return to the Cloud OnRamp for SaaS Dashboard screen.
7. Click **Manage Cloud OnRamp for SaaS** and choose **Gateways**. The page displays the following elements:
    - Attach Gateways: Attach gateway sites.
    - Detach Gateways: Remove gateway sites from the Cloud onRamp service.
    - Edit Gateways: Edit interfaces on gateway sites.
    - Gateways table: Display gateway sites configured for Cloud onRamp service.
8. In the **Manage Gateways** window, click **Attach Gateways**. The **Attach Gateways** dialog box displays all sites in your overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
9. In the **Device Class** field, choose one of the following operating systems:

- **Cisco OS**: Cisco IOS XE SD-WAN devices
- **Viptela OS (vEdge)**: Cisco vEdge devices

10. Choose one or more gateway sites from **Available Sites** and move them to **Selected Sites**.

11. (Cisco vEdge devices for releases before Cisco IOS XE Release 17.7.1a) To specify GRE interfaces for Cloud OnRamp for SaaS to use, perform the actions in Steps 11a through 11d.

    (Cisco vEdge devices for releases from Cisco IOS XE Release 17.7.1a) To specify the VPN 0 interfaces or service VPN interfaces in gateway sites for Cloud OnRamp for SaaS to use, perform the actions in Steps 11a through 11d.

Note If you do not specify interfaces for Cloud OnRamp for SaaS to use, the system selects a NAT-enabled physical interface from VPN 0.

    a. Click **Add interfaces** to selected sites (optional), located in the bottom-right corner of the **Attach Gateways** window.

    b. Click **Select Interfaces**.

    c. From the available interfaces, choose the GRE interfaces to add (for releases before Cisco IOS XE Release 17.7.1a), or the VPN 0 interfaces or service VPN interfaces to add (for releases from Cisco IOS XE Release 17.7.1a).

    d. Click **Save Changes**.

12. (Cisco IOS XE SD-WAN devices) To configure the routers at a gateway site, perform the following steps.

Note If you don’t specify interfaces for Cloud OnRamp for SaaS, an error message indicates that the interfaces aren’t VPN 0.

    a. Click **Add interfaces to selected sites**.

    b. The **Attach Gateways** window shows each WAN edge router at the gateway site.

    Beginning with Cisco IOS XE Release 17.6.1a, you can choose Service VPN or VPN 0 if the gateway uses Cisco IOS XE SD-WAN devices.

    - If the routers at the gateway site connect to the internet using service VPN connections (VPN 1, VPN 2, …), choose **Service VPN**.
    - If the routers at the gateway site connect to the internet using VPN 0, choose **VPN 0**.

Note

- Correctly choosing **Service VPN** or **VPN 0** requires information about how the gateway site connects to the internet.
- All WAN edge routers at the gateway site must use either service VPN or VPN 0 connections for internet access. Cloud OnRamp for SaaS does not support a mix of both.

c. Do one of the following:

   - If you chose **Service VPN**, then for each WAN edge router, choose the interfaces to use for internet connectivity.
   - If you chose **VPN 0**, then either choose **All DIA TLOC**, or choose **TLOC list** and specify the colors to include in the TLOC list.

d. Click **Save Changes**.

13. Click **Attach**. Cisco vManage saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
14. To return to the Cloud OnRamp for SaaS Dashboard, from the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

Configure Direct Internet Access (DIA) Sites

Note Cloud onRamp for SaaS requires an SD-WAN tunnel to each physical interface to enable SaaS probing through the interface. For a physical interface configured for DIA only, without any SD-WAN tunnels going to the SD-WAN fabric, configure a tunnel interface with a default or any dummy color in order to enable use of Cloud onRamp for SaaS. Without a tunnel interface and color configured, no SaaS probing can occur on a DIA-only physical interface.

1. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.
2. From the **Manage Cloud OnRamp for SaaS** drop-down list, located to the right of the title bar, choose **Direct Internet Access (DIA) Sites**.

   The **Manage DIA**window provides options to attach, detach, or edit DIA sites, and shows a table of sites configured for the Cloud onRamp service.
3. Click **Attach DIA Sites**. The **Attach DIA Sites** dialog box displays all sites in your overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
4. In the **Device Class** field, select one of the following:
   - **Cisco OS**: Cisco IOS XE SD-WAN devices
   - **Viptela OS (vEdge)**: Cisco vEdge devices
5. Choose one or more DIA sites from **Available Sites** and move them to **Selected Sites**.
6. (For Cisco vEdge devices) By default, if you don’t specify interfaces for Cloud OnRamp for SaaS to use, the system selects all NAT-enabled physical interfaces from VPN 0. Use the following steps to specify particular interfaces for Cloud OnRamp for SaaS.

   Note You can’t select a loopback interface.

   a. Click the link, **Add interfaces to selected sites** (optional), located in the bottom-right corner of the window.

   b. In the **Select Interfaces** drop-down list, choose interfaces to add.

   c. Click **Save Changes**.

7. (For Cisco IOS XE SD-WAN devices, optional) Specify TLOCs for a site.

   Note Configuring Cloud onRamp for SaaS when using a loopback as a TLOC interface is not supported.

   Note If you do not specify TLOCs, the **All DIA TLOC** option is used by default.

   a. Click the **Add TLOC to selected sites** link at the bottom-right corner of the **Attach DIA Sites** dialog box.

   b. In the **Edit Interfaces of Selected Sites** dialog box, choose **All DIA TLOC**, or **TLOC List** and specify a TLOC list.

   c. Click **Save Changes**.

8. Click **Attach**. The Cisco vManage NMS saves the feature template configuration to the devices. The **Task View** window displays a Validation Success message.

9. To return to the Cloud OnRamp for SaaS Dashboard, from the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

Configure Cloud onRamp for SaaS Over SIG Tunnels

Table 37: Feature History

Feature Name	Release Information	Description
Cloud onRamp for SaaS Over SIG Tunnels	Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature lets you to connect to Cloud onRamp for SaaS by means of a SIG tunnel.

Configure Cloud onRamp for SaaS over SIG Tunnels Using DIA

1. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

2. From **Manage Cloud OnRamp for SaaS**drop-down lsit, choose **Direct Internet Access (DIA) Sites**.

3. Click **Attach DIA Sites**.

   The **Attach DIA Sites** dialog box displays all the sites in your overlay network, with the available sites highlighted.

4. In **Device Class**, select:

Viptela OS (vEdge)

5. In the **Available Sites** pane, select a site that you want to attach, and click the right arrow. To remove a site, in the **Selected Sites** pane, click a site, and then click the left arrow.
6. Click **Add interfaces to selected sites**.
7.
8. Choose SIG tunnels from a list of interfaces or check the **All Auto SIG Interfaces** check box.
9. Click **Save Changes**.
10. Click **Attach**.

    Cisco vManage pushes the feature template configuration to the devices, and the **Task View** window displays a `Validation Success` message.

Configure Cloud onRamp for SaaS over SIG Tunnels Using a Gateway

To configure Cloud onRamp for SaaS over SIG tunnels a Gateway, perform the following steps:

1. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.
2. From **Manage Cloud OnRamp for SaaS** drop-down list, choose **Gateways**.
3. Click **Attach Gateways**.

   The **Attach Gateways** pop-up window displays all the sites in your overlay network, with available sites highlighted.
4. In **Device Class**, select:

   Viptela OS (vEdge)
5. In the **Available Sites** pane, select a site that you want to attach, and click the right arrow. To remove a site, in the **Selected Sites** pane, click a site, and then click the left arrow
6. Click **Add interfaces to selected sites**.
7. Choose SIG tunnels from a list of interfaces or check the **All Auto SIG Interfaces** check box.
8. Click **Save Changes**.
9. Click **Attach**. Cisco vManage pushes the feature template configuration to the devices, and the **Task View** window displays a `Validation Success` message.

View Details of Monitored Applications

1. Open Cloud onRamp for SaaS.
   - From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

     or
   - In Cisco vManage, click the cloud icon at the top right and click **Cloud onRamp for SaaS**.

   The page includes a tile for each monitored application, with the following information:
   - How many sites are operating with Cloud onRamp for SaaS.

- A color-coded rating of the Quality of Experience (vQoE) score for the application (green=good score, yellow=moderate score, red=poor score) on the devices operating at each site.

2. Optionally, you can click a tile to show details of Cloud onRamp for SaaS activity for the application, including the following:

Field	Description
vQoE Status	A green checkmark indicates that the vQoE score for the best path meets the criteria of an acceptable connection. The vQoE is calculated based on average loss and average latency. For Office 365 traffic, other connection metrics are also factored in to the vQoE score.
vQoE Score	For each site, this is the vQoE score of the best available path for the cloud application traffic. The vQoE score is determined by the Cloud onRamp for SaaS probe. Depending on the type of routers at the site, you can view details of the **vQoE Score** as follows: • Cisco IOS XE SD-WAN devices: To show a chart of the vQoE score history for each available interface, click the chart icon. In the chart, each interface vQoE score history is presented as a colored line. A solid line indicates that Cloud onRamp for SaaS has designated the interface as the best path for the cloud application at the given time on the chart. You can place the cursor over a line, at a particular time on the chart, to view details of the vQoE score of an interface at that time. From Cisco vManage Release 20.8.1, for the Office 365 application, the chart includes an option to show the vQoE score history for a specific service area, such as Exchange, Sharepoint, or Skype. For each service area, a solid line in the chart indicates the interface chosen as the best path at a given time. If you have enabled Cloud onRamp for SaaS to use Microsoft traffic metrics for Office 365 traffic, the choice of best path takes into account the Microsoft traffic metrics. • Cisco vEdge devices: To show a chart of the vQoE score history, click the chart icon. The chart shows the vQoE score for the best path chosen by Cloud onRamp for SaaS.
DIA Status	The type of connection to the internet, such as local (from the site), or through a gateway site.
Selected Interface	The interface providing the best path for the cloud application. **Note** If the DIA status is Gateway, this field displays **N/A**.
Activated Gateway	For a site that connects to the internet through a gateway site, this indicates the IP address of the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.

Field	Description
Local Color	For a site that connects to the internet through a gateway site, this is the local color identifier of the tunnel used to connect to the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.
Remote Color	For a site that connects to the internet through a gateway site, this is the remote (gateway site) color identifier of the tunnel used to connect to the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.
SDWAN Computed Score	This field is applicable only if the site uses Cisco IOS XE SD-WAN devices. It does not apply for Cisco vEdge devices. From Cisco vManage Release 20.8.1, for the Microsoft Office 365 application, an **SDWAN Computed Score** column provides links to view charts of the path scores (OK, NOT-OK, or INIT) provided by Microsoft telemetry for each Microsoft service area, including Exchange, Sharepoint, and Skype. The chart shows the scores over time for each available interface. The scores are defined as follows: • **OK**: Acceptable path • **NOT-OK**: Unacceptable path • **INIT**: Insufficient data These charts provide visibility into how Cloud onRamp for SaaS chooses a best path for each type of Microsoft Office 365 traffic. A use case for viewing the path score history is for determining whether Microsoft consistently rates a particular interface as NOT-OK for some types of traffic, such as Skype traffic.

Enable Application Feedback Metrics for Office 365 Traffic

Beginning with Cisco IOS XE Release 17.4.1a, you can enable the following types of application feedback from additional sources. Cloud onRamp for SaaS can use these metrics to help determine the best path for Office 365 traffic.

- Enable telemetry with Microsoft Exchange cloud servers, which can provide best path metrics for Office 365 traffic on specifically configured interfaces. This involves use of a Microsoft service called Microsoft 365 informed network routing. To understand this feature better, see the information available in the Microsoft 365 informed network routing document.

- Enable application response time (ART) metrics, which configures network devices to report ART metrics.

Before You Begin

- Enable monitoring for Office 365 traffic.

- Configure a policy for Office 365, for Cisco IOS XE SD-WAN devices.
- To enable NetFlow metrics, enable Cloud Services.

  (From the Cisco vManage menu, choose **Administration** > **Settings** > **Cloud Services**)
- To enable NetFlow metrics for devices in the network, enable the **NetFlow** and **Application** options in the localized policy for each device.

  (From the Cisco vManage menu, choose **Configuration** > **Policies** > **Localized Policy** > **Policy template**, **Policy Settings** section)
- Enable Cisco vAnalytics. See Cisco vAnalytics Insights.

Enable Application Feedback Metrics for Office 365 Traffic

1. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.
2. In the **Manage Cloud onRamp for SaaS** drop-down list, choose **Applications and Policy**.
3. In the **Office 365** row, click the **Enable Application Feedback for Path Selection** link.

   The **Application Feedback** dialog box opens.
4. In the **Application Feedback** dialog box, enable traffic metrics:
   - **Telemetry**: Enable Telemetry with Microsoft Exchange cloud servers to receive traffic metrics for Office 365 traffic over specific configured interfaces.

     If the option is disabled and the dialog box shows a message requesting sign-in to a Microsoft account, copy the code provided in the message and click the link to sign in. Provide the code on the Microsoft page that is displayed and log in with your Microsoft tenant account credentials when prompted. After signing in, the **Telemetry** option in the dialog box is enabled.
   - **Traffic Steering**: From Cisco vManage Release 20.9.1, check this check box to allow Cloud OnRamp for SaaS to factor in the Microsoft telemetry data in the best path decision. If you disable this, you can still view the Microsoft telemetry data in the Cisco vAnalytics dashboard, but the telemetry does not affect the best path decision.
   - (Optional) **Application Response Time (ART)**: Enable ART metrics.

   Note Enabling ART automatically configures devices to report ART metrics.
5. Click **Save**.

View Office 365 Application Logs

You can view a log of the metrics that factor into the best-path determination for Office 365 traffic. The metrics appear in a Cisco vAnalytics page specifically designed to display this information. The logs provide detailed information regarding status, but are not necessary for using Cloud onRamp for SaaS.

Beginning with Cisco vManage Release 20.8.1, you can view the path score history in a chart form. See View Details of Monitored Applications, on page 106.

Prerequisites

- Enable Microsoft traffic metrics.
- Enable monitoring for Office 365 traffic.

Procedure

1. In Cisco vManage, open **Configuration** > **Cloud onRamp for SaaS**.
2. Click the **Office 365** box.

   Note The box appears only if monitoring is enabled for Office 365 traffic.

3. In the **Office 365** window, click the **View Application Logs** link.
4. Log in using Cisco vAnalytics credentials. See Cisco vAnalytics Insights.

   A **Cisco SD-WAN vAnalytics** page opens. This is a Cisco vAnalytics view designed specifically for Cloud onRamp for SaaS, and only provides access to the Cloud onRamp for SaaS metrics for Office 365 traffic. It does not provide other Cisco vAnalytics functionality

5. Select an option from the cloud icon in the left pane to display various logs. Use the filter and interval options above the table to determine what log data to include.

Log Type	Description
Path Scores (**Cloud icon** > **Path Score**)	(This is the default display.) Shows a table with a log of path scores, according to interface. Each line shows the scores and related information for a specific interface at a given time. **Note** The Microsoft Teams service may appear in the table as Skype. The **Score** area includes the following columns: • **MSFT**: Path score determined by Microsoft. • **SDWAN**: Path score determined by all metrics (ART, Cloud OnRamp for SaaS path probing metrics, and Microsoft telemetry metrics). This is the score that primarily determines whether a path is acceptable for traffic. In the **MSFT** and **SDWAN** columns, the table shows the status as one of the following: • **OK**: Acceptable path • **NOT-OK**: Not acceptable path • **INIT**: Insufficient data

View Server Information Using the SD-AVC Cloud Connector

Before You Begin

- Enable SD-AVC (**Administration** > **Cluster Management**, click **...** and choose **Edit**, and choose **Enable SD-AVC**).
- Enable the SD-AVC Cloud Connector. See Enable Cisco SD-AVC Cloud Connector in the *Cisco SD-WAN Getting Started Guide*.

View Server Information

1. From the Cisco vManage menu, choose **Monitor** > **SD-AVC Cloud Connector**.
2. - For the Office 365 application, the **SD-AVC Cloud Connector** page shows the following information collected from Microsoft Cloud about the Microsoft application servers that handle Office 365 traffic:

Field	Description
Domain tab	
Application Name	Name of the application producing the traffic. Network-Based Application Recognition (NBAR), a component of Cisco IOS XE, provides the application name.
Domain	Destination domain of the traffic. This is the application server handling the cloud application traffic.
Service Area	The service area categorization, as determined by Microsoft, including **exchange**, **sharepoint**, **skype**, and **common**.
Category	Traffic categorization by Microsoft as **optimize**, **allow**, or **default**. A dash in this field indicates traffic that does not have a defined category.
IP Address tab	
IP	Destination IP of the traffic. This is the IP address of the application server handling the cloud application traffic.
Port	Destination port of the traffic.
L4 Protocol	Transport protocol of the traffic, such as TCP or UDP.
Application	Name of the application producing the traffic. NBAR, a component of Cisco IOS XE, provides the application name.
Category	Traffic categorization by Microsoft as **optimize**, **allow**, or **default**. A dash in this field indicates that traffic does not have a defined category.
Service Area	The service area categorization, as determined by Microsoft, including **exchange**, **sharepoint**, **skype**, and **common**.

3. Optionally, you can use the search field to filter the information in the table. For example, you can filter by an application name or by a domain name.

Application Lists

Table 38: Feature History

Feature Name	Release Information	Description
User-Defined SaaS Application Lists	Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	In Cisco vManage, you can define lists of one or more SaaS applications, together with the relevant application server. Cloud onRamp for SaaS handles these lists in the same way that it handles the predefined set of SaaS applications that it can monitor. When you enable a user-defined list, Cloud onRamp for SaaS probes for the best path to the application server and routes the application traffic for applications in the list to use the best path.

Create a User-Defined SaaS Application List Using Cisco vManage

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco vManage Release 20.8.1

1. Open the Cloud onRamp for SaaS page, using one of the following methods:

   - From the Cisco vManage main menu, choose **Configuration** > **Cloud onRamp for SaaS**.

     or

   - From the Cisco vManage menu, click the cloud icon near the top right and select **Cloud onRamp for SaaS**.

2. In the **Manage Cloud onRamp for SaaS** drop-down list, choose **SaaS Application Lists**.

3. Click **New Custom Application List**.

4. Enter a name for the list.

5. To add applications to the list, click the **Search** field and choose applications. The list includes standard applications and any custom applications that you have defined.

   Optionally, you can enter text in the **Search** field to filter for specific applications.

   The applications that you choose are added to the **Application** field, which shows each application in the list.

6. Optionally, to create a new custom application within this workflow, click the **Search** field and then click **New Custom Application**. Creating a custom application on this page is equivalent to defining a custom application in the centralized policy workflow, as described in Define Custom Applications. See Define Custom Applications Using Cisco vManage for information about the what information is required for defining a custom application, the use of wildcard characters, the logic applied when matching traffic to the attributes that you enter, and so on.

7. In the **SaaS Probe Endpoint Type** area, define the probe endpoint, which is the server that Cloud onRamp for SaaS probes to determine a best path for the traffic in the SaaS application list.

- Choose an endpoint type from the following options:
  - **IP Address**: Enter an IP address. Cloud onRamp for SaaS probes the server using port 80.
  - **FQDN**: Enter a fully qualified domain name.
  - **URL**: Enter a URL using HTTP or HTTPS. Cloud onRamp for SaaS probes the server using port 80 or port 443, depending on the URL provided.
- Enter an endpoint value, based on the endpoint type that you choose.

  Examples: 192.168.0.1, https://www.example.com

8. Click **Add**. The new SaaS application list appears in the table of application lists.

View SaaS Application Lists

Minimum supported releases: Cisco IOS XE Release 17.8.1a, Cisco vManage Release 20.8.1

1. Open the Cloud onRamp for SaaS page, using one of the following methods:
   - From the Cisco vManage main menu, choose **Configuration** > **Cloud onRamp for SaaS**.

     or

   - From the Cisco vManage menu, click the cloud icon near the top right and select **Cloud onRamp for SaaS**.
2. In the **Manage Cloud onRamp for SaaS** drop-down list, choose **SaaS Application Lists**.

   A table shows the details of each SaaS application list. Optionally, you can click an icon in the **Action** column to edit or delete a list.

Configure Controller Certificate Authorization Settings

Signed certificates are used to authenticate devices in the overlay network. Once authenticated, devices can establish secure sessions between each other. It is from the Cisco vManage that you generate these certificates and install them on the controller devices—Cisco vBond orchestrators,Cisco vManage, and Cisco vSmart controllers. You can use certificates signed by Symantec, or you can use enterprise root certificates.

The controller certification authorization settings establish how the certification generation for all controller devices will be done. They do not generate the certificates.

You need to select the certificate-generation method only once. The method you select is automatically used each time you add a device to the overlay network.

To have the Symantec signing server automatically generate, sign, and install certificates on each controller device:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Symantec Automated** (Recommended). This is the recommended method for handling controller signed certificates.

3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to confirm that you wish to have the Symantec signing server automatically generate, sign, and install certificates on each controller device.
4. Enter the first and last name of the requester of the certificate.
5. Enter the email address of the requester of the certificate. This address is required because the signed certificate and a confirmation email are sent to the requester via email; they are also made available though the customer portal.
6. Specify the validity period for the certificate. It can be 1, 2, or 3 years.
7. Enter a challenge phrase. The challenge phrase is your certificate password and is required when you renew or revoke a certificate.
8. Confirm your challenge phrase.
9. In **Certificate Retrieve Interval**, specify how often the Cisco vManage server checks if the Symantec signing server has sent the certificate.
10. Click **Save**.

To manually install certificates that the Symantec signing server has generated and signed:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Symantec Manual**.
3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to manually install certificates that the Symantec signing server has generated and signed.
4. Click **Save**.

To use enterprise root certificates:

1. From **Controller Certificate Authorization**, click **Edit**.
2. Click **Enterprise Root Certificate**.
3. In the **Confirm Certificate Authorization Change** dialog box, click **Proceed** to confirm that you wish to use enterprise root certificates.
4. In the **Certificate** box, either paste the certificate, or click **Select a file** and upload a file that contains the enterprise root certificate.
5. By default, the enterprise root certificate has the following properties: To view this information, issue the **show certificate signing-request decoded** command on a controller device, and check the output in the Subject line. For example:
   - Country: United States
   - State: California
   - City: San Jose
   - Organizational unit: ENB
   - Organization: CISCO
   - Domain Name: cisco.com

- Email: cisco-cloudops-sdwan@cisco.com

```
vSmart# show certificate signing-request decoded
    ...
    Subject: C=US, ST=California, L=San Jose, OU=ENB, O=CISCO, CN=vsmart-uuid
.cisco.com/emailAddress=cisco-cloudops-sdwan@cisco.com
    ...
```

To change one or more of the default CSR properties:

a. Click **Set CSR Properties**.

b. Enter the domain name to include in the CSR. This domain name is appended to the certificate number (CN).

c. Enter the organizational unit (OU) to include in the CSR.

d. Enter the organization (O) to include in the CSR.

e. Enter the city (L), state (ST), and two-letter country code (C) to include in the CSR.

f. Enter the email address (emailAddress) of the certificate requester.

g. Specify the validity period for the certificate. It can be 1, 2, or 3 years.

6. Click **Import & Save**.

Configure CUBE

Table 39: Feature History

Feature Name	Release Information	Description
Cisco Unified Border Element Configuration	Cisco IOS XE Release 17.7.1a Cisco vManage Release 20.7.1	You can configure Cisco Unified Border Element functionality by using Cisco IOS XE SD-WAN device CLI templates or CLI add-on feature templates.

To configure a device to use the CUBE functionality, create a Cisco IOS XE SD-WAN device CLI template or a CLI add-on feature template for the device.

For information about device CLI templates, see CLI Templates for Cisco IOS XE SD-WAN Device Routers.

For information about CLI add-on feature templates, see CLI Add-On Feature Templates.

For information about CUBE configuration and usage, see *Cisco Unified Border Element Configuration Guide*.

For information about the CUBE commands that Cisco SD-WAN supports for use in a CLI template, see CUBE Commands .

The following example shows a basic CUBE configuration using a CLI add-on template:

```
voice service voip
 ip address trusted list
```

```
  ipv4 10.0.0.0.255.0.0.0
  ipv6 2001:DB8:0:ABCD::1/48
  !
 allow-connections sip to sip
 sip
  no call service stop
  !
dial-peer voice 100 voip
  description Inbound LAN side dial-peer
  session protocol sipv2
  incoming called number .T
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 101 voip
  description Outbound LAN side dial-peer
  destination pattern [2-9].........
  session protocol sipv2
  session target ipv4:10.10.10.1
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 200 voip
  description Inbound WAN side dial-peer
  session protocol sipv2
  incoming called-number .T
  voice-class codec 1
  dtmf-relay rtp-nte
  !
 dial-peer voice 201 voip
  description Outbound WAN side dial-peer
  destination pattern [2-9].........
  session protocol sipv2
  session target ipv4:20.20.20.1
  voice-class codec 1
  dtmf-relay rtp-nte
```

Configure Custom Applications Using Cisco vManage

Prerequisites

Install Cisco SD-AVC as a component of Cisco SD-WAN. For information on how to enable SD-AVC on Cisco vManage, see Information on how to enable SD-AVC for Cisco SD-WAN devices.

Perform the following steps to configure custom applications:

1. In Cisco vManage, select **Configuration** > **Policies**.
2. Select **Centralized Policy**.
3. Click **Custom Options** and select **Centralized Policy** > **Lists**.
4. Click **Custom Applications**, and then click **New Custom Application**.
5. To define the application, provide an application name and enter match criteria. The match criteria can include one or more of the attributes provided: server names, IP addresses, and so on. You do not need to enter match criteria for all fields.

   The match logic follows these rules:

- Between all L3/L4 attributes, there is a logical AND. Traffic must match all conditions.
- Between L3/L4 and Server Names, there is a logical OR. Traffic must match either the server name or the L3/L4 attributes.

Field	**Description**
Application Name	(mandatory) Enter a name for the custom application. Maximum length: 32 characters
Server Names	One or more server names, separated by commas. You can include an asterisk wildcard match character (*) only at the beginning of the server name. Examples: *cisco.com, *.cisco.com (match www.cisco.com, developer.cisco.com, …)
L3/L4 Attributes	
IP Address	Enter one or more IPv4 addresses, separated by commas. Example: 10.0.1.1, 10.0.1.2 **Note** The subnet prefix range is 24 to 32.
Ports	Enter one or more ports or port ranges, separated by commas. Example: 30, 45-47
L4 Protocol	Select one of the following: TCP, UDP, TCP-UDP

6. Click **Add**. The new custom application appears in the table of custom applications.

Note To check the progress of creating the new custom application, click **Tasks** (clipboard icon). A panel opens, showing active and completed processes.

Example Custom Application Criteria

Criteria	**How to configure fields**
Domain name	**Server Names**: cisco.com

Criteria	How to configure fields
Set of IP addresses, set of ports, and L4 protocol	**IP Address**: 10.0.1.1, 10.0.1.2 **Ports**: 20, 25-37 **L4 Protocol**: TCP-UDP
Set of ports and L4 protocol	**Ports**: 30, 45-47 **L4 Protocol**: TCP

Configure Tunnels

Table 40: Feature History

Feature	Release Information	Description
IPSEC/GRE Tunnel Routing and Load-Balancing Using ECMP	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	You can use the SIG template to steer application traffic to Cisco Umbrella or a Third party SIG Provider. You can also configure weights for multiple GRE/IPSEC tunnels for distribution of traffic among multiple tunnels based on the configured weights.
Enable Layer 7 Health Check (Automatic Tunnels)	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	You can configure Automatic Tunnels using Cisco vManage.
Support for Zscaler Automatic IPSec Tunnel Provisioning	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature automates the provisioning of tunnels from Cisco SD-WAN routers to Zscaler. Using your Zscaler partner API credentials, you can automatically provisions tunnels to Zscaler Internet Access (ZIA) Public Service Edges. You can choose **Zscaler** in the Cisco Security Internet Gateway (SIG) and SIG credentials feature templates to automate tunnel provisioning. You can configure provisioning of tunnels from Cisco SD-WAN routers.

Feature	Release Information	Description
Layer 7 Health Check for Manual Tunnels	Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	You can create and attach trackers to manually created GRE or IPSec tunnels to a SIG endpoint. Trackers help failover traffic when a SIG tunnel is down. You can configure the trackers using the SIG feature template.
Global SIG Credentials Template	Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	With this feature, create a single global SIG Credentials template for each SIG provider (Cisco Umbrella or Zscaler). When you attach a SIG template to a device template, Cisco vManage automatically attaches the applicable global SIG Credentials template to the device template.

Configure Automatic Tunnels Using Cisco vManage

Prerequisites

To configure automatic tunneling to a SIG, complete the following requisites:

- Cisco Umbrella: To configure automatic tunnels to Cisco Umbrella, you can do one of the following
    - For Cisco vManage to fetch the API keys, specify Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**. Your Cisco Smart Account is the account that you use to log in to the Cisco Smart Software Manager (CSSM) portal.
    - To manually specify the API keys, generate Umbrella Management API keys. See *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

      Specify the generated keys in the SIG Credentials template.
- Zscaler Internet Access (ZIA): To configure automatic tunnels to Zscaler, do the following:
    1. Create partner API keys on the ZIA Partner Integrations page.
    2. Add the Partner Administrator role to the partner API keys.
    3. Create a Partner Administrator.
    4. Activate the changes.

  For more information, see *Managing SD-WAN Partner Keys* on the Zscaler Help Center.

  Specify the generated keys in the SIG Credentials template.

Create Cisco Umbrella SIG Credentials Template

Minimum supported release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a SIG Feature Template, on page 123, on selecting Umbrella as the SIG provider, Cisco vManage prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - SIG Credentials template** to create the Cisco Umbrella SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 41: SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Umbrella Global Credentials
Description	(Read only) Global credentials for Umbrella

1. In the **Basic Details** section, do one of the following:

   - Enable Cisco vManage to fetch credentials from the Cisco Umbrella portal:

     a. Ensure that you have added your Cisco Smart Account credentials here: **Administration** > **Settings** > **Smart Account Credentials**.

        Cisco vManage uses the Cisco Smart Account credentials to connect to the Cisco Umbrella portal.

     b. Click **Get Keys**.

        Cisco vManage obtains the following details:

        - Organization ID
        - Registration Key
        - Secret

   - Enter Cisco Umbrella credentials:

     Table 42: Cisco Umbrella Credentials

Field	Description
SIG Provider	(Read only) Umbrella
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see *Find Your Organization ID* in the *Cisco Umbrella SIG User Guide*.
Registration Key	Enter the Umbrella Management API Key. For more information, see *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

Field	Description
Secret	Enter the Umbrella Management API Secret. For more information, see *Management and Provisioning* > *Getting Started* > *Overview* in the *Cloud Security API* documentation on the Cisco DevNet portal.

2. To save the template, click **Save**.

Create Zscaler SIG Credentials Template

Minimum release: Cisco vManage Release 20.9.1

When you Create Automatic Tunnels Using a SIG Feature Template, on page 123, on selecting Zscaler as the SIG provider, Cisco vManage prompts you to create the global SIG credentials template, if you haven't yet created the template. Click **Click here to create - SIG Credentials template** to create the Zscaler SIG credentials template.

Template Name and **Description** fields are prefilled:

Table 43: SIG Credentials Template Name and Description

Field	Description
Template Name	(Read only) Zscaler-Global-Credentials
Description	(Read only) Global credentials for Zscaler

1. In the **Basic Details** section, enter the Zscaler credentials:

Table 44: Zscaler Credentials

Field	Description
SIG Provider	(Read only) Zscaler
Organization	Name of the organization in Zscaler cloud. For more information, see *ZIA Help* > *Getting Started* > *Admin Portal* > *About the Company Profile*.
Partner base URI	This is the base URI that Cisco vManage uses in REST API calls. To find this information on the Zscaler portal, see *ZIA Help* > *ZIA API* > *API Developer & Reference Guide* > *Getting Started*.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see *ZIA Help* > *Partner Integrations* > *Managing SD-WAN Partner Keys*.

2. To save the template, click **Save**.

Create SIG Credentials Template

Applicable releases: Cisco vManage Release 20.8.x and earlier releases.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **Other Templates**, click **SIG Credentials**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

7. In the **Description** field, enter a description for the feature template.
8. In **Basic Details** section, do the following:

   a. **SIG Provider**: Click **Umbrella** or **Zscaler**.

   b. For Cisco Umbrella, enter the following registration parameters or click **Get Keys** to have Cisco vManage fetch these parameters from the Cisco Umbrella portal.

      - **Organization ID**
      - **Registration Key**
      - **Secret**

      To fetch the parameters, Cisco vManage uses your Smart Account credentials to connect to the Cisco Umbrella portal. To manually enter the parameters, generate the values in your Umbrella account as described here.

   c. For Zscaler, enter the following details:

Field	Description
Organization	The name of the organization in Zscaler cloud. To find this information in Zscaler, see **Administration** > **Company Profile**.
Partner base URI	This is the Zscaler Cloud API that Cisco SD-WAN uses to connect to Zscaler. To find this information in Zscaler, see **Administration** > **API Key Management**.
Username	Username of the SD-WAN partner account.
Password	Password of the SD-WAN partner account.

Field	Description
Partner API key	The partner API key. To find the key in Zscaler, see **Zscaler Cloud Administration** > **Partner Integrations** > **SD-WAN**.

9. Click **Save**.

Create Automatic Tunnels Using a SIG Feature Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **VPN**, click **Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. (From Cisco vManage Release 20.9.1) **SIG Provider**: Click **Umbrella** or **Zscaler**.

   From Cisco vManage Release 20.9.1, on selecting **Umbrella** or **Zscaler** as the SIG provider, Cisco vManage prompts you to create the corresponding global SIG credentials template if you haven't yet created the template. Click **Click here to create - SIG Credentials template** to create the Cisco Umbrella or Zscaler SIG credentials template.
9. To create one or more trackers to monitor tunnel health, do the following in the **Tracker** section:

Note From Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1 , you can create customized trackers to monitor the health of automatic tunnels. If you do not customize the SLA parameters, Cisco vManage creates a default tracker for the tunnel.

   a. Click **New Tracker**.
   b. Configure the following:

Table 45: Tracker Parameters

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.

Field	Description
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds.
Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.

Note Prior to Cisco vManage Release 20.8.1, SIG tracker monitor statistics were reset at every Domain Name System (DNS) cache timeout interval.

Beginning with Cisco vManage Release 20.8.1, SIG tracker monitor statistics are no longer reset at every DNS cache timeout interval. SIG tracker monitor statistics are reset every two hours. A SIG tracker allows you to track the health of your SIG tunnels.

c. Click **Add**.

d. To add more trackers, repeat sub-step **b** to sub-step **d**.

10. To create tunnels, do the following in the **Configuration** section:

a. (Cisco 20.8.x and earlier releases) **SIG Provider**: Click **Umbrella** or **Zscaler**.

b. Click **Add Tunnel**.

c. Under **Basic Settings**, configure the following:

Table 46: Basic Settings

Field	Description
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec template.
Description	Enter a description for the interface.

Field	Description
Tracker	By default, a tracker is attached to monitor the health of automatic tunnels to Cisco Umbrella or Zscaler. If you configured a customized tracker in step **8**, choose the tracker. **Note** From Cisco SD-WAN Release 20.5.1 and Cisco vManage Release 20.5.1, you can create customized trackers to monitor the health of automatic tunnels.
Tunnel Source Interface	Enter the name of the source interface of the tunnel. This interface should be the egress interface and is typically the internet-facing interface.
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.

d. (Optional) Under **Advanced Options**, configure the following:

Table 47: General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: **No**.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco vManage enables a tracker for automatic tunnels. **Default**: **On**.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 10 to 3600 seconds **Default**: 10

Field	Description
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. Once 1 DPD message is missed by the peer, the router moves to a more aggressive state and sends the DPD retry message at the faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five aggressive DPD retry messages can be missed before the tunnel is marked as down. **Range**: 2 to 60 seconds **Default**: 3

Table 48: IKE

Field Name	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys. **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 14 2048-bit modulus

Table 49: IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: AES 256 GCM
Perfect Forward Secrecy	• Specify the PFS settings to use on the IPsec tunnel. • Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: None

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

11. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 50: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

12. (Optional) Modify the default configuration in the **Advanced Settings** section:

Table 51: Umbrella

Field	Description
Umbrella Primary Data-Center	Cisco vManage automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.
Umbrella Secondary Data-Center	Cisco vManage automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Cisco Umbrella data center, choose the data center from the drop-down list.

Table 52: Zscaler

Field	Description
Primary Data-Center	Cisco vManage automatically selects the primary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list.
Secondary Data-Center	Cisco vManage automatically selects the secondary data center closest to the WAN edge device. If you wish to route traffic to a specific Zscaler data center, choose the data center from the drop-down list.
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Enable Surrogate IP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Display Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Idle Time to Disassociation	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enforce Surrogate IP for known browsers	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off

Field	Description
Refresh Time Unit	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Minute
Refresh Time	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
First Time AUP Block Internet Access	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
Force SSL Inspection	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: Off
AUP Frequency	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. **Default**: 0

13. Click **Save**.

Create Manual Tunnels Using SIG Feature Template

From Cisco SD-WAN Release 20.4.1 and Cisco vManage Release 20.4.1, all SIG related workflows for automatic and manual tunnels have been consolidated into the SIG template. If you are using Cisco SD-WAN Release 20.4.1 and Cisco vManage Release 20.4.1, or later, use the SIG template to configure GRE or IPSec tunnels to a third-party SIG, or GRE tunnels to a Zscaler SIG.

For a software release earlier than Cisco SD-WAN Release 20.4.1, Cisco vManage Release 20.4.1, see *Configuring a GRE Tunnel or IPsec Tunnel from Cisco vManage.*

Layer 7 Health Check: The option to create trackers and monitor the health of manually created tunnels is available from Cisco SD-WAN Release 20.8.1, Cisco vManage Relase 20.8.1. In earlier releases, the Layer 7 Health Check feature is only available if you use VPN Interface GRE/IPSEC templates, and not with SIG templates.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. Choose the device for which you are creating the template.
5. Under **VPN**, click **Secure Internet Gateway (SIG)**.
6. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 to 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the feature template.
8. (Optional) To create one or more trackers to monitor tunnel health, do the following in the Tracker section:

Note The option to create trackers and monitor tunnel health is available from Cisco SD-WAN Release 20.8.1, Cisco vManage Relase 20.8.1.

   a. Click **New Tracker**.
   b. Configure the following:

Field	Description
Name	Enter a name for the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. **Range**: 100 to 1000 milliseconds **Default**: 300 milliseconds
Interval	Enter the time interval between probes to determine the status of the configured endpoint. **Range**: 20 to 600 seconds **Default**: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. **Range**: 1 to 10 **Default**: 3
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel. **Note** Both HTTP and HTTPS API URLs are supported.

   c. Click **Add**.
   d. To add more trackers, repeat sub-step **b** to sub-step **d**.

9. To create tunnels, do the following in the **Configuration** section:

   a. **SIG** Provider: Click **Generic**.

      Cisco vManage Release 20.4.x and earlier: Click **Third Party**.

   b. Click **Add Tunnel**.

   c. Under **Basic Settings**, configure the following:

Field	Description
Tunnel Type	Based on the type of tunnel you wish to create, click **ipsec** or **gre**.
Interface Name (0..255)	Enter the interface name. **Note** If you have attached the Cisco VPN Interface IPSec feature template or the Cisco VPN Interface GRE feature template to the same device, ensure that the interface number you enter is different from what you have entered in the IPSec or GRE templates.
Description	(Optional) Enter a description for the interface.
Source Type	Click **INTERFACE** or **IP**.
Tracker	(Optional) Choose a tracker to monitor tunnel health. **Note** From Cisco SD-WAN Release 20.8.1 and Cisco vManage Relase 20.8.1, you can create trackers to monitor tunnel health.
Track this interface for SIG	Enable or disable tracker for the tunnel. By default, Cisco vManage enables a tracker for automatic tunnels. **Default**: **On**.
Tunnel Source Interface	This field is displayed only if you chose the **Source Type** as **INTERFACE.** Enter the name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface.
Tunnel Source IP Address	This field is displayed only if you chose the **Source Type** as **IP.** Enter the IP address of the tunnel source.
IPv4 address	This field is displayed only if you chose the **Source Type** as **IP.** (Optional) Enter the tunnel interface's IP address.
Tunnel Destination IP Address/FQDN	Enter the IP address of the SIG provider endpoint.
Preshared Key	This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.

d. (Optional) Under **Advanced Options**, configure the following:

Table 53: (Tunnel Type: gre) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None

Table 54: (Tunnel Type: gre) Keep Alive

Field	Description
Interval	Time duration between successive GRE keepalive messages. **Range**: 0 to 65535 seconds **Default**: 0
Retries	Number of times the keepalive messages are sent to the remote device when no response is received from the remote device. If no response is received after these many tries, the remote device is declared down. **Range**: 0 to 255 **Default**: 3

Table 55: (Tunnel Type: ipsec) General

Field	Description
Shutdown	Click **No** to enable the interface; click **Yes** to disable. **Default**: No.
IP MTU	Specify the maximum MTU size of packets on the interface. **Range**: 576 to 2000 bytes **Default**: 1400 bytes

Field	Description
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. **Range**: 500 to 1460 bytes **Default**: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. **Range**: 0 to 65535 seconds **Default**: 10
DPD Retries	Specify how many unacknowledged packets to send before declaring an IKE peer to be dead and then removing the tunnel to the peer. **Range**: 0 to 255 **Default**:3

Table 56: (Tunnel Type: ipsec) IKE

Field	Description
IKE Rekey Interval	Specify the interval for refreshing IKE keys **Range:** 300 to 1209600 seconds (1 hour to 14 days) **Default**: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 **Default**: AES 256 CBC SHA1

Field	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. Choose one of the following: • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus **Default**: 16 4096-bit modulus
IKE ID for Local Endpoint	If the remote IKE peer requires a local end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's source IP address
IKE ID for Remote Endpoint	If the remote IKE peer requires a remote end point identifier, specify the same. **Range**: 1 to 64 characters **Default**: Tunnel's destination IP address

Table 57: (Tunnel Type: ipsec) IPSEC

Field	Description
IPsec Rekey Interval	Specify the interval for refreshing IPSec keys. **Range**: 300 to 1209600 seconds (1 hour to 14 days) **Default**: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. **Options**: 64, 128, 256, 512, 1024, 2048, 4096. **Default**: 512

Field	Description
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 **Default**: NULL SHA 512
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS. **Default**: Group-16 4096-bit modulus

e. Click **Add**.

f. To create more tunnels, repeat sub-step **b** to sub-step **e**.

10. To designate active and back-up tunnels and distribute traffic among tunnels, configure the following in the **High Availability** section:

Table 58: High Availability

Field	Description
Active	Choose a tunnel that connects to the primary data center.

Field	Description
Active Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Weight	Enter a weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with a weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

11. Click **Save**.

Redirect Traffic to a SIG

You can redirect traffic to a SIG in two ways:

- Using Data Policy. For more information, see Action Parameters in the Policies Configuration Guide.
- Using the Service route to SIG. For more information, see Modify Service VPN Template, on page 137

Modify Service VPN Template

To ensure that the device connects to the SIG, you must modify the VPN template to include a service route to the SIG.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. For the VPN template of the device, click **Edit**.
4. Click **IPv4 Route**.
5. Click the delete icon on any existing IPv4 route to the internet.
6. Click **Service Route**.
7. Click **New Service Route**.
8. Enter a Prefix (for example, 10.0.0.0/8).
9. For the service route, ensure that **SIG** is chosen.
10. Click **Add**.
11. Click **Update**.

Create Device Template

1. From the Cisco vManage menu, choose **Configuration > Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device** .

3. Click **Create Template** and click **From Feature Template**.
4. From the **Device Model** drop-down list, choose the device model for which you are creating the template.

   Cisco vManage displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is chosen by default.
5. From the **Device Role** drop-down list, choose **SDWAN Edge**.
6. In the **Template Name** field, enter a name for the device template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
7. In the **Description** field, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.
8. Click **Transport & Management VPN**.
9. In the **Transport & Management VPN** section, under **Additional Cisco VPN 0 Templates**, click **Secure Internet Gateway**.

10. From the **Secure Internet Gateway** drop-down list, choose the SIG feature template that you created earlier.

11. Click **Additional Templates**.

12. In the **Additional Templates** section,

    a. Automatic tunneling:

       (Cisco vManage Release 20.8.x and earlier) From the **SIG Credentials** drop-down list, choose the relevant SIG Credentials feature template.

       (From Cisco vManage Release 20.9.1) Cisco vManage automatically chooses the applicable global SIG Credentials feature template based on the SIG feature template configuration.

Note If there are any changes to the SIG credentials, for these changes to take effect, you must first remove the SIG feature template from the device template and push the device template. Thereafter, re-attach the SIG feature template and then push the template to the device. For information on pushing the device template, see Attach the SIG Template to Devices.

    b. Manual tunneling: No need to attach a **SIG Credentials** template.

13. Click **Create**.

    The new configuration template is displayed in the **Device Template** table. The **Feature Templates** column shows the number of feature templates that are included in the device template, and the **Type** column shows **Feature** to indicate that the device template was created from a collection of feature templates.

Attach Template to Devices

To attach one or more devices to the device template:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.

2. Click **Device Templates**, and choose the template that you created.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is called **Device**.

3. For the desired template, click **...** and click **Attach Devices**.

   The Attach Devices dialog box displays.

4. In the **Available Devices** column, choose a group and search for one or more devices, choose a device from the list, or click **Select All**.

5. Click the arrow pointing right to move the device to the **Selected Devices** column.

6. Click **Attach**.

7. If the template contains variables, enter the missing variable values for each device in one of the following ways:

- Enter the values manually for each device either in the table column or by clicking **...** in the row and clicking **Edit Device Template**. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
- Click **Import File** to upload a CSV file that lists all the variables and defines each variable value for each device.

8. Click **Update**.

Configuring a GRE Tunnel or IPsec Tunnel from Cisco vManage

Table 59: Feature History

Feature Name	Release Information	Description
Manual Configuration for GRE Tunnels and IPsec Tunnels	Cisco SD-WAN Release 20.1.1	This feature lets you manually configure a GRE tunnel by using the VPN Interface GRE template or an IPSec tunnel by using the VPN Interface IPSec template. For example, use this feature to manually configure a tunnel to a SIG.

Note From Cisco SD-WAN Release 20.4.1, Cisco vManage Release 20.4.1, all SIG related workflows for Automatic and Manual Tunnels have been consolidated into the SIG template. If you are using Cisco SD-WAN Release 20.4.1, Cisco vManage Release 20.4.1, or later, configure GRE or IPSec tunnels to a generic SIG, or GRE tunnels to a Zscaler SIG, using the SIG template.

Configure Devices

You can create and store configurations for all devices—the Cisco vManage systems themselves, Cisco vSmart Controllers, Cisco vBond Orchestrators, and routers— by using Cisco vManage. When the devices start up, they contact Cisco vManage, which then downloads the device configuration to the device. (A device that is starting up first contacts the Cisco vBond Orchestrator, which validates the device and then sends it the IP address of Cisco vManage.)

The general procedure for creating configuration for all devices is the same. This section provides a high-level description of the configuration procedure. It also describes the prerequisite steps that must be performed before you can create configurations and configure devices in the overlay network.

Feature Templates

Feature templates are the building blocks of complete configuration for a device. For each feature that you can enable on a device, Cisco vManage provides a template form that you fill out. The form allows you to set the values for all configurable parameters for that feature.

Because device configurations vary for different device types and the different types of routers, feature templates are specific to the type of device.

Some features are mandatory for device operation, so creating templates for these features is required. Also for the same feature, you can create multiple templates for the same device type.

Note In releases prior to Cisco SD-WAN Release 20.7.1, if you enter < or > special characters in a Cisco vManage feature template definition or description, Cisco vManage generates a 500 exception error while attempting to preview a Cisco vManage feature template.

Starting from Cisco SD-WAN Release 20.7.1, if you enter < or > special characters in a Cisco vManage feature template definition or description, the special characters are converted to their HTML equivalents, **&lt;** and **&gt;**. This applies to all feature templates. You no longer receive a 500 exception error when previewing a Cisco vManage feature template.

Device Configuration Workflow

Devices in the overlay network that are managed by Cisco vManage must be configured from Cisco vManage. The basic configuration procedure is straightforward:

1. Create feature templates.
   a. From the Cisco vManage menu, choose **Configuration** > **Templates**.
   b. Click **Feature Templates**, and click **Add Templates**.

   Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

2. Create device templates.
   a. From the Cisco vManage menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and click **Create Templates**.

   Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Attach device templates to individual devices.
   a. From the Cisco vManage menu, choose **Configuration** > **Templates**.
   b. Click **Device Templates**, and choose a template.

   Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

   c. Click **…**, and select **Attach Devices**.

Template Variables

Within a feature template, some configuration commands and command options are identical across all device types. Others—such as a device system IP address, its geographic latitude and longitude, the timezone, and the overlay network site identifier—are variable, changing from device to device. When you attach the device template to a device, you are prompted to enter actual values for these command variables. You can do this either manually, by typing the values for each variable and for each device, or you can upload an Excel file in CSV format that contains the values for each device.

Configuration Prerequisites

Security Prerequisistes

Before you can configure any device in the network, that device must be validated and authenticated so that Cisco vManage systems, Cisco vSmart Controllers, and Cisco vBond Orchestrators recognize it as being allowed in the overlay network.

To validate and authenticate the controllers in the overlay network—Cisco vManage systems, vSmart controllers, and Cisco vSmart Controllers, and Cisco vBond Orchestrators—a signed certificate must be installed on these devices.

To validate and authenticate the routers, you receive an authorized serial number file from Cisco, which lists the serial and chassis numbers for all the routers allowed in your network. Then, you upload the serial number file to Cisco vManage.

Variables Spreadsheet

The feature templates that you create most likely contain variables. To have Cisco vManage populate the variables with actual values when you attach a device template to a device, create an Excel file that lists the variable values for each device and save the file in CSV format.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be the following, in this order:

- csv-deviceId—Serial number of the device (used to uniquely identify the device). For routers, you receive the serial numbers in the authorized serial number file sent to you from Cisco. For other devices, the serial number is included in the signed certificate you receive from Symantec or from your root CA.

  csv-deviceIP—System IP address of the device (used to populate the **system ip address** command).

- csv-host-name—Hostname of the device (used to populate the **system hostname** command).

You can create a single spreadsheet for all devices in the overlay network—Cisco vSmart Controllers, Cisco vBond Orchestrators, and routers. You do not need to specify values for all variables for all devices.

Create a Device Template from Feature Templates

Device templates define a device's complete operational configuration. A device template consists of a number of feature templates. Each feature template defines the configuration for a particular Cisco SD-WAN software feature. Some feature templates are mandatory, indicated with an asterisk (*), and some are optional. Each mandatory feature template, and some of the optional ones, have a factory-default template. For software features that have a factory-default template, you can use either the factory-default template (named Factory_Default_*feature-name*_Template) or you can create a custom feature template.

Create a Device Template from Feature Templates

To create a device template:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click the **Create Template** drop-down list, and select **From Feature Template**.
4. From the **Device Model** drop-down list, select the type of device for which you wish to create the template.

   vManage NMS displays all the feature templates for that device type. The required feature templates are indicated with an asterisk (*), and the remaining templates are optional. The factory-default template for each feature is selected by default.

5. In the **Template Name** field, enter a name for the device template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

6. In the **Description** field, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.

7. To view the factory-default configuration for a feature template, select the desired feature template and click **View Template**.
8. Click **Cancel** to return to the **Configuration Template** screen.
9. To create a custom template for a feature, select the desired factory-default feature template and click **Create Template**. The template form is displayed.

   This form contains fields for naming the template and defining the feature parameters.

10. In the **Template Name** field, enter a name for the feature template.

    This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

11. In the **Description** field, enter a description for the feature template.

    This field is mandatory, and it can contain any characters and spaces.

12. For each field, enter the desired value. You may need to click a tab or the plus sign (+) to display additional fields.
13. When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list of the parameter field and select one of the following:

Table 60:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template. When you click **Device Specific**, the **Enter Key** box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Use Variable Values in Configuration Templates. To change the default key, type a new string and move the cursor out of the **Enter Key** box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

14. For some groups of parameters, you can mark the entire group as device-specific. To do this, check the **Mark as Optional Row** check box.

    These parameters are then grayed out so that you cannot enter a value for them in the feature template. You enter the value or values when you attach a device to a device template.

15. Click **Save**.

16. Repeat Steps 6 through 13 to create a custom template for each additional software feature. For details on creating specific feature templates, see the templates listed in **Available Feature Templates**.

17. Click **Create**. The new configuration template is displayed in the Device Template table.

    The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Another way to create device templates from feature templates is to first create one or more custom feature templates and then create device templates. You can create multiple feature templates for the same feature. For a list of feature templates, see **Available Feature Templates**.

1. Click **Feature**.

2. Click **Add Template**.

3. From **Select Devices**, select the type of device for which you wish to create a template.

   You can create a single feature template for features that are available on multiple device types. You must, however, create separate feature templates for software features that are available only on the device type you are configuring.

4. Select the feature template. The template form is displayed.

   This form contains fields for naming the template and fields for defining the required parameters. If the feature has optional parameters, then the template form shows a plus sign (+) after the required parameters.

5. In the **Template Name** field, enter a name for the feature template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

6. In the **Description** field, enter a description for the feature template.

   This field is mandatory, and it can contain any characters and spaces.

7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down list of each parameter's value box.

8. Click the plus sign (+) from the required parameters to set the values of optional parameters.

9. Click **Save**.

10. Repeat Steps 2 to 9 for each additional feature template you wish to create.

11. Click **Device**.

12. Click the **Create Template** drop-down list and select **From Feature Template**.

13. From the **Device Model** drop-down list, select the type of device for which you wish to create the device template.

    vManage NMS displays the feature templates for the device type you selected. The required feature templates are indicated with an asterisk (*). The remaining templates are optional.

14. In the **Template Name** field, enter a name for the device template.

    This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.

15. In the **Description** field, enter a description for the device template.

    This field is mandatory, and it can contain any characters and spaces.

16. To view the factory-default configuration for a feature template, select the desired feature template and click **View Template**.

17. Click **Cancel** to return to the **Configuration Template** screen.

18. To use the factory-default configuration, click **Create** to create the device template. The new device template is displayed in the **Device Template** table. The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

19. To modify the factory-default configuration, select the feature template for which you do not wish to use the factory-default template. From the drop-down list of available feature templates, select a feature template that you created.

20. Repeat Step 19 for each factory-default feature template you wish to modify.

21. Click **Create**. The new configuration template is displayed in the **Device Template** table.

The Feature Templates column shows the number of feature templates that are included in the device template, and the Type column shows "Feature" to indicate that the device template was created from a collection of feature templates.

Create a Device CLI Template

To create a device template by entering a CLI text-style configuration directly on the Cisco vManage:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

   Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click the **Create Template** drop-down list and select **CLI Template**.
4. From the **Device** Type drop-down list, select the type of device for which you wish to create the template.
5. In the **Template Name** field, enter a name for the device template.

   This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

6. In the **Description** field, enter a description for the device template.

   This field is mandatory, and it can contain any characters and spaces.

7. In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.
8. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format {{*variable-name*}}; for example, {{hostname}}.
9. Click **Add**. The new device template is displayed in the Device Template table.

   The **Feature Templates** column shows the number of feature templates that are included in the device template, and the Type column shows "CLI" to indicate that the device template was created from CLI text.

Configure Disaster Recovery

Table 61: Feature History

Release Name	Release Information	Feature Description
Disaster Recovery for Cisco vManage	Cisco SD-WAN Release 19.2.1 Cisco vManage Release 19.2.1	This feature helps you configure Cisco vManage in an active or standby mode to counteract hardware or software failures that may occur due to unforeseen circumstances.
Disaster Recovery for a 6 Node Cisco vManage Cluster.	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature provides support for disaster recovery for a 6 node Cisco vManage cluster.
Disaster Recovery for a Single Node Cisco vManage Cluster	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature provides support for disaster recovery for a Cisco vManage deployment with a single primary node.
Disaster Recovery User Password Change	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	You can change the disaster recovery user password for disaster recovery components from the Cisco vManage **Disaster Recovery** window.

Out of the three controllers that make up the Cisco SD-WAN solution (Cisco vManage, Cisco vSmart Controller, and Cisco vBond Orchestrator), Cisco vManage is the only one that is stateful and cannot be deployed in an active/active mode. The goal of the disaster recovery solution is to deploy Cisco vManageCisco vManage across two data centers in primary/secondary mode.

The disaster recovery option provides automatic failover of the primary cluster to the secondary cluster. Data is replicated from the primary cluster to the secondary cluster.

There are two disaster recovery options. The option that you use depends on the function that you want the arbitrator to perform. An arbitrator is a Cisco vManage cluster that is hosted in a third data center and that monitors the connectivity and reachability of the Cisco vManage clusters that are hosted in data center 1 and data center 2. The arbitrator can detect a failure of the primary Cisco vManage cluster and issue a switchover command to the secondary Cisco vManage cluster so that the secondary cluster assumes the role of the primary cluster.

The disaster recovery options are:

- Manual—If you want to make the clusters active, you can do it manually rather than having the arbitrator do the switchover. You can specify the switchover threshold.
- Automated —Arbitrator does the monitoring of the cluster and performs the necessary action.

  A highly available Cisco SD-WAN network contains three or more Cisco vManage systems in each domain. This scenario is referred to as a Cisco vManage cluster, andCisco vManage system in a cluster is referred to as a Cisco vManage instance.

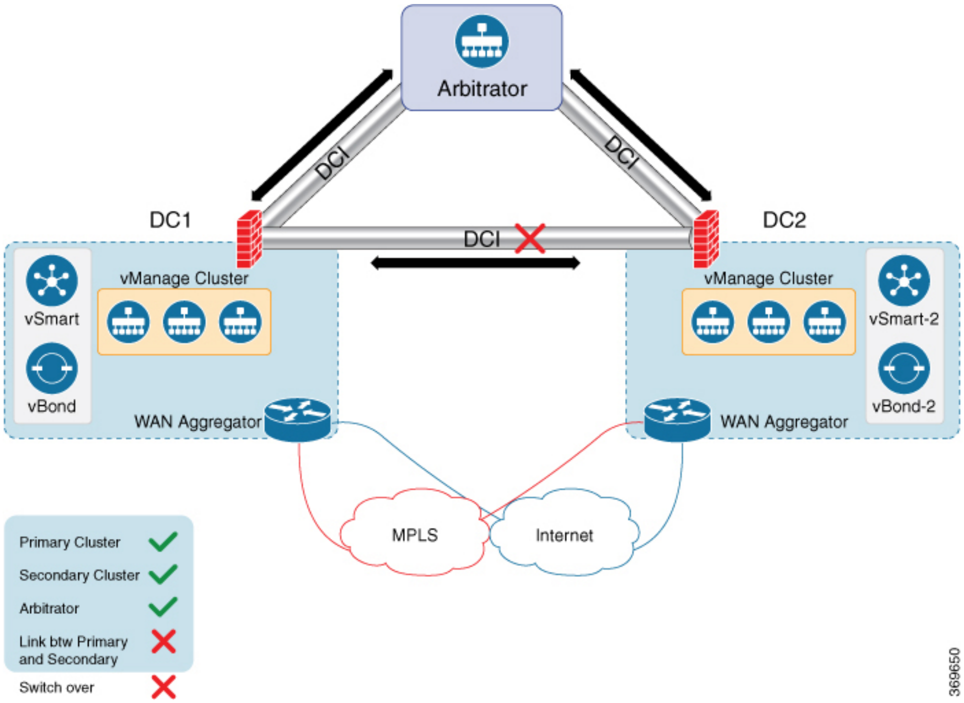
Disaster recovery is validated as follows:

- For releases earlier than Cisco IOS XE Release 17.4.1a and Cisco SD-WAN Release 20.4.1, disaster recovery is validated for a three-node cluster.
- In Cisco IOS XE Release 17.4.1a and Cisco SD-WAN Release 20.4.1, disaster recovery is validated for a six-node cluster.
- In Cisco IOS XE Release 17.5.1a and Cisco SD-WAN Release 20.5.1, disaster recovery is validated for a deployment with a single primary node.

Architecture Overview

The following diagram describes the high-level architecture of the disaster recovery solution.

The arbitrator is an additional Cisco vManage cluster that runs in arbitrator mode. The arbitrator monitors the health of the primary and the secondary clusters and performs the necessary actions.



Prerequisites

Before configuring disaster recovery, ensure that you have met the following requirements:

- For manual disaster recover configuration, ensure that you have two Cisco vManage clusters that contain the specific number of nodes as validated for your release. (The validated number of nodes for each release is described earlier in this section.)
- To configure the automated recovery option, ensure that you include an additional Cisco vManage node.
- Ensure that the primary and the secondary cluster are reachable by HTTPS on a transport VPN (VPN 0).

- Ensure that Cisco vSmart Controllers and Cisco vBond Orchestrators on the secondary cluster are connected to the primary cluster.
- Ensure that the nodes in the Cisco vManage primary cluster, the secondary cluster, and the arbitrator node are using the same Cisco vManage version.

Best Practices and Recommendations

- Ensure that you use a netadmin user privilege for Disaster Recovery registration. We recommend that you modify the factory-default password, admin before you start the registration process.
- To change user credentials, we recommend that you use the Cisco vManage GUI, and not use the CLI of a Cisco SD-WAN device.
- If Cisco vManage is configured using feature templates, ensure that you create separate feature templates for both the primary cluster and the secondary cluster. Create these templates in the primary cluster. After templates replicate to the secondary cluster, you can attach devices to templates in the secondary cluster.
- For an on-premises deployment, ensure that you regularly take backup of the Configuration database from the active Cisco vManage instance.

Changing the Cisco vManage or Cisco vBond Orchestrator Administrator Password

For releases earlier than Cisco SD-WAN Release 20.7.1, if you use Cisco vManage to change a user password that you entered during disaster recovery registration, first deregister disaster recovery from the Cisco vManage cluster, change the password, and then reregister disaster recovery on the cluster.

Changing the Disaster Recovery User Password for Disaster Recovery Components

During disaster recovery registration, you provide the user name and password of a Cisco vManage or a Cisco vBond Orchestrator user for the following disaster recovery components. You can provide the name and password of the same user for each of these components, or you can provide the names and passwords of different users for various components. The user names and passwords that you provide for a component identify the *disaster recovery user* who can access disaster recovery operations on the component.

- Cisco vManage servers in the active (primary) cluster. This component uses the password of a Cisco vManage user.
- Cisco vManage servers in the standby (secondary) cluster. This component uses the password of a Cisco vManage user.
- Arbitrator (applies only to automated disaster recovery). This component uses the password of a Cisco vManage user.
- Each Cisco vBond Orchestrator. This component uses the password of a Cisco vBond Orchestrator user.

If you change the Cisco vManage or Cisco vBond Orchestrator password of a disaster recovery user, you must change the disaster recovery component password for this user to the new password.

To change a password for the disaster recovery user, follow these steps:

1. From the Cisco vManage menu, choose **Administration** > **Disaster Recovery**.
2. Click **Pause Disaster Recovery**, and then click **OK** in the **Pause Disaster Recovery** dialog box that is displayed.

Data replication between the primary and secondary data centers stops and this option changes to **Resume Disaster Recovery**.

3. Click **Manage Password**.
4. In the **Manage Password** window, perform these actions:
    a. Click **Active Cluster**, and in the **Password** field that appears, enter the new active cluster password for the disaster recovery user.
    b. Click **Standby Cluster**, and in the **Password** field that appears, enter the new standby cluster password for the disaster recovery user.
    c. (For automatic disaster recovery only.) Click **Arbitrator**, and in the **Password** field that appears, enter the new active arbitrator password for the disaster recovery user.
    d. Click **vBond**, and in each **Password** field that appears, enter the new Cisco vBond Orchestrator password for the disaster recovery user. There is one **Password** field for each Cisco vBond Orchestrator.
    e. Click **Update**.

        The passwords are updated and the **Manage Password** window closes.
5. Click **Resume Disaster Recovery**, and then click **OK** in the **Resume Disaster Recovery** dialog box that is displayed.

    Data replication between the primary and secondary data centers restarts.

Enable Disaster Recovery on Day-0:

You need to bring up two separate clusters with no devices being shared, which means do not share any Cisco vSmart Controller, Cisco vBond Orchestrator, or Cisco vManage device.

On both clusters, configure the following:

Item	Action
Secondary cluster	Bring up the secondary Cisco vManage cluster with three Cisco vManage clusters.
Arbitrator	To assign an IP address for the OOB network, navigate to **Administration > Cluster Management**.
	Ensure reachability between the primary, secondary clusters, and arbitrator on VPN (0) using HTTPS.
	Ensure reachability between the primary cluster, secondary cluster, and Cisco vBond Orchestrators.

Verify after Registering for Disaster Recovery on Day-1

- Replication from the primary cluster to the secondary cluster happens at the configured intervals.
- Status check: **Administration > Disaster Recovery**.
- Arbitrator:

- First health check after 15 minutes. This check provides enough time for all the nodes to be up and running with the configured disaster recovery processes.
- Health check of the primary cluster, secondary cluster, and the arbitrator every five minutes.
- Check the */var/log/nms/vmanage-server.log* for the status information on the arbitrator cluster.

Configure Disaster Recovery

1. From the Cisco vManage menu, choose **Administration** > **Disaster Recovery**.
2. Click **Manage Disaster Recovery**.
3. To configure primary and secondary cluster, on the Cisco vManage Disaster Recovery screen, select an IP address for any Cisco vManage node within the respective cluster.

   If a cluster is behind a load balancer, specify the IP address of the load balancer.
4. Specify the following: **Start Time**, **Replication Interval**, and **Delay Threshold** for replicating data from the primary to the secondary cluster.

   The default value for **Delay Threshold** is 30 minutes.

   The default value for **Replication Interval** is 15 minutes.
5. From the Cisco vManage menu, choose **Administration** > **Disaster Recovery**, and for Cluster 2 (Secondary), click **Make Primary**.

   It can take 10 to 15 minutes to push all changes from all the devices.
6. You can also decide to pause disaster recovery, pause replication, or delete your disaster recovery configuration.

   After disaster recovery is configured and you have replicated data, you can view the following:

   - when your data was last replicated, how long it took to replicate, and the size of the data that was replicated.
   - when the primary cluster was switched over to the secondary cluster and the reason for the switchover.
   - the replication schedule and the delay threshold.

Disaster Recovery Striking the Primary Data Center

- Switchover happens only when all the nodes in the primary data center are lost.
- The arbitrator detects the loss of all the primary data center members and initiates switchover to the secondary data center.
- Secondary data center updates the Cisco vBond Orchestrator:
  - Invalidates old Cisco vManage systems.
  - New Cisco vManage systems from the secondary data center are updated, as valid.
  - Routers reach the Cisco vBond Orchestrator after losing control connections.
  - Routers start forming control connections with the new valid Cisco vManage systems.

Troubleshooting Tips

If disaster recovery registration fails, verify the following:

- Reachability to the Cisco vBond Orchestrator from all cluster members on the secondary cluster.
- Reachability between the secondary cluster, primary cluster, and the arbitrator on the transport interface (VPN 0).
- Check that you have the correct username and password.

If disaster recovery registration fails due to arbitrator reachability, check the following:

- You must configure the arbitrator in cluster mode. From the Cisco vManage menu, choose **Administration** > **Cluster Management**, and add a Cisco vManage system as the arbitrator.
- If the IP address is not assigned to the correct arbitrator, log on to the arbitrator cluster and do the following:
  - From the Cisco vManage menu, choose **Administration** > **Cluster Management**.
  - Edit the Cisco vManage system.
  - Choose the correct IP address from the drop-down list and save the configuration.

  The disaster recovery consul process uses this IP address for disaster recovery communication. This is set once you configure the Cisco vManage system in cluster mode.

Configure GPS Using Cisco vManage

Use the GPS template for all Cisco cellular routers running Cisco SD-WAN software.

For Cisco devices running Cisco SD-WAN software, you can configure the GPS and National Marine Electronics Association (NMEA) streaming. You enable both these features to allow 4G LTE routers to obtain GPS coordinates.

Note You can configure GPS using Cisco vManage starting from the Cisco vManage Release 20.6.1 and onwards.

You can configure GPS using a Cisco vManage feature template. For geofencing to work, you need to configure GPS. To configure a GPS feature template, navigate to **Configuration** > **Templates** > **Feature Templates** > **GPS**.

In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

For more information on geofencing, see Configure Geofencing.

Navigate to the Template Screen and Name the Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **Create Template**.
4. From the **Create Template** drop-down list, choose **From Feature Template**.
5. From the **Device Model** drop-down list, choose the type of device for which you wish to create the template.
6. Click **Cellular**.
7. In **Additional Cellular Controller Templates**, click **GPS**.
8. To create a custom template for GPS, click the **GPS** drop-down list and then click **Create Template**. The GPS template form is displayed. This form contains fields for naming the template, and fields for defining the GPS parameters.
9. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
10. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to **Default** (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down list to the left of the parameter field and select either **Device Specific** or **Global**.

Configure GPS

To configure GPS parameters for the cellular router, configure the following parameters. Parameters marked with an asterisk are required to configure the GPS feature.

Table 62:

Parameter Name	Description
GPS	Click **On** to enable the GPS feature on the router.
GPS Mode	Select the GPS mode: • **MS-based**—Use mobile station–based assistance, also called assisted GPS mode, when determining position. In this mode, a network data session is used to obtain the GPS satellite locations, resulting in a faster fix of location coordinates. • **Standalone**—Use satellite information when determining position. **Note** Standalone mode is currently not supported for geofencing.
NMEA	Click **On** to enable the use of NMEA streams to help in determining position. NMEA streams data from the router's 4G LTE Pluggable Interface Module (PIM) to any device, such as a Windows-based PC, that is running a commercially available GPS-based application.

Parameter Name	Description
Source Address	(Optional) Enter the IP address of the interface that connects to the router's PIM. **Note** This option is not used for configuring geofencing.
Destination Address	(Optional) Enter the IP address of the NMEA server. The NMEA server can be local or remote. **Note** This option is not used for configuring geofencing.
Destination Port	(Optional) Enter the number of the port to use to send NMEA data to the server. **Note** This option is not used for configuring geofencing.

To save the feature template, click **Save**.

Configure Groups of Interest for Centralized Policy

In **Create Groups of Interest**, create new groups of list types as described in the following sections to use in a centralized policy:

Configure Application

1. In the groups of interest list, click **Application** list type.
2. Click **New Application List**.
3. Enter a name for the list.
4. Choose either **Application** or **Application Family**.

   Application can be the names of one or more applications, such as **Third Party Control**, **ABC News**, **Mircosoft Teams**, and so on. The Cisco vEdge devices support about 2300 different applications. To list the supported applications, use the **?** in the CLI.

   Application Family can be one or more of the following: **antivirus**, **application-service**, **audio_video**, **authentication**, **behavioral**, **compression**, **database**, **encrypted**, **erp**, **file-server**, **file-transfer**, **forum**, **game**, **instant-messaging**, **mail**, **microsoft-office**, **middleware**, **network-management**, **network-service**, **peer-to-peer**, **printer**, **routing**, **security-service**, **standard**, **telephony**, **terminal**, **thin-client**, **tunneling**, **wap**, **web**, and **webmail**.
5. In the **Select** drop-down, in the 'Search' filter, select the required applications or application families.
6. Click **Add**.

A few application lists are preconfigured. You cannot edit or delete these lists.

Microsoft_Apps—Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the Entries column.

Google_Apps—Includes Google applications, such as gmail, Google maps, and YouTube. To display a full list of Google applications, click the list in the Entries column.

Configure Color

1. In the groups of interest list, click **Color**.
2. Click **New Color List**.
3. Enter a name for the list.
4. In the **Select Color** drop-down, in the 'Search' filter select the required colors.

   Colors can be: 3g, biz-internet, blue, bronze, custom1 through custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, and silver.
5. Click **Add**.

To configure multiple colors in a single list, you can select multiple colors from the drop-down.

Configure Community

Table 63: Feature History

Feature Name	Release Information	Description
Ability to Match and Set Communities	Cisco SD-WAN Release 20.5.1 Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	You can create groups of communities to use in a match clause of a route map in Cisco vManage.

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

1. In the group of interest list, click **Community**.
2. Click **New Community List**.
3. Enter a name for the community list.
4. Choose either **Standard** or **Expanded**.
   - Standard community lists are used to specify communities and community numbers.
   - Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to specify patterns to match community attributes.
5. In the **Add Community** field, enter one or more data prefixes separated by commas in any of the following formats:
   - *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535.
   - **internet**: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices.
   - **local-as**: Routes in this community are not advertised outside the local AS number.

- **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.
- **no-export**: Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.

6. Click **Add**.

Configure Data Prefix

1. In the **Groups of Interest** list, click **Data Prefix**.
2. Click **New Data Prefix List**.
3. Enter a name for the list.
4. Choose either **IPv4** or **IPv6**.
5. In the **Add Data Prefix** field, enter one or more data prefixes separated by commas.
6. Click **Add**.

Configure Policer

1. In the groups of interest list, click **Policer**.
2. Click **New Policer List**.
3. Enter a name for the list.
4. Define the policing parameters:
   a. In the **Burst** field, enter the maximum traffic burst size, a value from 15,000 to 10,000,000 bytes.
   b. In the **Exceed** field, select the action to take when the burst size or traffic rate is exceeded. It can be **drop**, which sets the packet loss priority (PLP) to **low**.

      You can use the **remark** action to set the packet loss priority (PLP) to **high**.
   c. In the **Rate** field, enter the maximum traffic rate, a value from 0 through $2^{64} - 1$ bits per second (bps).
5. Click **Add**.

Configure Prefix

1. In the groups of interest list, click **Prefix**.
2. Click **New Prefix List**.
3. Enter a name for the list.
4. In the **Add Prefix** field, enter one or more data prefixes separated by commas.
5. Click **Add**.

Configure Site

1. In the groups of interest list, click **Site**.
2. Click **New Site List**.
3. Enter a name for the list.
4. In the **Add Site** field, enter one or more site IDs separated by commas.

   For example, 100 or 200 separated by commas or in the range, 1- 4294967295.
5. Click **Add**.

Configure App Probe Class

1. In the groups of interest list, click **App Probe Class**.
2. Click **New App Probe Class**.
3. Enter the probe class name in the **Probe Class Name** field.
4. Select the required forwarding class from the **Forwarding Class** drop-down list.
5. In the **Entries** pane, select the appropriate color from the **Color** drop-down list and enter the **DSCP** value.

   You can add more entries if needed by clicking on the + symbol.
6. Click **Save**.

Configure SLA Class

1. In the groups of interest list, click **SLA Class**.
2. Click **New SLA Class List**.
3. Enter a name for the list.
4. Define the SLA class parameters:
   a. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.
   b. In the **Latency** field, enter the maximum packet latency on the connection, a value from 0 through 1,000 milliseconds.
   c. In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
   d. Select the required app probe class from the **App Probe Class** drop-down list.
5. (Optional) Select the **Fallback Best Tunnel** checkbox to enable the best tunnel criteria.

   This optional filed is available from Cisco SD-WAN Release 20.5.1 to pick the best path or color from the available colors when SLA is not met. When this option is selected, you can choose the required criteria from the drop-down. The criteria are a combination of one or more of loss, latency, and, jitter values.
6. Select the **Criteria** from the drop-down list. The available criteria are:

- Latency
- Loss
- Jitter
- Latency, Loss
- Latency, Jitter
- Loss, Latency
- Loss, Jitter
- Jitter, Latency
- Jitter, Loss
- Latency, Loss, Jitter
- Latency, Jitter, Loss
- Loss, Latency, Jitter
- Loss, Jitter, Latency
- Jitter, Latency, Loss
- Jitter, Loss, Latency

7. Enter the **Loss Variance (%)**, **Latency Variance (ms)**, and the **Jitter Variance (ms)** for the selected criteria.
8. Click **Add**.

Configure TLOC

1. In the groups of interest list, click **TLOC**.
2. Click **New TLOC List**. The **TLOC List** popup displays.
3. Enter a name for the list.
4. In the **TLOC IP** field, enter the system IP address for the TLOC.
5. In the **Color** field, select the TLOC's color.
6. In the **Encap** field, select the encapsulation type.
7. In the **Preference** field, optionally select a preference to associate with the TLOC.

   The range is 0 to 4294967295.
8. Click **Add TLOC** to add another TLOC to the list.
9. Click **Save**.

Note To use the `set tloc` and `set tloc-list` commands, you must use the set-vpn command.

For each TLOC, specify its address, color, and encapsulation. Optionally, set a preference value (from 0 to 232 – 1) to associate with the TLOC address. When you apply a TLOC list in an action accept condition, when multiple TLOCs are available and satisfy the match conditions, the TLOC with the highest preference value is used. If two or more of TLOCs have the highest preference value, traffic is sent among them in an ECMP fashion.

Configure VPN

1. In the groups of interest list, click **VPN**.
2. Click **New VPN List**.
3. Enter a name for the list.
4. In the **Add VPN** field, enter one or more VPN IDs separated by commas.

   For example, 100 or 200 separated by commas or in the range, 1- 65530.
5. Click **Add**.

Configure Region

Minimum release: Cisco vManage Release 20.7.1

To configure a list of regions for Multi-Region Fabric (formerly Hierarchical SD-WAN), ensure that Multi-Region Fabric is enabled in **Administration** > **Settings**.

1. In the groups of interest list, click **Region**.
2. Click **New Region List**.
3. In the **Region List Name** field, enter a name for the region list.
4. In the **Add Region** field, enter one or more regions, separated by commas, or enter a range.

   For example, specify regions 1, 3 with commas, or a range 1-4.
5. Click **Add**.

Click **Next** to move to **Configure Topology and VPN Membership** in the wizard.

Configure Groups of Interest for Localized Policy

In **Create Groups of Interest**, create lists of groups to use in a localized policy:

In Create Groups of Interest, create new groups of list types as described in the following sections to use in a localized policy:

Configure As Path

1. In the group of interest list, click **AS Path**.

2. Click **New AS Path List**.
3. Enter a name for the list.
4. Enter the AS path, separating AS numbers with a comma.
5. Click **Add**.

   AS Path list specifies one or more BGP AS paths. You can write each AS as a single number or as a regular expression. To specify more than one AS in a single path, include the list separated by commas. To configure multiple AS paths in a single list, include multiple **as-path** options, specifying one AS path in each option.

Configure Community

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

1. In the group of interest list, click **Community**.
2. Click **New Community List**.
3. Enter a name for the community list.
4. In the **Add Community** field, enter one or more data prefixes separated by commas in any of the following formats:
   - *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535.
   - **internet**: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices.
   - **local-as**: Routes in this community are not advertised outside the local AS number.
   - **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers.
   - **no-export**: Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.
5. Click **Add**.

Configure Data Prefix

1. In the **Group of Interest** list, click **Data Prefix**.
2. Click **New Data Prefix List**.
3. Enter a name for the list.
4. Enter one or more IP prefixes.
5. Click **Add**.

A data prefix list specifies one or more IP prefixes. You can specify both unicast and multicast addresses. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.

Configure Extended Community

1. In the group of interest list, click **Extended Community**.
2. Click **New Extended Community List**.
3. Enter a name for the list.
4. Enter the BGP extended community in the following formats:
   - **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address.
   - **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.
5. Click **Add**.

Configure Class Map

1. In the group of interest list, click **Class Map**.
2. Click **New Class List**.
3. Enter a name for the class.
4. Select a required queue from the **Queue** drop-down list.
5. Click **Save**.

Configure Mirror

1. In the group of interest list, click **Mirror**.
2. Click **New Mirror List**. The Mirror List popup displays.
3. Enter a name for the list.
4. In the **Remote Destination IP** field, enter the IP address of the destination for which to mirror the packets.
5. In the **Source IP** field, enter the IP address of the source of the packets to mirror.
6. Click **Add**.

   To configure mirroring parameters, define the remote destination to which to mirror the packets, and define the source of the packets. Mirroring applies to unicast traffic only. It does not apply to multicast traffic.

Configure Policer

1. In the group of interest list, click **Policer**.
2. Click **New Policer List**.
3. Enter a name for the list.
4. In the **Burst (bps)** field, enter maximum traffic burst size. It can be a value from 15000 to 10000000 bytes.
5. In the **Exceed** field, select the action to take when the burst size or traffic rate is exceeded. Select **Drop** (the default) to set the packet loss priority (PLP) to low. Select **Remark** to set the PLP to high.
6. In the **Rate (bps)** field, enter the maximum traffic rate. It can be value from 8 through 2^{64} bps (8 through 100000000000).
7. Click **Add**.

Configure Prefix

1. In the group of interest list, click **Prefix**.
2. Click **New Prefix List**.
3. Enter a name for the list.
4. In the **Internet Protocol** field, click either **IPv4** or **IPv6**.
5. Under **Add Prefix**, enter the prefix for the list. (An example is displayed.) Optionally, click the green **Import** link on the right-hand side to import a prefix list.
6. Click **Add**.

Click **Next** to move to **Configure Forwarding Classes/QoS** in the wizard.

Configure Lawful Intercept 2.0 Workflow

Table 64: Feature History

Feature Name	Release Information	Description
Lawful Intercept 2.0	Cisco vManage Release 20.9.1	This feature lets you configure a Lawful Intercept in Cisco vManage. Cisco vManage and Cisco vSmart Controller provides LEA with key information so that they can decrypt the Cisco SD-WAN IPsec traffic captured by the MSP.

Note The Lawful Intercept feature can be configured only through Cisco vManage, and not through the CLI.

To configure Lawful Intercept in Cisco vManage, perform the following steps:

1. Create Lawful Intercept Administrator
2. Create Lawful Intercept API User
3. Create an Intercept

Configure an NTP Parent

Table 65: Feature History

Feature Name	Release Information	Feature Description
Configure a Cisco vEdge Device as an NTP Parent and Optionally to Support NTP in Symmetric Active Mode.	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	Use the Cisco vManage device CLI template to configure a Cisco vEdge device as an NTP parent and configure the device to support NTP in symmetric active mode.

Starting with Cisco SD-WAN Release 20.4.1, you can configure a supported Cisco vEdge device as an NTP parent device by using the device CLI template. A device that is configured in this way acts as the NTP server to which other nodes in the deployment synchronize their clocks. You can configure multiple devices as NTP parents. The NTP server functionality is supported for IPv4, but not for IPv6.

You also can configure a device that is configured as an NTP parent device to support NTP in symmetric active mode. See "Configure Support for NTP in Symmetric Active Mode."

Use the following commands to configure device as an NTP parent device using a Cisco vEdge device device CLI template. For more information about configuring device CLI template, see "Create a Device CLI Template" in *Systems and Interfaces Configuration Guide*.

```
Device# config terminal
Device(config)# system
Device(config-system) ntp
Device(config-ntp)# parent
Device(config-parent)# enable
Device(config-parent)# source-interface loopback511
Device(config-parent)# stratum 6
Device(config-parent)# vpn 511
Device(config-parent)# exit
```

Restrictions and Limitations

- You can configure a device as an NTP parent only through a Cisco vManage CLI template. Cisco vManage feature templates do not support this configuration.
- The source interface must be in the same VPN that the vpn keyword defines.

Verify Configuration

Use the following show command to verify NTP parent configuration. The sample output shows that the server also is configured to support NTP in symmetric active mode.

```
Device# show running-config system ntp

system
 ntp
```

```
  keys
  authentication 101 md5 $8$vV6PtHeLdiEcLqDNLqV/mCWN5X92yT8PUPOwDCQgS4c=
  authentication 108 md5 $8$NTzFC6sRZiFUYeHw/pOY2dEoiO6dxphecDs7YnRKeuY=
  trusted 101 108
!
parent
 enable
 stratum 6
 source-interface loopback511
 vpn 511
exit
server 10.20.25.1
 source-interface ge0/1
 vpn 511
 version 4
exit
peer 172.16.10.100
 key 101
 vpn 511
 version 4
 source-interface ge0/1
exit
```

Configure On-Demand Tunnels Using Cisco vManage

Table 66: Feature History

Feature Name	Release Information	Description
Dynamic On-Demand Tunnels	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	You can configure on-demand tunnels between any two Cisco SD-WAN spoke devices. These tunnels are triggered to be set up only when there is traffic between the two devices.

Note

- See the Prerequisites for On-Demand Tunnels.
- Do not enable on-demand on the hub device.

On the spoke devices, enable on-demand at the system level on all VPN-0 transport interfaces. In the case of multi-homed sites, enable on-demand on all systems in the site.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.

4. Select a device.
5. From **Basic Information**, select **Cisco System**.
6. Click **Advanced**.
7. Enable **On-demand Tunnel**.
8. (optional) Configure the **On-demand Tunnel Idle Timeout** time. The default idle timeout value is 10 minutes. Range: 1 to 65535 minutes
9. Attach the System feature template to the device template for the spoke device.

Configure Password Policies Using Cisco vManage

Table 67: Feature History

Feature Name	Release Information	Description
Support for Password Policies using Cisco AAA	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	You can now configure password policies to ensure that your users use strong passwords and can be customized based on your requirements. To configure password policies, push the `password-policy` commands to your device using Cisco vManage device CLI templates. For more information on the `password-policy` commands, see the `aaa` command reference page.

Configure password policies for Cisco AAA by doing the following:

1. Navigate to **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **Create Template**.
4. Click **CLI Template**.
5. From the **Device Model** drop-down list, choose your Cisco vEdge device.
6. Enter a **Template Name**.
7. Enter a **Description**.
8. (Optional) From the **Load Running config from reachable device:** drop-down list, choose a device from which to load the running configuration.

9. Enter or append the password policy configuration.

   For more information on the `password-policy` commands, see the `aaa` command reference page.

10. Click **Add**.

    The device templates page appears.

11. Attach the templates to your devices as described in Attach a Device Template to Devices.

Configure Port Forwarding with NAT DIA

Table 68: Feature History

Feature Name	Release Information	Description
Support for Port Forwarding with NAT DIA	Cisco vManage Release 20.9.1	With this feature, you can define one or more port-forwarding rules to send packets received on a particular port from an external network to reach devices on an internal network.

Minimum supported releases: Cisco IOS XE Release 17.9.1a, Cisco vManage Release 20.9.1

Create port-forwarding rules to allow access to a private network from the public domain.

Before You Begin

1. Configure and apply a data policy.
2. Configure a **Cisco VPN Interface Ethernet** template or edit an existing **Cisco VPN Interface Ethernet** template.
3. Configure interface overload mode. Interface overload mode is enabled by default.
4. Configure a NAT pool.

Configure Port Forwarding with NAT DIA

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

> **Note** In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. To edit a **Cisco VPN Interface Ethernet** template, click **...** adjacent to the template name and choose **Edit**.
4. Click **NAT**.
5. Under **NAT Pool**, click **New NAT Pool**.

6. Enter the required NAT pool parameters.

   For more information on the NAT pool parameters, see Configure a NAT Pool and a Loopback Interface.

7. Click **Add**.

8. To create a port-forwarding rule, click **Port Forward** > **New Port Forwarding Rule** and configure the parameters as described in the table.

Table 69: Port-Forwarding Parameters for NAT DIA

Parameter Name	Description
Protocol	Choose the **TCP** or **UDP** protocol to which to apply the port-forwarding rule. To match the same ports for both TCP and UDP traffic, configure two rules.
Source IP Address	Enter the source IP address to be translated.
Source Port	Enter a port number to define the source port to be translated. Range is 0 to 65535.
Translated Source IP Address	Specify the NAT IP address that will be advertised into OMP. Port forwarding is applied to traffic that is destined to this IP address from the overlay with the translated port match.
Translate Port	Enter the port number to apply port forwarding to. Range is 0 to 65535. Beginning with Cisco IOS XE Release 17.5.1a, static translated source IP addresses must be within the configured dynamic NAT pool IP address range.
Static NAT Direction	Select the direction in which to perform network address translation.
Source VPN ID	Specify the service-side VPN from which the traffic is being sent.

9. Click **Update**.

Configure HTTP/HTTPS Proxy Server

Table 70: Feature History

Feature Name	Release Information	Description
HTTP/HTTPS Proxy Server for Cisco vManage Communication with External Servers	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	Cisco vManage uses HTTP/HTTPS to access some web services and for some REST API calls. With this feature, you can channel the HTTP/HTTPS communication through an HTTP/HTTPS proxy server.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. For the **HTTP/HTTPS Proxy** setting, click **Edit**.
3. For the **Enable HTTP/HTTPS Proxy** setting, click **Enabled**.
4. Enter the **HTTP/HTTPS Proxy IP Address** and **Port** number.
5. Click **Save**.

Note Cisco vManage uses TCP port 7 echo request to validate reachability of the proxy server. Ensure that you configure your firewall and proxy server to allow the echo requests to make the destination host ports accessible.

Cisco vManage verifies that the HTTP/HTTPS proxy server is reachable and saves the server details in the configuration database. HTTP/HTTPS connections and REST API calls to external servers are directed through the proxy server.

If the HTTP/HTTPS proxy server is not reachable, Cisco vManage displays an error message on the GUI indicating the reason for failure.

Configure Port Connectivity for Cloud OnRamp Colocation Cluster

Table 71: Feature History

Feature Name	Release Information	Description
Flexible Topologies	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1 Cisco NFVIS Release 4.2.1	You can configure the Stackwise Virtual Switch Link (SVL) and uplink ports of switches, and Cisco CSP data ports using the **Port Connectivity** configuration settings of Cloud OnRamp for Colocation cluster .
Support for SVL Port Configuration on 100G Interfaces	Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1 Cisco NFVIS Release 4.8.1	With this feature, you can configure SVL ports on 100-G Ethernet interfaces of Cisco Catalyst 9500-48Y4C switches, thus ensuring a high level of performance and throughput.

Prerequisites for Configuring SVL and Uplink Ports

- When configuring the SVL and uplink ports, ensure that the port numbers you configure on Cisco vManage match the physically cabled ports.
- Ensure that you assign serial numbers to both the switches. See Create and Activate Clusters.

Configure SVL and Uplink Ports

Note Before configuring the SVL and uplink ports using the **Cluster Topology** window, ensure that you create a Cloud OnRamp for Colocation cluster. See Create and Activate Clusters.

- On the **Cluster Topology** window, click **Add** next to **Port Connectivity**.

  In the **Port Connectivity** configuration window, both the configured switches appear. Hover over a switch port to view the port number and the port type.

Note For more information about SVL and uplink ports, see Wiring Requirements in the Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide.

Change Default SVL and Uplink Ports

Before you change the default port number and port type, note the following information about Cisco Catalyst 9500-40X and Cisco Catalyst 9500-48Y4C switches:

- From Cisco vManage Release 20.8.1, you can configure two SVL ports and one Dual-Active Detection (DAD) port when creating a colocation cluster with two Cisco Catalyst 9500-40X switches or two Cisco Catalyst 9500-48Y4C switches.
- To ensure that SVL and DAD ports are configured correctly for Cisco Catalyst 9500-48Y4C switches, note the following information:
  - Configure the SVL ports on same-speed interfaces, that is, either 25-G interfaces or 100-G interfaces. Ensure that both switches have the same configuration.
  - Configure the DAD port only on 25-G interfaces on both switches.
  - In case of an existing cluster, you can change the SVL ports only if it is inactive.
  - A cluster created in releases earlier than Cisco vManage Release 20.8.1 automatically displays two SVL ports and one DAD port after the upgrade to Cisco vManage Release 20.8.1.
- In case of Cisco Catalyst 9500-40X switches, you must configure the SVL and DAD ports on 10-G interfaces on both switches.
- The following are the default SVL, DAD, and uplink ports of Cisco Catalyst 9500 switches:

  Cisco Catalyst 9500-40X

  - SVL ports: Te1/0/38-Te1/0/39, and Te2/0/38-Te2/0/39

  In Cisco vManage Release 20.7.x and earlier releases, the default SVL ports are Te1/0/38-Te1/0/40 and Te2/0/38-Te2/0/40.

  - DAD ports: Te1/0/40 and Te2/0/40
  - Uplink ports: Te1/0/36, Te2/0/36 (input VLAN handoff), Te1/0/37, and Te2/0/37 (output VLAN handoff)

  Cisco Catalyst 9500-48Y4C

  - SVL ports: Hu1/0/49-Hu1/0/50 and Hu2/0/49-Hu2/0/50

    In Cisco vManage Release 20.7.x and earlier releases, the default SVL ports are Twe1/0/46-Twe1/0/48 and Twe2/0/46-Twe2/0/48.

  - DAD ports: Twe1/0/48 and Twe2/0/48
  - Uplink ports: Twe1/0/44, Twe2/0/44 (input VLAN handoff), Twe1/0/45, and Twe2/0/45 (output VLAN handoff) for 25-G throughput.

- I, E, and S represent the ingress, egress, and SVL ports, respectively.
- Ensure that the physical cabling is the same as the default configuration, and click **Save**.

To change the default ports when the connectivity is different for SVL and uplink ports, perform the following:

1. If both the switches are using the same ports:

   a. Click a port on a switch that corresponds to a physically connected port.

   b. To add the port configuration to the other switch, check the **Apply change** check box.

   If both the switches aren’t using the same ports:

   a. Click a port on **Switch1**.

   b. Choose a port type from the **Port Type** drop-down list.

   c. Click a port on **Switch2** and then choose the port type.

2. To add another port, repeat step 1.
3. Click **Save**.
4. To edit port connectivity information, in the **Cluster Topology** window, click **Edit** next to **Port Connectivity**.

Note You can modify the SVL and uplink ports of a cluster when the cluster hasn’t been activated.

5. To reset the ports to default settings, click **Reset**.

The remaining ports (SR-IOV and OVS) on the Cisco CSP devices and the connections with switches are automatically discovered using Link Layer Discovery Protocol (LLDP) when you activate a cluster. You don't need to configure those ports.

Cisco Colo Manager (CCM) discovers switch neighbor ports and identifies whether all Niantic and Fortville ports are connected. If any port isn't connected, CCM sends notifications to Cisco vManage that you can view in the task view window.

Configure SLA Class

Table 72: Feature History

Feature Name	Release Information	Description
Best of the Worst (BOW) Tunnel Selection	Cisco vManage Release 20.5.1 Cisco SD-WAN Release 20.5.1	You can configure best tunnel path to pick the best path while configuring SLA class.

1. From the Cisco vManage menu, select **Configuration** > **Policies**. Centralized Policy is selected and displayed by default.
2. Click **Add Policy**.
3. In the create groups of interest page, from the left pane, click **SLA Class**, and then click **New SLA Class List**.
4. In the **SLA Class List Name** field, enter a name for SLA class list.
5. Define the SLA class parameters:
   a. In the **Loss** field, enter the maximum packet loss on the connection, a value from 0 through 100 percent.
   b. In the **Latency** field, enter the maximum packet latency on the connection, a value from 1 through 1,000 milliseconds.
   c. In the **Jitter** field, enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
   d. Choose the required app probe class from the **App Probe Class** drop-down list.
6. (Optional) Check the **Fallback Best Tunnel** check box to enable the best tunnel criteria.

   This optional field is available from Cisco SD-WAN Release 20.5.1 to pick the best path or color from the available colors when a SLA is not met. When this option is selected, you can choose the required criteria from the drop-down. The criteria are a combination of one or more of loss, latency, and jitter values.
7. Select the **Criteria** from the drop-down. The available criteria are:
   - None
   - Latency
   - Loss
   - Jitter

- Latency, Loss
- Latency, Jitter
- Loss, Latency
- Loss, Jitter
- Jitter, Latency
- Jitter, Loss
- Latency, Loss, Jitter
- Latency, Jitter, Loss
- Loss, Latency, Jitter
- Loss, Jitter, Latency
- Jitter, Latency, Loss
- Jitter, Loss, Latency

8. (Optional) Enter the **Loss Variance (%)**, **Latency Variance (ms)**, and the **Jitter Variance (ms)** for the selected criteria.

   For more information, see Configure Variance for Best Tunnel Path.

9. Click **Add**.

Configure SNMPv3 on Cisco vEdge Devices Using Cisco vManage

Table 73: Feature History

Feature Name	Release Information	Description
Support for SNMPv3 AES-256 bit Authentication Protocol	Cisco vManage Release 20.5.1 Cisco SD-WAN Release 20.5.1	You can now configure SNMPv3 users with SHA-256 protocol and AES-256 bit encryption on Cisco vEdge devices.

To configure SNMPv3, in SNMP Version, navigate to template page and configure groups and trap information:

- From the Cisco vManage menu, choose **Configuration** > **Templates**.
- Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

- From the **Create Template** drop-down, select **From Feature Template**.
- From the **Device Model** drop-down, select the type of device for which you are creating the template.
- Click **Additional Templates**, which scrolls the page to **Additional Templates** section.
- From the **SNMP** drop-down under Additional Templates, click **Create Template**.

  The SNMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining SNMP parameters.
- In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
- In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.
- In **SNMP Version** section, click **V3**. For SNMPv3, you can configure groups, users, and trap information.
- In the Trap section, select **Trap Group** to configure trap. Then click **Add New Trap Group**, and configure the parameters as listed below:

Table 74: Trap Group Parameters for Cisco vEdge Devices

Parameter Name	Description
Group Name	Enter a name for the trap group. It can be from 1–32 characters long.
Trap Type Modules	Click **Add Trap Type Modules**, and configure the following parameters: In **Severity Levels**, select one or more severity levels for the trap. Supported security levels for the trap are critical, major, and minor. In **Module Name**, choose the type of traps to include in the trap group: • all: All trap types. • app-route: Traps generated by application-aware routing. • bfd: Traps generated by BFD and BFD sessions. • control: Traps generated by DTLS and TLS sessions. • dhcp: Traps generated by DHCP. • hardware: Traps generated by Viptela hardware. • omp: Traps generated by OMP. • routing: Traps generated by BGP, OSPF, and PIM. • security: Trap generated by certificates, vSmart and vEdge serial number files, and IPsec. • system: Traps generated by system-wide functions. • vpn: Traps generated by VPN-specific functions, including interfaces and VRRP.

To save the trap type module, click **Save**.

To configure SNMP views, in the **View & Groups** section, select **View**. Then click **New View**, and configure the following parameters:

Table 75: View and Groups Parameters

Parameter Name	Description
Name	Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 255 characters. You must add a view name for all views before adding a group.
Object Identifiers (OID)	Click **Add Object Identifiers** and configure the following parameters: • Object Identifier: Enter the OID of the object. For example, to view the Internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the Cisco SD-WAN MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name. **Note** Starting from Cisco vManage Release 20.6.1, SNMPv3 configuration of user with auth "sha-256" and priv "aes-256-cfb-128" does not support oid with (*) wildcard. • Exclude OID: Click **Off** to include the OID in the view or click **On** to exclude the OID from the view. To remove an OID from the list, click the **Delete** icon for the entry. To add the OIDs to the view list, click **Add**.

To configure the SNMP group, click **New Group**, and configure the following parameters:

Note It's mandatory to create an SNMP view before you proceed with SNMP group configuration.

Table 76: SNMP Group Parameters for Cisco vEdge Devices

Parameter Name	Description
Name	Enter the name for the group. The name can be from 1 through 32 characters and can include angle brackets (< and >).

Parameter Name	Description
Security Level	Choose the **Security Level** from the drop-down for the SNMPv3 security model: SNMPv3 is a security model in which an authentication strategy for a user and the group in which the user resides are set up. A security level is the permitted level of security within a security model. • noAuthNoPriv: Uses a username match for authentication. • authNoPriv: Provides authentication based on the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) algorithms. • authPriv: Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.
View	Choose the view from the drop-down to apply to the group. The view specifies the portion of the MIB tree the group can access.

To add the SNMP group, click **Add**.

In the User section, click **Add New User** and enter the following parameters to configure SNMPv3 users:

Table 77: SNMPv3 User Parameters

Parameter Name	Description
User	Enter a name of the SNMP user. It can be 1–32 alphanumeric characters.
Authentication Protocol	Choose the authentication mechanism for the user: • MD5 digest. • SHA-1 message digest. • SHA-256 message digest. **Note** Starting from Cisco SD-WAN Release 20.5.1, SHA-256 authentication protocol was introduced. When you choose SHA-256 as the authentication protocol, you must set the security level as `authPriv`. **Note** MD5 authentication protocol is deprecated for Cisco SD-WAN Release 20.3.2 and later releases.
Authentication Password	If you have the localized MD5 or SHA digest, you can specify the respective string as password. The digest is in the format aa:bb:cc:dd where aa, bb, cc, and dd are hexadecimal values. Also, the digest should be exactly 16 octets in length.

Parameter Name	Description
Privacy Protocol	Choose the privacy type for the user: • For SHA-1 authentication protocol choose AES-CFB-128—Advanced Encryption Standard cipher algorithm is used in cipher feedback mode, with a 128-bit key. • Starting from Cisco SD-WAN Release 20.5.1, for SHA-256 authentication protocol choose AES-256-CFB-128—Advanced Encryption Standard cipher algorithm is used in cipher feedback mode, with a 256-bit key. **Note** An authentication protocol SHA-1 is no longer supported and when a trap target is configured with SHA-1 for an SNMPv3 user, no SNMP trap is generated. You need to configure an SNMPv3 user with the SHA-256 authentication protocol.
Privacy Password	Enter the authentication password either in cleartext or as an AES-encrypted key.
Group	Choose the group name from the drop-down. All the configured SNMPv3 group names are listed in the drop-down.

To configure trap target servers, in the Trap section, select **Trap Target Server**. Then click **Add New Trap Group**, and configure the parameters as listed below:

Note It's mandatory to create User before creating Trap Target Server.

Table 78: Trap Target Server Parameters

Parameter Name	Description
VPN ID	Enter the number of the VPN to use to reach the trap server. *Range:* 0–65530.
IP Address	Enter the IP address of the SNMP server.
UDP Port	Enter the UDP port number for connecting to the SNMP server. *Range:* 1 though 65535.
User Name	Choose the name of the user from the drop-down.
Source Interface	Enter the interface used to send traps to the remote SNMP server.

To add the Trap Target Server, click **Add**.

To save the feature template, click **Save**.

Note The SNMP walk application is blocked if you switch the SNMPv3 configuration to SNMPv2 configuration in the device template and apply this change through a template push. This is because the **snmp mib community-map** command for SNMPv3 isn't removed during the configuration change. Hence, you cannot switch from SNMPv3 to SNMPv2 directly, when the SNMPv3 configuration template is active. To switch to SNMPv2, you must first remove the SNMPv3 configuration from the device and then push the SNMPv2 template through a separate commit.

Configure Traffic Rules

Table 79: Feature History

Feature Name	Release Information	Description
Policy Matching with ICMP Message	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	You can now define a new match condition that can be used to specify a list of ICMP messages for centralized data policies, localized data policies, and Application-Aware Routing policies.

When you first open the **Configure Traffic Rules** window, **Application-Aware Routing** is selected by default.

You can also view already created AAR routing policies listed in the page. It provides various information related to the policies such as the Name of the policy, Type, Mode, Description, Update By, and Last Updated details.

Note You can refer to the Mode column for the security status details of the policy. The status helps to differentiate whether the policy is used in unified security or not. The mode status is applicable only for security policies and not relevant to any centralized or localized policies.

For more information on configuring traffic rules for the SD-WAN Application Intelligence Engine (SAIE) flow, see SD-WAN Application Intelligence Engine Flow.

Note In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

To configure traffic rules for a centralized data policy:

1. Click **Traffic Data**.
2. Click the **Add Policy** drop-down.
3. Click **Create New**. The **Add Data Policy** window displays.
4. Enter a name and a description for the data policy.

5. In the right pane, click **Sequence Type**. The **Add Data Policy** popup opens.

6. Select the type of data policy you want to create, **Application Firewall**, **QoS**, **Service Chaining**, **Traffic Engineering**, or **Custom**.

Note If you want to configure multiple types of data policies for the same match condition, you need to configure a custom policy.

7. A policy sequence containing the text string **Application**, **Firewall**, **QoS**, **Service Chaining**, **Traffic Engineering**, or **Custom** is added in the left pane.

8. Double-click the text string, and enter a name for the policy sequence. The name you type is displayed both in the Sequence Type list in the left pane and in the right pane.

9. In the right pane, click **Sequence Rule**. The **Match/Action** box opens, and **Match** is selected by default. The available policy match conditions are listed below the box.

Match Condition	Procedure
None (match all packets)	Do not specify any match conditions.
Applications /Application Family List	**a.** In the **Match** conditions, click **Applications/Application Family List**. **b.** In the drop-down, select the application family. **c.** To create an application list: **1.** Click **New Application List**. **2.** Enter a name for the list. **3.** Click **Application** to create a list of individual applications. Click **Application Family** to create a list of related applications. **4.** In the **Select Application** drop-down, select the desired applications or application families. **5.** Click **Save**.
Destination Data Prefix	**a.** In the **Match** conditions, click **Destination Data Prefix**. **b.** To match a list of destination prefixes, select the list from the drop-down. **c.** To match an individual destination prefix, enter the prefix in the **Destination: IP Prefix** field.
Destination Port	**a.** In the **Match** conditions, click **Destination Port**. **b.** In the **Destination Port** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Match Condition	Procedure
DNS Application List	Add an application list to enable split DNS. **a.** In the **Match** conditions, click **DNS Application List**. **b.** In the drop-down, select the application family.
DNS	Add an application list to process split DNS. **a.** In the **Match** conditions, click **DNS**. **b.** In the drop-down, select **Request** to process DNS requests for the DNS applications, and select **Response** to process DNS responses for the applications.
DSCP	**a.** In the **Match** conditions, click **DSCP**. **b.** In the **DSCP** field, type the DSCP value, a number from 0 through 63.
Packet Length	**a.** In the **Match** conditions, click **Packet Length**. **b.** In the **Packet Length** field, type the length, a value from 0 through 65535.
PLP	**a.** In the **Match** conditions, click **PLP** to set the **Packet Loss Priority**. **b.** In the **PLP** drop-down, select **Low** or **High**. To set the PLP to **High**, apply a policer that includes the **exceed remark** option.
Protocol	**a.** In the **Match** conditions, click **Protocol**. **b.** In the **Protocol** field, type the Internet Protocol number, a number from 0 through 255.
ICMP Message	To match ICMP messages, in the Protocol field, set the Internet Protocol Number to 1, or 58, or both. **Note** This field is available from , Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1.
Source Data Prefix	**a.** In the **Match** conditions, click **Source Data Prefix**. **b.** To match a list of source prefixes, select the list from the drop-down. **c.** To match an individual source prefix, enter the prefix in the **Source** field.
Source Port	**a.** In the **Match** conditions, click **Source Port**. **b.** In the **Source** field, enter the port number. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
TCP	**a.** In the **Match** conditions, click **TCP**. **b.** In the **TCP** field, **syn** is the only option available.

10. For QoS and Traffic Engineering data policies: From the **Protocol** drop-down list, select **IPv4** to apply the policy only to IPv4 address families, **IPv6** to apply the policy only to IPv6 address families, or **Both** to apply the policy to IPv4 and IPv6 address families.

11. To select one or more **Match** conditions, click its box and set the values as described.

Note Not all match conditions are available for all policy sequence types.

12. To select actions to take on matching data traffic, click the **Actions** box.

13. To drop matching traffic, click **Drop**. The available policy actions are listed in the right side.

14. To accept matching traffic, click **Accept**. The available policy actions are listed in the right side.

15. Set the policy action as described.

Note Not all actions are available for all match conditions.

Action Condition	Description	Procedure
Counter	Count matching data packets.	**a.** In the **Action** conditions, click **Counter**. **b.** In the **Counter Name** field, enter the name of the file in which to store packet counters.
DSCP	Assign a DSCP value to matching data packets.	**a.** In the **Action** conditions, click **DSCP**. **b.** In the **DSCP** field, type the DSCP value, a number from 0 through 63.
Forwarding Class	Assign a forwarding class to matching data packets.	**a.** In the **Match** conditions, click **Forwarding Class**. **b.** In the **Forwarding Class** field, type the class value, which can be up to 32 characters long.
Log	Place a sampled set of packets that match the SLA class rule into system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.	**a.** In the **Action** conditions, click **Log** to enable logging.
Policer	Apply a policer to matching data packets.	**a.** In the **Match** conditions, click **Policer**. **b.** In the **Policer** drop-down field, select the name of a policer.

Action Condition	Description	Procedure
Loss Correction	Apply loss correction to matching data packets. Forward Error Correction (FEC) recovers lost packets on a link by sending redundant data, enabling the receiver to correct errors without the need to request retransmission of data. FEC is supported only for IPSEC tunnels, it is not supported for GRE tunnels. • **FEC Adaptive** – Corresponding packets are subjected to FEC only if the tunnels that they go through have been deemed unreliable based on measured loss. Adaptive FEC starts to work at 2% packet loss; this value is hard-coded and is not configurable. • **FEC Always** – Corresponding packets are always subjected to FEC. • **Packet Duplication** – Sends duplicate packets over a single tunnel. If more than one tunnel is available, duplicated packets will be sent over the tunnel with the best parameters.	**a.** In the **Match** conditions, click **Loss Correction**. **b.** In the **Loss Correction** field, select **FEC Adaptive**, **FEC Always**, or **Packet Duplication**.
Click **Save Match and Actions**.		

16. Create additional sequence rules as desired. Drag and drop to re-arrange them.
17. Click **Save Data Policy**.
18. Click **Next** to move to **Apply Policies to Sites and VPNs** in the wizard.

Match Parameters - Data Policy

A centralized data policy can match IP prefixes and fields in the IP headers, as well as applications. You can also enable split DNS.

Each sequence in a policy can contain one match condition.

Table 80:

Match Condition	Description
Omit	Match all packets.
Applications/Application Family List	Applications or application families.
Destination Data Prefix	Group of destination prefixes, IP prefix and prefix length. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).

Match Condition	Description
Destination Region	Choose one of the following: • **Primary**: Match traffic if the destination device is in the same primary region (also called access region) as the source. This traffic reaches the destination using a multi-hop path, through the core region. • **Secondary**: Match traffic if the destination device is not in the same primary region as the source but is within the same secondary region as the source. This traffic can reach the destination using a direct tunnel, as described for secondary regions. • **Other**: Match traffic if the destination device is not in the same primary region or secondary region as the source. This traffic requires a multi-hop path from the source to the destination. **Note** Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Release 17.9.1a
DNS Application List	Enables split DNS, to resolve and process DNS requests and responses on an application-by-application basis. Name of an **app-list** list . This list specifies the applications whose DNS requests are processed.
DNS	Specify the direction in which to process DNS packets. To process DNS requests sent by the applications (for outbound DNS queries), specify **dns request**. To process DNS responses returned from DNS servers to the applications, specify **dns response**.
DSCP	Specifies the DSCP value.
Packet length	Specifies the packet length. The range is 0 through 65535; specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).
Packet Loss Priority (PLP)	Specifies the packet loss priority. By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Protocol	Specifies Internet protocol number. The range is 0 through 255.
ICMP Message	For Protocol IPv4 when you enter a Protocol value as 1, the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. Likewise, the **ICMP Message** field displays for Protocol IPv6 when you enter a Protocol value as 58. When you select Protocol as Both, the **ICMP Message or ICMPv6 Message** field displays. **Note** This field is available from , Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1.
Source Data Prefix	Specifies the group of source prefixes or an individual source prefix.
Source Port	Specifies the source port number. The range is 0 through 65535; specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
TCP Flag	Specifies the TCP flag, syn.
Traffic To	In a Multi-Region Fabric architecture, match border router traffic flowing to the access region that the border router is serving, the core region, or a service VPN. **Note** Minimum release: Cisco vManage Release 20.8.1

Table 81: ICMP Message Types/Codes and Corresponding Enumeration Values

Type	Code	Enumeration
0	0	echo-reply
3		unreachable
	0	net-unreachable
	1	host-unreachable
	2	protocol-unreachable
	3	port-unreachable
	4	packet-too-big
	5	source-route-failed
	6	network-unknown
	7	host-unknown
	8	host-isolated
	9	dod-net-prohibited
	10	dod-host-prohibited
	11	net-tos-unreachable
	12	host-tos-unreachable
	13	administratively-prohibited
	14	host-precedence-unreachable
	15	precedence-unreachable
5		redirect
	0	net-redirect
	1	host-redirect
	2	net-tos-redirect
	3	host-tos-redirect
8	0	echo
9	0	router-advertisement
10	0	router-solicitation
11		time-exceeded
	0	ttl-exceeded
	1	reassembly-timeout

12		parameter-problem
	0	general-parameter-problem
	1	option-missing
	2	no-room-for-option
13	0	timestamp-request
14	0	timestamp-reply
40	0	photuris
42	0	extended-echo
43		extended-echo-reply
	0	echo-reply-no-error
	1	malformed-query
	2	interface-error
	3	table-entry-error
	4	multiple-interface-match

Table 82: ICMPv6 Message Types/Codes and Corresponding Enumeration Values

Type	Code	Enumeration
1		unreachable
	0	no-route
	1	no-admin
	2	beyond-scope
	3	destination-unreachable
	4	port-unreachable
	5	source-policy
	6	reject-route
	7	source-route-header
2	0	packet-too-big
3		time-exceeded
	0	hop-limit
	1	reassembly-timeout

4		parameter-problem
	0	Header
	1	next-header
	2	parameter-option
128	0	echo-request
129	0	echo-reply
130	0	mld-query
131	0	mld-report
132	0	mld-reduction
133	0	router-solicitation
134	0	router-advertisement
135	0	nd-ns
136	0	nd-na
137	0	redirect
138		router-renumbering
	0	renum-command
	1	renum-result
	255	renum-seq-number
139		ni-query
	0	ni-query-v6-address
	1	ni-query-name
	2	ni-query-v4-address
140		ni-response
	0	ni-response-success
	1	ni-response-refuse
	2	ni-response-qtype-unknown
141	0	ind-solicitation
142	0	ind-advertisement
143		mldv2-report
144	0	dhaad-request
145	0	dhaad-reply
146	0	mpd-solicitation
147	0	mpd-advertisement

148	0	cp-solicitation
149	0	cp-advertisement
151	0	mr-advertisement
152	0	mr-solicitation
153	0	mr-termination
155	0	rpl-control

Match Parameters

Access List Parameters

Access lists can match IP prefixes and fields in the IP headers.

In the CLI, you configure the match parameters with the **policy access-list sequence match** command.

Each sequence in an access-list must contain one match condition.

For access lists, you can match these parameters:

Match Condition	Description
Class	Name of a class defined with a **policy class-map** command.
Destination Data Prefix	Name of a data-prefix-list list.
Destination Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
DSCP	Specifies the DSCP value. The range is 0 through 63.
Protocol	Specifies the internet protocol number. The range is 0 through 255.
ICMP Message	When you select a Protocol value as 1 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. When you select a Next Header value as 58 the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. **Note** This field is available from , Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1.
Packet Length	Specifies the length of the packet. The range can be from 0 through 65535. Specify a single length, a list of lengths (with numbers separated by a space), or a range of lengths (with the two numbers separated with a hyphen [-]).
Source Data Prefix	Specifies the name of a **data-prefix-list** list.
PLP	Specifies the Packet Loss Priority (PLP) (**high** | **low**). By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.

Match Condition	Description
Source Port	Specifies a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]). The range is 0 through 65535.
TCP	**syn**

Route Policy Parameters

For route policies, you can match these parameters:

Match Condition	Description
Address	Specifies the name of a **Prefix-List** list.
AS Path List	Specifies one or more BGP AS path lists. You can write each AS as a single number or as a regular expression. To specify more than one AS number in a single path, include the list in quotation marks (" "). To configure multiple AS numbers in a single list, include multiple **AS Path** options, specifying one AS path in each option.
Community List	List of one of more BGP communities. In **Community List**, you can specify: • *aa*:*nn*: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the Internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.
Extended Community List	Specifies the list of one or more BGP extended communities. In **community**, you can specify: • **rt** (*aa*:*nn* | *ip-address*): Route target community, which is one or more routers that can receive a set of routes carried by BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. • **soo** (*aa*:*nn* | *ip-address*): Route origin community, which is one or more routers that can inject a set of routes into BGP. Specify this as the AS number and network number, where each number is a 2-byte value with a range from 1 to 65535, or as an IP address. To configure multiple extended BGP communities in a single list, include multiple **community** options, specifying one community in each option.
BGP Local Preference	Specifies the BGP local preference number. The range is 0 through 4294967295.
Metric	Specifies the route metric value. The range is 0 through 4294967295.

Match Condition	Description
Next Hop	Specifies the name of an IP prefix list.
OMP Tag	Specifies the OMP tag number. The range is 0 through 4294967295.
Origin	Specifies the BGP origin code. The optionss are: EGP (default), IGP, Incomplete.
OSPF Tag	Specifies the OSPF tag number. The range is 0 through 4294967295.
Peer	Specifies the peer IP address.

Structural Components of Policy Configuration for Application-Aware Routing

Here are the structural components required to configure application-aware routing policy. Each one is explained in more detail in the sections below.

```
policy
  lists
    app-list list-name
      (app application-name | app-family application-family)
    prefix-list list-name
      ip-prefix prefix
    site-list list-name
      site-id site-id
    vpn-list list-name
      vpn-id vpn-id
 log-frequency number
 sla-class sla-class-name
   jitter milliseconds
   latency milliseconds
   loss percentage
 app-route-policy policy-name
   vpn-list list-name
     sequence number
       match
         match-parameters
       action
         backup-sla-preferred-color colors
         count counter-name
         log
         sla-class sla-class-name [strict] [preferred-color colors]
     default-action
       sla-class sla-class-name
apply-policy site-list list-name
  app-route-policy policy-name
```

Lists

Application-aware routing policy uses the following types of lists to group related items. You configure these lists under the **policy lists** command hierarchy on Cisco vSmart Controllers.

Table 83:

List Type	Description	Command

Applications and application families	List of one or more applications or application families running on the subnets connected to the Cisco SD-WANdevice. Each **app-list** can contain either applications or application families, but you cannot mix the two. To configure multiple applications or application families in a single list, include multiple **app** or **app-family** options, specifying one application or application family in each **app** or **app-family** option.
	• *application-name* is the name of an application. The Cisco SD-WAN device supports about 2300 different applications.
	• *application-family* is the name of an application family. It can one of the following: **antivirus**, **application-service**, **audio_video**, **authentication**, **behavioral**, **compression**, **database**, **encrypted**, **erp**, **file-server**, **file-transfer**, **forum**, **game**, **instant-messaging**, **mail**, **microsoft-office**, **middleware**, **network-management**, **network-service**, **peer-to-peer**, **printer**, **routing**, **security-service**, **standard**, **telephony**, **terminal**, **thin-client**, **tunneling**, **wap**, **web**, and **webmail**.
		`app-list list-name`
		`(app application-name |`
		`app-family application-family)`

Data prefixes	List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple **ip-prefix** options, specifying one prefix in each option.	`data-prefix-list list-name`
		`ip-prefix prefix/length`

List Type	Description	Command
Sites	List of one or more site identifiers in the overlay network. To configure multiple sites in a single list, include multiple **site-id** options, specifying one site number in each option. You can specify a single site identifier (such as **site-id 1**) or a range of site identifiers (such as **site-id 1-10**).	`site-list` *list-name* `  site-id` *site-id*
VPNs	List of one or more VPNs in the overlay network. To configure multiple VPNs in a single list, include multiple **vpn** options, specifying one VPN number in each option. You can specify a single VPN identifier (such as **vpn-id 1**) or a range of VPN identifiers (such as **vpn-id 1-10**).	`vpn-list` *list-name* `  vpn` *vpn-id*

In the Cisco vSmart Controller configuration, you can create multiple iterations of each type of list. For example, it is common to create multiple site lists and multiple VPN lists so that you can apply data policy to different sites and different customer VPNs across the network.

When you create multiple iterations of a type of list (for example, when you create multiple VPN lists), you can include the same values or overlapping values in more than one of these list. You can do this either on purpose, to meet the design needs of your network, or you can do this accidentally, which might occur when you use ranges to specify values. (You can use ranges to specify data prefixes, site identifiers, and VPNs.) Here are two examples of lists that are configured with ranges and that contain overlapping values:

- **vpn-list list-1 vpn 1-10**

  vpn-list list-2 vpn 6-8

- **site-list list-1 site 1-10**

  site-list list-2 site 5-15

When you configure data policies that contain lists with overlapping values, or when you apply data policies, you must ensure that the lists included in the policies, or included when applying the policies, do not contain overlapping values. To do this, you must manually audit your configurations. The Cisco SD-WAN configuration software performs no validation on the contents of lists, on the data policies themselves, or on how the policies are applied to ensure that there are no overlapping values.

If you configure or apply data policies that contain lists with overlapping values to the same site, one policy is applied and the others are ignored. Which policy is applied is a function of the internal behavior of Cisco SD-WAN device when it processes the configuration. This decision is not under user control, so the outcome is not predictable.

Logging Frequency

If you configure a logging action, by default, the Cisco SD-WAN device logs all data packet headers to a syslog file. To log only a sample of the data packet headers:

```
vEdge(config)# policy log-frequency number
```

number specifies how often to to log packet headers. For example, if you configure **log-frequency 20**, every sixteenth packet is logged. While you can configure any integer value for the frequency, the software rounds the value down to the nearest power of 2.

SLA Classes

An SLA (service-level agreement) determines the action taken in application-aware routing. An SLA class defines the maximum jitter, maximum latency, maximum packet loss, or a combination of these values for the Cisco SD-WAN device's data plane tunnels. (Each tunnel is defined by a local TLOC–remote TLOC pair.) You configure SLA classes under the **policy sla-class** command hierarchy onCisco vSmart Controllers. In Cisco SD-WAN Release 20.1.x and onwards, you can configure a maximum of eight SLA classes. However, only 4 unique SLA classes can be defined in an application aware route policy. In older releases, you can configure a maximum of four SLA classes.

Note In Cisco SD-WAN Release 20.3.1, you cannot configure more than four different SLA classes on Cisco SD-WAN devices. The application-aware routing policy is rejected, if you configure more than four different SLA classes.

You can configure the following parameters in an SLA class:

Table 84:

Description	Command	Value or Range
Maximum acceptable packet jitter on the data plane tunnel	**jitter** *milliseconds*	1 through 1000 milliseconds
Maximum acceptable packet latency on the data plane tunnel.	**latency** *milliseconds*	1 through 1000 milliseconds
Maximum acceptable packet loss on the data plane tunnel.	**loss** *percentage*	0 through 100 percent

VPN Lists

Each application-aware policy instance is associated with a VPN list. You configure VPN lists with the **policy app-route-policy vpn-list** command. The VPN list you specify must be one that you created with a **policy lists vpn-list** command.

Sequences

Within each VPN list, an application-aware policy contains sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy. You configure sequences with the **policy app-aware-policy vpn-list sequence** command.

Each sequence in an application-aware policy can contain one **match** command and one **action** command.

Match Parameters

Application-aware routing policy can match IP prefixes and fields in the IP headers. You configure the match parameters with the **match** command under the **policy app-route-policy vpn-list sequence** command hierarchy on Cisco vSmart Controllers.

You can match these parameters:

Table 85:

Description	Command	Value or Range
Match all packets	Omit **match** command	—
Applications or application families	**app-list** *list-name*	Name of an **app-list** list
Group of destination prefixes	**destination-data-prefix-list** *list-name*	Name of a **data-prefix-list** list
Individual destination prefix	**destination-ip** *prefix/length*	IP prefix and prefix length
Destination port number	**destination-port** *number*	0 through 65535. Specify a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-]).
DSCP value	**dscp** *number*	0 through 63
Internet Protocol number	**protocol** *number*	0 through 255
For Protocol IPv4 when you enter a Protocol value as 1, the **ICMP Message** field displays where you can select an ICMP message to apply to the data policy. Likewise, the **ICMP Message** field displays for Protocol IPv6 when you you enter a Protocol value as 58. When you select Protocol as Both, the **ICMP Message or ICMPv6 Message** field displays. **Note** This field is available from , Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1.	**icmp-msg** *value* **icmp6-msg** *value*	For **`icmp-msg`** and **`icmp6-msg`** message types, refer to the ICMP Message Types/Codes and Corresponding Enumeration Values table.

Description	Command	Value or Range
Packet loss priority (PLP)	**plp**	(**high** | **low**) By default, packets have a PLP value of **low**. To set the PLP value to **high**, apply a policer that includes the **exceed remark** option.
Group of source prefixes	**source-data-prefix-list** *list-name*	Name of a **data-prefix-list** list
Individual source prefix	**source-ip** *prefix*/*length*	IP prefix and prefix length
Source port number	**source-port** *number*	0 through 65535; enter a single port number, a list of port numbers (with numbers separated by a space), or a range of port numbers (with the two numbers separated with a hyphen [-])
Split DNS, to resolve and process DNS requests on an application-by-application basis	**dns-app-list** *list-name* **dns** (**request** | **response**)	Name of an **app-list** list. This list specifies the applications whose DNS requests are processed. To process DNS requests sent by the applications (for outbound DNS queries), specify **dns request**. To process DNS responses returned from DNS servers to the applications, specify **dns response**.

Action Parameters

When data traffic matches the match parameters, the specified action is applied to it. For application-aware routing policy, the action is to apply an SLA class. The SLA class defines the maximum packet latency or maximum packet loss, or both, that the application allows on the data plane tunnel used to transmit its data. TheCisco SD-WAN software examines the recently measured performance characteristics of the data plane tunnels and directs the data traffic to the WAN connection that meets the specified SLA.

The following actions can be configured:

Table 86:

Description	Command	Value or Range
When no tunnel matches the SLA, direct the data traffic to a specific tunnel. Data traffic is sent out the configured tunnel if that tunnel interface is available. If that tunnel is unavailable, traffic is sent out another available tunnel. You can specify one or more colors. The backup SLA preferred color is a loose matching, not a strict matching.	**backup-sla-preferred-color** *colors*	**3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green lte**, **metro-ethernet**, **mpls**, **private1** through **private6**, **public-internet**, **red**, **silver**
Count matching data packets.	**action count** *counter-n ame*	Name of a counter.

Description	Command	Value or Range
Place a sampled set of packets that match the SLA class rule into the messages and vsyslog system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.	**action log**	To display logging information, use the **show app log flow-all**, **show app log flows**, and **show log** commands on the Cisco vEdge device.
SLA class to match. All matching data traffic is directed to a tunnel whose performance matches the SLA parameters defined in the class. The software first tries to send the traffic through a tunnel that matches the SLA. If a single tunnel matches the SLA, data traffic is sent through that tunnel. If two or more tunnels match, traffic is distributed among them. If no tunnel matches the SLA, data traffic is sent through one of the available tunnels.	**action sla-class** *sla-class-name*	SLA class name defined in **policy sla-class** command
Group of data plane tunnel colors to prefer when an SLA class match occurs. Traffic is load-balanced across all tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. That is, color preference is a loose matching, not a strict matching.	**action sla-class** *sla-class-name* **preferred-color** *colors*	SLA class name defined in **policy sla-class** command and one of the supported tunnel colors.
Strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Note that for policy configured with this option, data traffic that matches the match conditions is dropped until the application-aware routing path is established.	**action sla-class** *sla-class-name* **strict** **action sla-class** *sla-class-name* **preferred-color** *color* **strict** **action sla-class** *sla-class-name* **preferred-color** *colors* **strict**	SLA class name defined in **policy sla-class** command

If more than one data plane tunnel satisfies an SLA class criteria, the Cisco SD-WAN device selects one of them by performing load-balancing across the equal paths.

Default Action

A policy's default action defines how to handle packets that match none of the match conditions. For application-aware routing policy, if you do not configure a default action, all data packets are accepted and transmitted based on normal routing decisions, with no consideration of SLA.

To modify this behavior, include the **default-action sla-class** *sla-class-name* command in the policy, specifying the name of an SLA class you defined in the **policy sla-class** command.

When you apply an SLA class in a policy's default action, you cannot specify the **strict** option.

If no data plane tunnel satisfies the SLA class in the default action, the Cisco SD-WAN device selects one of the available tunnels by performing load-balancing across equal paths.

Expected behavior when data flow matches both AAR and data policies:

1. When data policy local TLOC action is configured, the **App-route preferred-color** and **backup-preferred-color** actions are ignored.
2. The **sla-class** and **sla-strict** actions are retained from the application routing configuration.
3. The data policy TLOC takes precedence.

When there is a **local-tloc-list** action that has multiple options, choose the local-TLOC that meets SLA.

- If no **local-tloc** meets SLA, then choose equal-cost multi-path routing (ECMP) for the traffic over the **local-tloc-list**.
- If none of the **local-tloc** is up, then choose a TLOC that is up.
- If none of the **local-tloc** is up and the DP is configured in restrict mode, then drop the traffic.

Configure Service Chaining

Table 87: Feature History

Feature Name	Release Information	Description
Service insertion tracker support	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	You can configure service chaining for a device from the **Service** tab.

Here is the workflow for configuring service chaining for a device managed by Cisco SD-WAN:

1. Service devices are accessed through a specific VRF. In the VPN template that corresponds to the VRF for a service device, configure service chaining, specifying the service type and device addresses. By default, the tracking feature adds each service device status update to the service log. You can disable this in the VPN template.
2. Attach the VPN template to the device template for the device managed by Cisco SD-WAN.
3. Apply the device template to the device.

Configure Service Chaining Using Cisco vManage

To configure service chaining for a device.

1. In Cisco vManage, create a VPN template.
2. ClickService.
3. In the **Service** section, click **New Service** and configure the following:
   - **Service Type**: Select the type of service that the service device is providing.
   - **IP Address**: IP Address is the only working option.
   - **IPv4 Address**: Enter between one and four addresses for the device.
   - **Tracking**: Determines whether the periodic health updates of the service device are recorded in the system log. Default: On

Note Maximum number of services: 8

4. Click **Add**. The service appears in the table of configured services.

Configure Sessions in Cisco vManage

Table 88: Feature History

Feature History	Release Information	Description
Configure Sessions in Cisco vManage	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	This feature lets you see all the HTTP sessions that are open within Cisco vManage. It gives you details about the username, source IP address, domain of the user, and other information. A user with User Management Write access, or a netadmin user can trigger a log out of any suspicious user's session.

Set a Client Session Timeout in Cisco vManage

You can set a client session timeout in Cisco vManage. When a timeout is set, such as no keyboard or keystroke activity, the client is automatically logged out of the system.

Note You can edit Client Session Timeout in a multitenant environment only if you have a Provider access.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Click **Client Session Timeout**.
3. Click **Edit**.

4. Click **Enabled**.
5. Specify the timeout value, in minutes.
6. Click **Save**.

Set a Session Lifetime in Cisco vManage

You can specify how long to keep your session active by setting the session lifetime, in minutes. A session lifetime indicates the amount of time for which a session can be active. If you keep a session active without letting the session expire, you will be logged out of the session in 24 hours, which is the default session timeout value.

The default session lifetime is 1440 minutes or 24 hours.

Note You can edit Session Lifetime in a multitenant environment only if you have a Provider access.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Click **Session Life Time**.
3. Click **Edit**.
4. In the **SessionLifeTime** field, specify the session timeout value, in minutes, from the drop-down list.
5. Click **Save**.

Set the Server Session Timeout in Cisco vManage

You can configure the server session timeout in Cisco vManage. The server session timeout indicates how long the server should keep a session running before it expires due to inactivity. The default server session timeout is 30 minutes.

Note Server Session Timeout is not available in a multitenant environment even if you have a Provider access or a Tenant access.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Click **Server Session Timeout**.
3. Click **Edit**.
4. In the **Timeout(minutes)** field, specify the timeout value, in minutes.
5. Click **Save**.

Enable Maximum Sessions Per User

You can enable the maximum number of concurrent HTTP sessions allowed per username. If you enter 2 as the value, you can only open two concurrent HTTP sessions. If you try to open a third HTTP session with the same username, the third session is granted access, and the oldest session is logged out.

Note Maximum Session Per User is not available in a multitenant environment even if you have a Provider access or a Tenant access.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Click **Max Sessions Per User**.
3. Click **Edit**.
4. Click **Enabled**.

   By default, **Max Sessions Per User**, is set to **Disabled**.
5. In the **Max Sessions Per User** field, specify a value for the maximum number of user sessions.
6. Click **Save**.

Single Sign-On Using Azure Active Directory (AD)

Table 89: Feature History

Feature Name	Release Information	Description
Single Sign-On Using Azure AD	Cisco vManage Release 20.8.1	Single Sign-On (SSO) with security assertion mark-up language (SAML) gives faster, easier, and trusted access to cloud applications without storing passwords or requiring you to log in to each application individually.

Configure TACACS Authentication for Cloud OnRamp Colocation Cluster

Table 90: Feature History

Feature Name	Release Information	Description
TACACS Authentication	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	You can configure the TACACS authentication for users using the **TACACS** configuration settings of Cloud OnRamp for Colocation cluster.

The TACACS authentication determines the valid users who can access the Cisco CSP and Cisco Catalyst 9500 devices after a cluster is active.

Points to consider

- By default, the admin users with Role-based access control (RBAC) are authorized to access the Cisco CSP and Cisco Catalyst 9500 devices.
- Do not configure the same user with different passwords when configuring using TACACS and RBAC. If same user with a different password is configured on TACACS and RBAC, the RBAC user and password authentication is used.

To authenticate users:

Note Before configuring the TACACS authentication for users using the **Cluster Topology** window, ensure that you create a Cloud OnRamp for Colocation cluster. See Create and Activate Clusters.

1. To add TACACS server configuration, on the **Cluster Topology** window, click **Other Settings** > **Add** next to **TACACS**.

   To edit TACACS server configuration, in the **Cluster Topology** window, click **Other Settings** > **Edit** next to **TACACS**.

   In the **TACACS** configuration window, enter information about the following:

   - Template Name—The TACACS template name can contain 128 alphanumeric characters.
   - (Optional) Description—The description can contain 2048 alphanumeric characters.

2. To add a new TACACS server, click **+ New TACACS SERVER**.

   - In **Server IP Address**, enter the IPv4 address.

     Use IPv4 addresses for hostnames of TACACS server.

   - In **Secret** enter the password and confirm the password in **Confirm Secret**.

3. Click **Add**

   The new TACACS server details are listed in the **TACACS** configuration window.

   Note You can add a maximum of four TACACS servers.

4. To add another TACACS server, repeat step 2 to step 3.

   When authenticating users, if the first TACACS server is not reachable, the next server is verified until all the four servers are verified.

5. Click **Save**.

6. To delete a TACACS server configuration, choose a row from the TACACS server details list and click **Delete** under **Action**.

Note To modify an existing TACACS server information, ensure to delete a TACACS server and then add a new server.

7. To view the TACACS server configuration, in Cisco vManage, click **Configuration** > **Devices**.

   For the desired Cisco CSP device or Cisco Catalyst 9500 switch, click **...** and choose **Running Configuration**.

Configure Cisco vBond Orchestrator

Once you have set up and started the virtual machine (VM) for Cisco vBond Orchestrator in your overlay network, Cisco vBond Orchestrator comes up with a factory-default configuration. You then need to manually configure few basic features and functions so that the devices can be authenticated and verified and can join the overlay network. Among these features, you configure the device as Cisco vBond Orchestrator providing the system IP address, and you configure a WAN interface that connects to the Internet. This interface must have a public IP address so that all Cisco vEdge devices in the overlay network can connect to Cisco vBond Orchestrator.

You create the initial configuration by using SSH to open a CLI session to Cisco vBond Orchestrator.

After you have created the initial configuration, you create the full configuration by creating configuration templates on Cisco vManage and then attach the templates to Cisco vBond Orchestrator. When you attach the configuration templates to Cisco vBond Orchestrator, the configuration parameters in the templates overwrite the initial configuration.

Create Initial Configuration for Cisco vBond Orchestrator

To create the initial configuration on Cisco vBond Orchestrator using a CLI session:

1. Open a CLI session to Cisco vEdge device via SSH.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

   ```
   vBond#config
   vBond(config)#
   ```

4. Configure the hostname:

   ```
   vBond(config)#system host-name hostname
   ```

   Configuring the hostname is optional, but is recommended because this name in included as part of the prompt in the CLI and it is used on various Cisco vManage screens to refer to the device.

5. Configure the system IP address:

   ```
   vBond(config-system)#system-ip ip-address
   ```

   Cisco vManage uses the system IP address to identify the device so that the NMS can download the full configuration to the device.

6. Configure the IP address of Cisco vBond Orchestrator. Cisco vBond Orchestrator's IP address must be a public IP address, to allow all Cisco vEdge devices in the overlay network to reach Cisco vBond Orchestrator:

   ```
   vBond(config-system)#vbond ip-address local
   ```

   In Releases 16.3 and later, the address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. A vBond orchestrator is effectively a vEdge router that performs only the orchestrator functions. The **local** option designates the device to be Cisco vBond Orchestrator, not a vEdge router. Cisco vBond Orchestrator must run on a standalone virtual machine (VM) or hardware router; it cannot coexist in the same device as a software or hardware vEdge router.

7. Configure a time limit for confirming that a software upgrade is successful:

   ```
   vBond(config-system)#upgrade-confirm minutes
   ```

   The time can be from 1 through 60 minutes. If you configure this time limit, when you upgrade the software on the device, Cisco vManage (when it comes up) or you must confirm that a software upgrade is successful within the configured number of minutes. If the device does not received the confirmation within the configured time, it reverts to the previous software image.

8. Change the password for the user "admin":

   ```
   vBond(config-system)#user admin password password
   ```

   The default password is "admin".

9. Configure an interface in VPN 0, to connect to the Internet or other WAN transport network. In Releases 16.3 and later, the IP address can be an IPv4 or an IPv6 address. In earlier releases, it must be an IPv4 address. Ensure that the prefix you configure for the interface contains the IP address that you configure in the **vbond local** command.

   ```
   vBond(config)#vpn 0 interface interface-name
   vBond(config-interface)#ip address ipv4-prefix/length
   vBond(config-interface)#ipv6 address ipv6-prefix/length
   vBond(config-interface)#no shutdown
   ```

Note The IP address must be a public address so that all devices in the overlay network can reach Cisco vBond Orchestrator.

10. Commit the configuration:

    ```
    vBond(config)#commit and-quit
    vBond#
    ```

11. Verify that the configuration is correct and complete:

    ```
    vBond#show running-config
    ```

After the overlay network is up and operational, create a vBond configuration template on the Cisco vManage that contains the initial configuration parameters. Use the following vManage feature templates:

- System feature template to configure the hostname, system IP address, and vBond functionality.
- AAA feature template to configure a password for the "admin" user.
- VPN Interface Ethernet feature template to configure the interface in VPN 0.

In addition, it is recommended that you configure the following general system parameters:

- From the Cisco vManage menu, choose **Administration** > **Settings** and configure Organization name.
- From the Cisco vManage menu, choose **Configuration** > **Templates**. From System configuration template drop-down, select **create template** and configure Timezone, NTP servers, and device physical location.
- Click **Additional Templates** and from banner feature template drop-down, select **Create Template**. Configure Login banner.
- From System feature configuration template drop-down, select **Create Template** and configure disk and server parameters.
- From AAA feature configuration template drop-down, select **Create Template** and configure AAA, RADIUS and TACACS servers.
- Click **Additional Templates** and from SNMP feature template drop-down, select **Create Template** and configure SNMP.

Note The IP address must be a public address so that all devices in the overlay network can reach Cisco vBond Orchestrator.

Sample Initial CLI Configuration

Below is an example of a simple configuration on Cisco vBond Orchestrator. Note that this configuration includes a number of settings from the factory-default configuration and shows a number of default configuration values.

```
vBond#show running-config
system
 host-name         vBond
 gps-location latitude 40.7127837
 gps-location longitude -74.00594130000002
 system-ip         172.16.240.161
 organization-name "Cisco"
 clock timezone America/Los_Angeles
 vbond 11.1.1.14 local
 aaa
  auth-order local radius tacacs
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password encrypted-password
  !
 !
 logging
  disk
```

```
    enable
   !
!
vpn 0
 interface ge0/0
  ip address 11.1.1.14/24
  no shutdown
 !
 ip route 0.0.0.0/0 11.1.1.1
!
vpn 512
 interface eth0
  ip dhcp-client
  no shutdown
 !
!
```

What's Next

See *Add Cisco vBond Orchestrator to the Overlay Network*.

Create Configuration Templates for Cisco vBond Orchestrator

This article describes how to configure Cisco vBond Orchestrators that are being managed by Cisco vManage. These devices must be configured from Cisco vManage. If you configure them directly from the CLI on the router, Cisco vManage overwrites the configuration with the one stored on the NMS system.

Create Configuration Templates for Cisco vManage

You should create configuration templates for Cisco vManage.

Configuration Prerequisites

Security Prerequisites

Before you can configure Cisco vManage in the Cisco SD-WAN overlay network, you must have generated a certificate for it, and the certificate must already be installed on the device. See Generate a Certificate.

Variables Spreadsheet

The feature templates that you create will contain variables. For Cisco vManage to populate the variables with actual values when you attach a device template to a device, either enter the values manually or click **Import File** in the upper right corner to load an Excel file in CSV format that contains the variables values.

In the spreadsheet, the header row contains the variable name and each row after that corresponds to a device, defining the values of the variables. The first three columns in the spreadsheet must be (in order):

- csv-deviceId—Serial number of the device (used to uniquely identify the device).
- csv-deviceIP—System IP address of the device (used to populate the **system ip address** command).
- csv-host-name—Hostname of the device (used to populate the **system hostname** command).

You can create a single spreadsheet for all devices in the overlay network—Cisco vManages, routers, Cisco vSmart Controllers, and Cisco vBond Orchestrators. You do not need to specify values for all variables for all devices.

Feature Templates for Cisco vManages

The following features are mandatory for Cisco vManage operation, so you must create a feature template for each of them:

Table 91:

Feature	Template Name
Authentication, Authorization, and Accounting (AAA)	AAA
Security	Security
System-wide parameters	System
Transport VPN (VPN 0)	VPN, with the VPN ID set to 0.
Management VPN (for out-of-band management traffic)	VPN, with the VPN ID set to 512.

Create Feature Templates

Feature templates are the building blocks of a Cisco vManage's complete configuration. For each feature that you can enable on Cisco vManage, a template form is provided that you fill out with the desired parameters for that feature.

You must create feature templates for the mandatory Cisco vManage features.

You can create multiple templates for the same feature.

To create vManage feature templates:

1. From the Cisco vManage menu, select **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

3. Click **Add Template**.
4. In the left pane, from **Select Devices**, select **vManage**. You can create a single feature template for features that are available on both the Cisco vManage and other devices. You must, however, create separate feature templates for software features that are available only on Cisco vManage.
5. In the right pane, select the template. The template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining parameters applicable to that template. Optional parameters are generally grayed out. A plus (+) sign is displayed to the right when you can add multiple entries for the same parameter.
6. Enter a template name and description. These fields are mandatory. You cannot use any special characters in template names.

7. For each required parameter, choose the desired value, and if applicable, select the scope of the parameter. Select the scope from the drop-down menu available to the left of each parameter field.
8. Click the plus sign (+) below the required parameters to set values for additional parameters, if applicable.
9. Click **Create**.
10. Create feature templates for each of the required features listed in the previous section.
    a. For the transport VPN, use the template called VPN-vManage and in the VPN Template section, set the VPN to 0, with a scope of Global.
    b. For the management VPN, use the template called VPN-vManage and in the VPN Template section, set the VPN to 512, with a scope of Global.
11. Create any additional feature templates for each optional feature that you want to enable on Cisco vManage.

Release Information

Introduced in Cisco vManage in Release 15.3.

Create Configuration Templates for Cisco vSmart Controller

For Cisco vSmart Controllers that are being managed by a Cisco vManage, you must configure them from Cisco vManage. If you configure them directly from the CLI on Cisco vSmart Controller, Cisco vManage overwrites the configuration with the one stored on Cisco vManage.

Determine Why a Device Rejects a Template

When you attach a template to a device using the screen, the device might reject the template. One reason that this may occur is because the device template contains incorrect variable values. When a device rejects a template, it reverts to the previous configuration.

To determine why the device rejected the template:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Locate the device. The **Template Status** column indicates why the device rejected the template.

Export Device Data in CSV Format

In an overlay network, you might have multiple devices of the same type that have identical or effectively identical configurations. For example, in a network with redundant Cisco vSmart Controllers, each controller must be configured with identical policies. Another example is a network with Cisco vEdge devices at multiple sites, where each Cisco vEdge device is providing identical services at each site.

Because the configurations for these devices are essentially identical, you can create one set of feature templates, which you then consolidate into one device template that you use to configure all the devices. You can create an Excel file in CSV format that lists the variables and defines each device specific variable value for each device. Then you can load the file when you attach a device template to a device.

To export data for all devices to a file in CSV format, click the Export icon. This icon, which is a downward-pointing arrow, is located to the right of the filter criteria both in the WAN Edge List and in the Controllers tab.

vManage NMS downloads all data from the device table to an Excel file in CSV format.

Configure Cisco vSmart Controllers

Add a vSmart Controller

After the Cisco vBond Orchestrator authenticates Cisco vEdge devices, the Cisco vBond Orchestrator provides Cisco vEdge devices information that they need to connect to the Cisco vSmart Controller. A Cisco vSmart Controller controls the flow of data traffic throughout the network via data and app-route policies. To configure Cisco vSmart Controllers:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **Controllers**.
3. Click the **Add Controller** drop-down list and select **vSmart**.
4. In the **Add vSmart** window:
    a. Enter the system IP address of the Cisco vSmart Controller.
    b. Enter the username and password to access the Cisco vSmart Controller.
    c. Select the protocol to use for control-plane connections. The default is DTLS. The DTLS (Datagram Transport Layer Security) protocol is designed to provide security for UDP communications.
    d. If you select TLS, enter the port number to use for TLS connections. The default is 23456.

       The TLS (Transport Socket Layer) protocol that provides communications security over a network.
    e. Check the **Generate CSR** check box to allow the certificate-generation process to occur automatically.
    f. Click **Add**.
5. Repeat Steps 2, 3 and 4 to add additional Cisco vSmart Controllers. The vManage NMS can support up to 20 Cisco vSmart Controllers in the network.

The new Cisco vSmart Controller is added to the list of controllers in the Controllers screen.

Edit Controller Details

Editing controller details lets you update the IP address and login credentials of a controller device. To edit controller details:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and select the controller.
3. Click **…**, and click **Edit**.
4. In the **Edit** window, edit the IP address and the login credentials.
5. Click **Save**.

Delete a Controller

Deleting a controller removes it from the overlay. Delete a controller it if you are replacing it or if you no longer need it in your network.

To delete a controller:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and select the controller.
3. Click **…**, and click **Invalidate**.
4. To confirm the removal of the device and all its control connections, click **OK**.

Configure Reverse Proxy on Controllers

To configure reverse proxy on an individual vManage NMS and Cisco vSmart Controller:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **Controllers**, and select the controller.
3. Click **…**, and click **Add Reverse Proxy**.

   The **Add Reverse Proxy** dialog box is displayed.
4. Click **Add Reverse Proxy**.
5. Configure the private IP address and port number for the device. The private IP address is the IP address of the transport interface in VPN 0. The default port number is 12346. This is the port used to establish the connections that handle control and traffic in the overlay network.
6. Configure the proxy IP address and port number for the device, to create the mapping between the private and public IP addresses and port numbers.
7. If the Cisco vManage NMS or Cisco vSmart Controller has multiple cores, repeat Steps 5 and 6 for each core.
8. Click **Add**.

To enable reverse proxy in the overlay network, from the Cisco vManage menu, choose **Administration** > **Settings**. Then from the Reverse Proxy bar, click **Edit**. Click **Enabled**, and click **Save**.

Enable Data Stream Collection from a WAN Edge Router

By default, collecting streams of data from a network device is not enabled.

To collect data streams from a WAN Edge router in the overlay network, perform the following steps.

Collecting data streams also requires that VPN 512 be configured in your Cisco SD-WAN network.

1. From the Cisco vManage menu, select **Administration** > **Settings**.
2. For **Data Stream**, click **Edit**.
3. Click **Enabled**.
4. From Cisco vManage Release 20.4.1, choose one of the following **IP Address Type** options:
   - **Transport**: Click this option send the data stream to the transport IP address of the Cisco vManage node to which the device is connected.
   - **Management**: Click this option send the data stream to the management IP address of the Cisco vManage node to which the device is connected.
   - **System**: Click this option to send the data stream to the internally configured system IP address of theCisco vManage node to which the device is connected.

     In a Cisco vManage cluster deployment, we recommend that you choose **System** so that the data stream is collected from edge devices that are managed by all Cisco vManage instances in the cluster.
5. From Cisco vManage Release 20.4.1, perform one of these actions:
   - If you choose **Transport** as the IP address type, in the **Hostname** field, enter the public transports IP address that is used to connect to the router.

     You can determine this IP address by using an SSH client to access the router and entering the **`show interface`** CLI command.
   - If you choose **Management** as the IP address type, in the **Hostname** field, enter the IP address or name of the host to collect the data.

     We recommend that this host is one that is used for out-of-band management and that it is located in the management VPN.

   This **Hostname** option is dimmed when **IP Address Type** is **System**.
6. In the **VPN** field, enter the number of the VPN in which the host is located.

   We recommend that this VPN be the management VPN, which is typically VPN 512.

   This **VPN** option is dimmed when **IP Address Type** is **System**.
7. Click **Save**.

Enable Timeout Value for a Cisco vManage Client Session

By default, a user's session to a Cisco vManage client remains established indefinitely and never times out.

To set how long a Cisco vManage client session is inactive before a user is logged out:

1. From the Cisco vManage menu, select **Administration** > **Settings**.
2. For Client Session Timeout option, click **Edit**.
3. Click **Enabled**, and enter the timeout value, in minutes. This value can be from 10 to 180 minutes.
4. Click **Save**.

The client session timeout value applies to all Cisco vManage servers in a Cisco vManage cluster.

Enable vAnalytics

1. Open a support case with Cisco, https://mycase.cloudapps.cisco.com/case, and provide the following information:

   - Customer name
   - Organization Name (as configured in vManage)
   - Cisco Sales/SE contact
   - Approved by (customer contact)
   - Customer email
   - Approved by customer on (specify date)

   Customer approval is needed as vAnalytics collects network and application-related data, and this data is stored in the US-West cloud region in Amazon Web Services.

   After receiving this information, Cisco takes approximately 24 to 48 hours to ready the backend set up and provide the appropriate log-on credentials for vAnalytics.

   Once you receive log-on credentials for vAnalytics:

   a. Navigate to the Cisco vManage Dashboard **Administration** > **Settings** tab.

   b. Click the **Edit** button to the right of the vAnalytics bar.

   c. In the Enable vAnalytics field, click **Enabled**.

   d. Enter **SSO Username** and **SSO Password**.

   e. Check the **I agree** check box.

   f. Click **Save**.

Enforce Software Version on Devices

If you are using the Cisco SD-WAN hosted service, you can enforce a version of the Cisco SD-WAN software to run on a router when it first joins the overlay network.

To ensure that templates are in sync after an upgrade that enforces a software version, make sure of the following before you perform the upgrade:

- The bootflash and flash on the router must have enough free space to support the upgrade
- The version of the SD-WAN image that is on the device before the upgrade must be a lower version than the enforced SD-WAN version you specify in the following procedure

To enforce a version of the Cisco SD-WAN software to run on a router when it first joins the overlay network, follow these steps:

1. Ensure that the software image for the desired device software version is present in the Cisco vManage software image repository:
   a. From the Cisco vManage menu, choose **Maintenance** > **Software Repository**.

      The Software Repository screen opens and displays a table of software images. If the desired software image is present in the repository, continue with Step 2.

   b. If you need to add a software image, click **Add New Software**.
   c. Select the location from which to download the software images, either Cisco vManage, Remote Server, or Remote Server - vManage.
   d. Select an x86-based or a MIPS-based software image.
   e. To place the image in the repository, click **Add**.
2. From the Cisco vManage menu, choose **Administration** > **Settings**.
3. From **Enforce Software Version (ZTP)**, click **Edit**.
4. In **Enforce Software Version**, click **Enabled**.
5. From the **Version** drop-down list, select the version of the software to enforce on the device when they join the network.
6. Click **Save**.

Enforce Strong Passwords

We recommend the use of strong passwords. You must enable password policy rules in Cisco vManage to enforce use of strong passwords.

After you enable a password policy rule, the passwords that are created for new users must meet the requirements that the rule defines. In addition, for releases from Cisco vManage Release 20.9.1, you are prompted to change your password the next time you log in if your existing password does not meet the requirements that the rule defines.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. In **Password Policy**, choose **Edit**.
3. Perform one of these actions, based on your Cisco vManage release:
   - For releases before Cisco vManage Release 20.9.1, click **Enabled**.

- For releases from Cisco vManage Release 20.9.1 click **Medium Security** or **High Security** to choose the password criteria.

By default, **Password Policy** is set to **Disabled**.

4. In the **Password Expiration Time (Days)** field, you can specify the number of days for when the password expires.

   By default, password expiration is 90 days.

   Before your password expires, a banner prompts you to change your password. If the password expiration time is 60 days or more, this banner first appears at 30 days before your password expires. If the password expiration time is less than 60 days, this banner first appears at half the number of days that are configured for the expiration time. If you do not change your password before it expires, you are blocked from logging in. In such a scenario, an admin user can change your password and restore your access.

Note The password expiration policy does not apply to the admin user.

5. Click **Save**.

Install Signed Certificates on vEdge Cloud Routers

When a vEdge Cloud router virtual machine (VM) instance starts, it has a factory-default configuration, which allows the router to boot. However, the router is unable to join the overlay network. For the router to be able to join the overlay network, you must install a signed certificate on the router. The signed certificates are generated based on the router's serial number, and they are used to authorize the router to participate in the overlay network.

Starting from Releases 17.1, the Cisco vManage can act as a Certificate Authority (CA), and in this role it can automatically generate and install signed certificates on vEdge Cloud routers. You can also use another CA and then install the signed certificate manually. For Releases 16.3 and earlier, you manually install signed Symantec certificates on vEdge Cloud routers.

To install signed certificates:

1. Retrieve the vEdge authorized serial number file. This file contains the serial numbers of all the vEdge routers that are allowed to join the overlay network.
2. Upload the vEdge authorized serial number file to Cisco vManage.
3. Install a signed certificate on each vEdge Cloud router.

Retrieve vEdge Authorized Serial Number File

1. Go to http://viptela.com/support/ and log in.
2. Click **Downloads**.
3. Click **My Serial Number Files**. The screen displays the serial number files. Starting from Releases 17.1, the filename extension is .viptela. For Releases 16.3 and earlier, the filename extension is .txt.
4. Click the most recent serial number file to download it.

Upload vEdge Authorized Serial Number File

1. From the Cisco vManage menu, select **Configuration** > **Devices**.
2. Click **vEdge List**, and select **Upload vEdge List**.
3. In the Upload vEdge window:
   a. Click **Choose File**, and select the vEdge authorized serial number file you downloaded from Cisco.
   b. To automatically validate the vEdge routers and send their serial numbers to the controllers, click and select the checkbox **Validate the Uploaded vEdge List** and **Send to Controllers**. If you do not select this option, you must individually validate each router in the **Configuration** > **Certificates** > **vEdge List** page.
4. Click **Upload**.

During the process of uploading the vEdge authorized serial number file, the Cisco vManage generates a token for each vEdge Cloud router listed in the file. This token is used as a one-time password for the router. The Cisco vManage sends the token to the vBond orchestrator and the vSmart controller.

After the vEdge authorized serial number file has been uploaded, a list of vEdge routers in the network is displayed in the vEdge Routers Table in the **Configuration** > **Devices** page, with details about each router, including the router's chassis number and its token.

Install Signed Certificates in Releases 17.1 and Later

Starting from Releases 17.1, to install a signed certificates on a vEdge Cloud router, you first generate and download a bootstrap configuration file for the router. This file contains all the information necessary to allow the Cisco vManage to generate a signed certificate for the vEdge Cloud router. You then copy the contents of this file into the configuration for the router's VM instance. For this method to work, the router and the Cisco vManage must both be running Release 17.1 or later. Finally, you download the signed certificate to the router. You can configure the Cisco vManage to do this automatically or manually.

The bootstrap configuration file contains the following information:

- UUID, which is used as the router's chassis number.
- Token, which is a randomly generated one-time password that the router uses to authenticate itself with the vBond orchestrator and the Cisco vManage.
- IP address or DNS name of the vBond orchestrator.
- Organization name.
- If you have already created a device configuration template and attached it to the vEdge Cloud router, the bootstrap configuration file contains this configuration. For information about creating and attaching a configuration template, see Create Configuration Templates for a vEdge Router .

You can generate a bootstrap configuration file that contains information for an individual router or for multiple routers.

Starting from Releases 17.1, you can also have Symantec generate signed certificates that you install manually on each router, as described later in this article, but this method is not recommended.

Configure the Cisco vBond Orchestrator and Organization Name

Before you can generate a bootstrap configuration file, you must configure the vBond orchestrator DNS name or address and your organization name:

1. From the Cisco vManage menu, select **Administration** > **Settings**.
2. For vBond, click **Edit**.
3. In the vBond DNS/IP Address: Port field, enter the DNS name or IP address of the vBond orchestrator.
4. Click **Save**.
5. For Organization Name, click **View** and verify the orgnization name configured. This name must be identical to that configured on the Cisco vBond Orchestrator.
6. Click **Save**.

Configure Automatic or Manual vEdge Cloud Authorization

Signed certificates must be installed on each vEdge cloud router so that the router is authorized to participate in the overlay network. You can use the Cisco vManage as the CA to generate and install the signed certificate, or you can use an enterprise CA to install the signed certificate.

It is recommended that you use the Cisco vManage as a CA. In this role, Cisco vManage automatically generates and installs a signed certificate on the vEdge Cloud router. Having Cisco vManage act as a CA is the default setting. You can view this setting in the WAN vEdge Cloud Certificate Authorization, on the Cisco vManage **Administration** > **Settings** page.

To use an enterprise CA for generating signed certificates for vEdge Cloud routers:

1. From the Cisco vManage menu, select **Administration** > **Settings**.
2. For WAN Edge Cloud Certificate Authorization, select **Manual**.
3. Click **Save**.

Generate a Bootstrap Configuration File

To generate a bootstrap configuration file for a vEdge Cloud router:

1. From the Cisco vManage menu, select **Configuration** > **Devices**.
2. To generate a bootstrap configuration file for one or multiple vEdge Cloud routers:
   a. Click **WAN Edge List**, select **Export Bootstrap Configuration**.
   b. In the Generate Bootstrap Configuration field, select the file format:
      - For a vEdge Cloud router on a KVM hypervisor or on an AWS server, select **Cloud-Init** to generate a token, vBond orchestrator IP address, vEdge Cloud router UUID, and organization name.
      - For a vEdge Cloud router on a VMware hypervisor, select Encoded String to generate an encoded string.

   c. From the **Available Devices** column, select one or more routers.
   d. Click the arrow pointing to right to move the selected routers to **Selected Devices** column.

e. Click **Generate Generic Configuration**. The bootstrap configuration is downloaded in a .zip file, which contains one .cfg file for each router.

3. To generate a bootstrap configuration file individually for each vEdge Cloud router:

   a. Click **WAN Edge List**, select the desired vEdge Cloud router.

   b. For the desired vEdge Cloud router, click **...**, and select **Generate Bootstrap Configuration**.

   c. In the **Generate Bootstrap Configuration** window, select the file format:

      - For a vEdge Cloud router on a KVM hypervisor or on an AWS server, select Cloud-Init to generate a token, vBond orchestrator IP address, vEdge Cloud router UUID, and organization name.
      - For a vEdge Cloud router on a VMware hypervisor, select Encoded String to generate an encoded string.

Note Beginning with Cisco vManage Release 20.7.1, there is an option available when generating a bootstrap configuration file for a Cisco vEdge device, enabling you generate two different forms of the bootstrap configuration file.

- If you are generating a bootstrap configuration file for a Cisco vEdge device that is using Cisco SD-WAN Release 20.4.x or earlier, then check the **The version of this device is 20.4.x or earlier** check box.
- If you are generating a bootstrap configuration for a Cisco vEdge device that is using Cisco SD-WAN Release 20.5.1 or later, then do not use the check box.

   d. Click **Download** to download the bootstrap configuration. The bootstrap configuration is downloaded in a .cfg file.

   Then use the contents of the bootstrap configuration file to configure the vEdge Cloud router instance in AWS, ESXi, or KVM. For example, to configure a router instance in AWS, paste the text of the Cloud-Init configuration into the User data field:

By default, the **ge0/0** interface is the router's tunnel interface, and it is configured as a DHCP client. To use a different interface or to use a static IP address, and if you did not attach a device configuration template to the router, change the vEdge Cloud router's configuration from the CLI. See *Configuring Network Interfaces*.

Install the Certificate on the vEdge Cloud Router

If you are using automated vEdge Cloud certificate authorization, which is the default, after you configure the vEdge Cloud router instance, Cisco vManage automatically installs a certificate on the router and the router's token changes to its serial number. You can view the router's serial number in the **Configuration** > **Devices** page. After the router's control connections to the Cisco vManage come up, any templates attached to the router are automatically pushed to the router.

If you are using manual vEdge Cloud certificate authorization, after you configure the vEdge Cloud router instance, follow this procedure to install a certificate on the router:

1. Install the enterprise root certificate chain on the router:

```
vEdge# request root-cert-chain install filename [vpn vpn-id]
```

Then, Cisco vManage generates a CSR.

2. Download the CSR:
    a. From the Cisco vManage menu, select **Configuration** > **Certificates**.
    b. For the selected vEdge Cloud router for which to sign a certificate, click **...** and select **View CSR**.
    c. To download the CSR, click **Download**.

3. Send the certificate to a third-party signing authority, to have them sign it.

4. Import the certificate into the device:
    a. From the Cisco vManage menu, select **Configuration** > **Certificates**.
    b. Click **Controllers**, and select **Install Certificate**.
    c. In the **Install Certificate** page, paste the certificate into the Certificate Text field, or click **Select a File** to upload the certificate in a file.
    d. Click **Install**.

5. Issue the following REST API call, specifying the IP address of your Cisco vManage:

```
https://vmanage-ip-address/dataservice/system/device/sync/rootcertchain
```

Create the vEdge Cloud Router Bootstrap Configuration from the CLI

It is recommended that you generate the vEdge Cloud router's bootstrap configuration using Cisco vManage. If, for some reason, you do not want to do this, you can create the bootstrap configuration using the CLI. With this process, you must still, however, use Cisco vManage. You collect some of this information for the bootstrap configuration from Cisco vManage, and after you have created the bootstrap configuration, you use Cisco vManage to install the signed certificate on the router.

Installing signed certificates by creating a bootstrap configuration from the CLI is a three-step process:

1. Edit the router's configuration file to add the DNS name or IP address of the vBond orchestrator and your organization name.
2. Send the router's chassis and token numbers to Cisco vManage.
3. Have Cisco vManage authenticate the vEdge Cloud router and install the signed certificate on the router.

To edit the vEdge Cloud router's configuration file from the CLI:

1. Open a CLI session to the vEdge Cloud router via SSH. To do this in Cisco vManage, select **Tools** > **SSH Terminal** page, and select the desired router.
2. Log in as the user **admin**, using the default password, **admin**. The CLI prompt is displayed.
3. Enter configuration mode:

```
vEdge# config
vEdge(config)#
```

4. Configure the IP address of the vBond orchestrator or a DNS name that points to the vBond orchestrator. The vBond orchestrator's IP address must be a public IP address:

```
vEdge(config)# system vbond (dns-name | ip-address)
```

5. Configure the organization name:

   ```
   vEdge(config-system)# organization-name name
   ```

6. Commit the configuration:

   ```
   vEdge(config)# commit and-quit
   vEdge#
   ```

To send the vEdge Cloud router's chassis and token numbers to Cisco vManage:

1. Locate the vEdge Cloud router's token and chassis number:
   a. From the Cisco vManage menu, select **Configuration** > **Devices**.
   b. Click **WAN Edge List**, locate the vEdge Cloud router.
   c. Make a note of the values in the vEdge Cloud router's Serial No./Token and Chassis Number columns.
2. Send the router's bootstrap configuration information to Cisco vManage:

   ```
   vEdge# request vedge-cloud activate chassis-number chassis-number token token-number
   ```

Issue the **show control local-properties** command on the router to verify the vBond IP address, the organization name the chassis number, and the token. You can also verify whether the certificate is valid.

Finally, have Cisco vManage authenticate the vEdge Cloud router and install the signed certificate on the router.

If you are using automated vEdge Cloud certificate authorization, which is the default, the Cisco vManage uses the chassis and token numbers to authenticate the router. Then, Cisco vManage automatically installs a certificate on the router and the router's token changes to a serial number. You can display the router's serial number in the **Configuration** > **Devices** page. After the router's control connections to Cisco vManage come up, any templates attached to the router are automatically pushed to the router.

If you are using manual vEdge Cloud certificate authorization, after you configure the vEdge Cloud router instance, follow this procedure to install a certificate on the router:

1. Install the enterprise root certificate chain on the router:

   ```
   vEdge# request root-cert-chain install filename [vpn vpn-id]
   ```

   After you install the root chain certificate on the router, and after Cisco vManage receives the chassis and token numbers, Cisco vManage generates a CSR.
2. Download the CSR:
   a. From the Cisco vManage menu, select **Configuration** > **Certificates**.
   b. For the selected vEdge Cloud router for which to sign a certificate, click **...** and select **View CSR**.
   c. To download the CSR, click **Download**.
3. Send the certificate to a third-party signing authority, to have them sign it.
4. Import the certificate into the device:
   a. From the Cisco vManage menu, select **Configuration** > **Certificates**.
   b. Click Controllers and select **Install Certificate**.

c. In the **Install Certificate** page, paste the certificate into the Certificate Text field, or click **Select a File** to upload the certificate in a file.

d. Click **Install**.

5. Issue the following REST API call, specifying the IP address of your Cisco vManage:

   https://*vmanage-ip-address***/dataservice/system/device/sync/rootcertchain**

Install Signed Certificates in Releases 16.3 and Earlier

For vEdge Cloud router virtual machine (VM) instances running Releases 16.3 and earlier, when the vEdge Cloud router VM starts, it has a factory-default configuration, but is unable to join the overlay network because no signed certificate is installed. You must install a signed Symantec certificate on the vEdge Cloud router so that it can participate in the overlay network.

To generate a certificate signing request (CSR) and install the signed certificate on the vEdge Cloud router:

1. Log in to the vEdge Cloud router as the user **admin**, using the default password, **admin**. If the vEdge Cloud router is provided through AWS, use your AWS key pair to log in. The CLI prompt is displayed.

2. Generate a CSR for the vEdge Cloud router:

```
vEdge# request csr upload path
```

   path is the full path and filename where you want to upload the CSR. The path can be in a directory on the local device or on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided. When prompted, enter and then confirm your organization name. For example:

```
vEdge# request csr upload home/admin/vm9.csr
Uploading CSR via VPN 0
Enter organization name            : Cisco
Re-enter organization name         : Cisco
Generating CSR for this vEdge device
........[DONE]
Copying ... /home/admin/vm9.csr via VPN 0
CSR upload successful
```

3. Log in to the Symantec Certificate Enrollment portal:

   https://certmanager.<wbr/>websecurity.symantec.com/<wbr/>mcelp/enroll/index?jur_hash=<wbr/>f422d7ceb508a24e32ea7de4f78d37<wbr/>f8

4. In the **Select Certificate Type** drop-down, select **Standard Intranet SSL** and click **Go**. The Certificate Enrollment page is displayed. Cisco SD-WAN uses the information you provide on this form to confirm the identity of the certificate requestor and to approve your certificate request. To complete the Certificate Enrollment form:

   a. In the Your Contact Information section, specify the First Name, Last Name, and Email Address of the requestor.

   b. In the Server Platform and Certificate Signing section, select Apache from the Select Server Platform drop-down. In the Enter Certificate Signing Request (CSR) box, upload the generated CSR file, or copy and paste the contents of the CSR file. (For details about how to do this, log in to support.viptela.com. Click Certificate, and read the Symantec certificate instructions.)

   c. In the Certificate Options section, enter the validity period for the certificate.

d. In the Challenge Phrase section, enter and then re-enter a challenge phrase. You use the challenge phrase to renew, and, if necessary, to revoke a certificate on the Symantec Customer Portal. It is recommended that you specify a different challenge phrase for each CSR.

e. Accept the Subscriber Agreement. The system generates a confirmation message and sends an email to the requestor confirming the certificate request. It also sends an email to the Cisco to approve the CSR.

5. After Cisco approves the CSR, Symantec sends the signed certificate to the requestor. The signed certificate is also available through the Symantec Enrollment portal.

6. Install the certificate on the vEdge Cloud router:

```
vEdge# request certificate install filename [vpn vpn-id]
```

   The file can be in your home directory on the local device, or it can be on a remote device reachable through FTP, HTTP, SCP, or TFTP. If you are using SCP, you are prompted for the directory name and filename; no file path name is provided.

7. Verify that the certificate is installed and valid:

```
vEdge# show certificate validity
```

After you have installed the certificate on the vEdge Cloud router, the vBond orchestator is able to validate and authenticate the router, and the router is able to join the overlay network.

What's Next

See *Send vEdge Serial Numbers to the Controller Devices*.

Manage a Network Hierarchy

Table 92: Feature History

Feature Name	Release Information	Description
Network Hierarchy and Resource Management	Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	You can create a network hierarchy in Cisco vManage to represent the geographical locations of your network. You can create a region, an area, and a site in a network hierarchy. In addition, you can assign a site ID and a region ID to a device.

The Network Hierarchy and Resource Management feature enables you to do the following:

- Create a region
- Create an area
- Create, edit, and delete a site

Create a Region in a Network Hierarchy

Before You Begin

Ensure that the **Multi-Region Fabric** option in Cisco vManage is enabled.

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Click **Edit** adjacent to the **Multi-Region Fabric** option.
3. Click **Enabled**, and then click **Save**.

Create a Region

1. From the Cisco vManage menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global or area) in the left pane and choose **Add MRF Region**.

Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add a region.

3. In the **Name** field, enter a name for the region. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the region.
5. From the **Parent** drop-down list, choose a parent node.
6. Click **Add**.

Create an Area in a Network Hierarchy

1. From the Cisco vManage menu, choose **Configuration** > **Network Hierarchy**.
2. Click **…** adjacent to a node (global, region, or area) in the left pane and choose **Add Area**.

Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add an area.

3. In the **Name** field, enter a name for the area. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the area.
5. From the **Parent** drop-down list, choose a parent node.
6. Click **Add**.

Create a Site in a Network Hierarchy

1. From the Cisco vManage menu, choose **Configuration** > **Network Hierarchy**.

2. Click **…** adjacent to a node (global, region, or area) in the left pane and choose **Add Site**.

Note In Cisco vManage Release 20.9.x, you can also use the **Add Node** option to add a site.

3. In the **Name** field, enter a name for the site. The name must be unique and can contain only letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.).
4. In the **Description** field, enter a description of the site.
5. From the **Parent** drop-down list, choose a parent node.
6. In the **Site ID** field, enter a site ID.

   If you do not enter the site ID, Cisco vManage generates a site ID for the site.
7. Click **Add**.

Assign a Site ID to a Device

You can assign a site ID to a device using one of the following ways.

Use the Quick Connect Workflow

1. From the Cisco vManage menu, choose **Workflows** > **Workflow Library**.
2. Start the **Quick Connect** workflow.
3. Follow the instructions provided in the workflow.
4. On the **Add and Review Device Configuration** page, enter the site ID of the device.

Note

- You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.

Use a Template

1. From the Cisco vManage menu, choose **Configuration** > **Devices** > **WAN Edge List**.
2. Check if a device is attached to a device template.
3. From the Cisco vManage menu, choose **Configuration** > **Templates** > **Feature Templates**.
4. Click **…** adjacent to the System feature template and choose **Edit**.
5. Click the **Basic Configuration** tab and set the scope of the **Site ID** field to **Global** and enter the site ID.
6. Click **Update**.
7. Click **Configure Devices** to push the configuration to the device.

In Step 5, if you set the scope of the **Site ID** field to **Device Specific**, do the following:

1. From the Cisco vManage menu, choose **Configuration** > **Templates** > **Device Templates**.
2. Click **…** adjacent to the device template and choose **Edit Device Template**.
3. In the **Site ID** field, enter the site ID.

   You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.
4. Click **Update**.
5. Click **Configure Devices** to push the configuration to the device.

Use a Configuration Group

The configuration group flow is applicable only for the Cisco IOS XE SD-WAN devices.

1. From the Cisco vManage menu, choose **Configuration** > **Templates** > **Configuration Groups**.
2. Click **…** adjacent to the configuration group name and choose **Edit**.
3. Click **Associated Devices**.
4. Choose a device that is associated with the configuration group and click **Deploy**.

   The **DeployConfiguration Group** workflow starts.
5. Follow the instructions provided in the workflow.
6. On the **Add and Review Device Configuration** page, enter the site ID of the device.

   You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.

Assign a Region ID to a Device

Before You Begin

- Have access to the **Multi-Region Fabric** feature.
- Ensure that the region is available in the network hierarchy.

Assign a Region ID

1. From the Cisco vManage menu, choose **Configuration** > **Devices** > **WAN Edge List**.
2. Check if the corresponding device is attached to a device template.
3. From the Cisco vManage menu, choose **Configuration** > **Templates** > **Feature Templates**.
4. Click **…** adjacent to the System feature template and choose **Edit**.

5. Click the **Basic Configuration** tab and set the scope of the **Region ID** field to **Global** and enter the region ID.

   You can use any of the existing region IDs that are available in the network hierarchy. If the specified region ID is not available in the network hierarchy, the template push operation to the devices fails.

6. Click **Update**.
7. Click **Configure Devices** to push the configuration to the device.

In Step 5, if you set the scope of the **Region ID** field to **Device Specific**, do the following:

1. From the Cisco vManage menu, choose **Configuration** > **Templates** > **Device Templates**.
2. Click **…** adjacent to the device template and choose **Edit Device Template**.
3. In the **Region ID** field, enter the region ID.
4. Click **Update**.
5. Click **Configure Devices** to push the configuration to the device.

Manage Certificates in Cisco vManage

Perform certificate operations in Cisco vManage on the **Configuration** > **Certificates** page.

- Top bar—On the left are the menu icon, for expanding and collapsing the Cisco vManage menu, and the vManage product name. On the right are a number of icons and the user profile drop-down.
- Title bar—Includes the title of the screen, Certificates.
- WAN Edge List tab—Install the router authorized serial number file on the controllers in the overlay network and manage the serial numbers in the file. When you first open the Certificates screen, the WAN Edge List tab is selected.
  - Send to Controllers—Send the WAN edge router chassis and serial numbers to the controllers in the network.
  - Table of WAN edge routers in the overlay network—To re-arrange the columns, drag the column title to the desired position.
- Controllers tab—Install certificates and download the device serial numbers to the vBond orchestrator.
  - Send to vBond—Send the controller serial numbers to the Cisco vBond Orchestrator.
  - Install Certificate—Install the signed certificates on the controller devices. This button is available only if you select Manual in **Administration** > **Settings** > **Certificate Signing by Symantec**.
  - Export Root Certificate—Display a copy of the root certificate for the controller devices that you can download to a file.
  - Table of controller devices in the overlay network—To re-arrange the columns, drag the column title to the desired position.
  - Certificate status bar—Located at the bottom of the screen, this bar is available only if you select Server Automated in **Administration** > **Settings** > **Certificate Authorization**. It displays the states of the certificate installation process:

    - Device Added
    - Generate CSR
    - Waiting for Certificate
    - Send to Controllers

  A green check mark indicates that the step has been completed. A grey check mark indicates that the step has not yet been performed.

- Search box—Includes the Search Options drop-down, for a Contains or Match string.
- Refresh icon—Click to refresh data in the device table with the most current data.
- Export icon—Click to download all data to a file, in CSV format.
- Show Table Fields icon—Click the icon to display or hide columns from the device table. By default, all columns are displayed.

Authorize a Controller Certificate for an Enterprise Root Certificate

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. In the **Controller Certificate Authorization** area, click **Edit**.
3. Click **Enterprise Root Certificate**. If a warning appears, click **Proceed** to continue.
4. Click **Set CSR Properties**.
5. Paste an SSL certificate into the **Certificate** field or click **Select a file** and navigate to an SSL certificate file.
6. (Optional) In the **Subject Alternative Name (SAN) DNS Names** field, you can enter multiple host names to use the same SSL certificate.

   Example: cisco.com and cisco2.com
7. (Optional) In the **Subject Alternative Name (SAN) URIs** field, you can enter multiple URIs to use the same SSL certificate.

   Example: cisco.com and support.cisco.com

   This is helpful for an organization that uses a single certificate for a host name, without using different subdomains for different parts of the organization.

Check the WAN Edge Router Certificate Status

In the **WAN Edge List** tab, check the **Validate** column. The status can be one of the following:

- Valid (shown in green)—The router's certificate is valid.
- Staging (shown in yellow)—The router is in the staging state.
- Invalid (shown in red)—The router's certificate is not valid.

Validate a WAN Edge Router

When you add Cisco vEdge devices and WAN routers to the network using the **Configuration** > **Devices** screen, you can automatically validate the routers and send their chassis and serial numbers to the controller devices by clicking the checkbox Validate the uploaded WAN Edge List and send to controllers. If you do not select this option, you must individually validate each router and send their chassis and serial numbers to the controller devices. To do so:

1. In the **WAN Edge List** tab, select the router to validate.
2. In the **Validate** column, click **Valid**.
3. Click **OK** to confirm the move to the valid state.
4. Repeat the steps above for each router you wish to validate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco vManage NMS displays the Push WAN Edge List screen showing the status of the push operation.

Stage a WAN Edge Router

When you initially bring up and configure a WAN Edge router, you can place it in staging state using the Cisco vManage instance. When the router is in this state, you can configure the router, and you can test that the router is able to establish operational connections with the vSmart controller and the vManage instance.

After you physically place the router at its production site, you change the router's state from staging to valid. It is only at this point that the router joins the actual production network. To stage a router:

1. In the WAN Edge List tab, select the router to stage.
2. In the **Validate** column, click **Staging**.
3. Click **OK** to confirm the move to the staging state.
4. Click **Send to Controllers** in the upper left corner of the screen to sync the WAN edge authorized serial number file with the controllers. vManage NMS displays the **Push WAN Edge List** screen showing the status of the push operation.
5. To unstage, validate the WAN Edge Router.

Invalidate a WAN Edge Router

1. In the **WAN Edge List** tab, select the router to invalidate.
2. In the **Validate** column, click **Invalid**.
3. Click **OK** to confirm the move to the invalid state.
4. Repeat the steps above for each router you wish to invalidate.
5. Click the **Send to Controllers** button in the upper left corner of the screen to send the chassis and serial numbers of the validated routers to the controller devices in the network. Cisco vManage instance displays the **Push WAN Edge List** screen showing the status of the push operation.

Send the Controller Serial Numbers to Cisco vBond Orchestrator

To determine which controllers in the overlay network are valid, the Cisco vBond Orchestrator keeps a list of the controller serial numbers. The Cisco vManage instance learns these serial numbers during the certificate-generation process.

To send the controller serial numbers to the Cisco vBond Orchestrator:

1. In the **Controllers** tab, check the certificate status bar at the bottom of the screen. If the **Send to Controllers** check mark is green, all serial numbers have already been sent to the Cisco vBond Orchestrator. If it is grey, you can send one or more serial numbers to the Cisco vBond Orchestrator.
2. Click the **Send to vBond** button in the **Controllers** tab. A controller's serial number is sent only once to the Cisco vBond Orchestrator. If all serial numbers have been sent, when you click **Send to vBond**, an error message is displayed. To resend a controller's serial number, you must first select the device and then select **Invalid in the Validity** column.

After the serial numbers have been sent, click the **Tasks** icon in the Cisco vManage toolbar to display a log of the file download and other recent activities.

Install Signed Certificate

If in **Administration** > **Settings** > **Certificate Signing by Symantec**, you selected the **Manual** option for the certificate-generation process, use the **Install Certificate** button to manually install certificates on the controller devices.

After Symantec or your enterprise root CA has signed the certificates, they return the files containing the individual signed certificates. Place them on a server in your local network. Then install them on each controller:

1. In the **Controllers** tab, click **Install Certificate**.
2. In the **Install Certificate** window, select a file, or copy and paste the certificate text.
3. Click **Install** to install the certificate on the device. The certificate contains information that identifies the controller, so you do not need to select the device on which to install the certificate.
4. Repeat Steps the steps above to install additional certificates.

Export Root Certificate

1. In the **Controllers** tab, click the **Export Root Certificate** button.
2. In the **Export Root Certificate** window, click **Download** to export the root certificate to a file.
3. Click **Close**.

View a Certificate Signing Request

1. In the WAN Edge List or **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row, and click **View CSR** to view the certificate signing request (CSR).

View a Device Certificate Signing Request

1. In the **WAN Edge List** or **Controllers** tab, select a Cisco IOS XE SD-WAN device.
2. Click the **More Actions** icon to the right of the row, and click **View Device CSR** to view the certificate signing request (CSR).

   For a Cisco IOS XE SD-WAN device where trustpoint has been configured, clicking the **More Actions** icon allows you to view three options:

   - View Device CSR
   - Generate Feature CSR
   - View Feature CSR

Note Cisco vManage will generate alarms only if device certificate is installed through Cisco vManage. If you install certificate manually, Cisco vManage will not generate alarms for certificate expiration.

View the Certificate

1. In the **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row and click **View Certificate**.

Generate a Controller Certificate Signing Request

1. From the Cisco vManage menu, choose **Configuration** > **Certificates**.
2. Click **Controllers**.
3. For the desired controller, click **…** and choose **Generate CSR**.

   The **Generate CSR** window is displayed.
4. In the **Generate CSR** window, click **Download** to download the file to your local PC (that is, to the PC you are using to connect to the Cisco vManage NMS).
5. Repeat the preceding steps to generate a CSR for another controller.

Generate a Feature Certificate Signing Request

1. From the Cisco vManage menu, choose **Configuration** > **Certificates**.
2. Click **WAN Edge List**.
3. For the desired device, click **…** and choose **Generate Feature CSR**.

   The **Generate Feature CSR** window is displayed.

4. In the **Generate Feature CSR** window, click **OK** to continue with the generation of feature CSR. This step authenticates the device trustpoint that has been set and extracts the CSR from the device.
5. Repeat the steps above for each device for which you are generating a CSR.

Reset the RSA Key Pair

1. In the **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row and click **Reset RSA**.
3. Click **OK** to confirm resetting of the device's RSA key and to generate a new CSR with new public or private keys.

Invalidate a Device

1. In the **Controllers** tab, select a device.
2. Click the **More Actions** icon to the right of the row and click **Invalidate**.
3. Click **OK** to confirm invalidation of the device.

View Log of Certificate Activities

To view the status of certificate-related activities:

1. Click the **Tasks** icon located in the vManage toolbar. Cisco vManage NMS displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. Cisco vManage NMS opens a status window displaying the status of the task and details of the device on which the task was performed.

View a Signed Certificate

Signed certificates are used to authenticate Cisco SD-WAN devices in the overlay network. To view the contents of a signed certificate using Cisco vManage:

1. From the Cisco vManage menu, choose **Configuration** > **Certificates**.
2. Click **Controllers**.
3. For the desired device, click **...** and choose **View Certificate** to view the installed certificate.

Manage Root Certificate Authority Certificates in Cisco vManage

Feature Name	Release Information	Description
Support for Managing Root CA Certificates in Cisco vManage	Cisco IOS XE Release 17.4.1a Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	Add and manage root certificate authority (CA) certificates.

Add a Root Certificate Authority Certificate

1. In Cisco vManage, choose **Administration** > **Root CA Management**.
2. Click **Modify Root CA**.
3. In the **Root Certificate** field, paste in certificate text, or click **Select a File** to load a certificate from a file.
4. Click **Add**. The new certificate appears in the certificate table. The **Recent Status** column indicates that the certificate has not yet been installed.
5. Click **Next** and review the details of any certificates that have not been installed.
6. Click **Save** to install the certificate(s). The new certificate appears in the certificate table.

View a Root Certificate Authority Certificate

1. In Cisco vManage, choose **Administration** > **Root CA Management**.
2. (optional) In the search field, enter text to filter the certificate view. You can filter by certificate text or attribute values, such as serial number.
3. In the table of certificates, click **More Actions** (**…**) and choose **View**. A pop-up window appears, displaying the certificate and its details.

Delete a Root Certificate

Use this procedure to delete a root Certificate Authority (CA) certificate.

1. In Cisco vManage, choose **Administration** > **Root CA Management**.
2. Click **Modify Root CA**.
3. Select one or more root certificates in the table and click the **trash** icon in the **Action** column. The table shows the certificate as marked for deletion.
4. Click **Next** and review the details of any certificates that are marked for deletion.
5. Click **Save** to delete the certificate(s).

Manage Device Templates

Edit a Device Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** or **Feature Templates**, and select a template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

3. Click **…**, and click **Edit**.

You cannot change the name of a device or feature template when that is attached to a device.

Note You can edit templates simultaneously from one or more vManage servers. For simultaneous template edit operations, the following rules apply:

- You cannot edit the same device or feature template simultaneously.
- When you are editing a device template, all other feature templates attached to that device template are locked and you cannot perform any edit operations on them.
- When you are editing a feature template that is attached to a device template, that device template as well as all other feature templates attached to it are locked and you cannot perform any edit operations on them.

Delete a Template

Deleting a template does not remove the associated configuration from devices.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** or **Feature Templates**, and select a template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

3. Click **…**, and click **Delete**.
4. To confirm the deletion of the template, click **OK**.

Copy a Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.

2. Click **Device Templates** or **Feature Templates**, and select a template.

> **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

3. Click **…**, and click **Copy**.
4. Enter a new template name and description.
5. Click **Copy**.

Edit a CLI Device Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and select a template.

> **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Edit**.
4. Under **Device CLI Template**, edit the template.
5. Click **Update**.

Manage Licenses for Smart Licensing Using Policy

Table 93: Feature History

Feature Name	Release Information	Description
License Management for Smart Licensing Using Policy, Using Cisco vManage	Cisco IOS XE Release 17.5.1a Cisco vManage Release 20.5.1	Cisco vManage shows available DNA licenses, assigns licenses to devices, and reports license consumption to Cisco Smart Software Manager (Cisco SSM).
Support for License Management Offline Mode and Compliance Alarms	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	You can manage Cisco SD-WAN licenses through a Cisco vManage instance that is not connected to the internet. To synchronize license and compliance information between Cisco vManage and Cisco SSM, you must periodically download synchronization files from Cisco vManage and upload the files to Cisco SSM.

Feature Name	Release Information	Description
Support for Postpaid MSLA License Billing Models	Cisco IOS XE Release 17.8.1a Cisco vManage Release 20.8.1	For postpaid Managed Services License Agreement (MSLA) program licenses, Cisco SD-WAN supports two distinct billing models for licenses—committed (MSLA-C) and uncommitted (MSLA-U). The procedure for assigning a postpaid license enables you to choose one of these two MSLA license types.
Support for License Management Using a Proxy Server	Cisco IOS XE Release 17.9.1a Cisco vManage Release 20.9.1	If you configure Cisco vManage to use a proxy server for internet access, Cisco vManage uses the proxy server to connect to Cisco SSM or an on-prem SSM.
Support for Managing Licenses Using Cisco Smart Software Manager On-Prem	Cisco IOS XE Release 17.9.1a Cisco vManage Release 20.9.1	Cisco vManage can synchronize device licenses using a Cisco SSM on-prem license server. This is useful for organizations that use Cisco SSM on-prem to accommodate a strict security policy that does not permit devices to communicate with Cisco SSM over a direct internet connection.

Configure the License Reporting Mode

Before You Begin

When using Cisco SD-WAN multitenancy, only the service provider configures the Cisco SSM license server details, using the license server credentials.

Configure the License Reporting Mode

1. For Cisco vManage Release 20.9.1 and later, from the Cisco vManage menu, choose **Administration** > **Settings**.

Note In Cisco vManage Release 20.8.x and earlier, to configure the license reporting mode, from the Cisco vManage menu, choose **Administration** > **License Management**. Click **Sync Licenses & Refresh Devices** and choose a license reporting mode. Then continue with the procedure for synchronizing licenses.

2. In the **License Reporting** section, click **Edit** and choose one of the following:

Note Changing the mode causes Cisco vManage to permanently clear any license information that it is currently storing.

- Online
- Offline

- On-prem

  Enter the following information for the Cisco SSM on-prem server:

Field	Description
SSM Server	IP address of the Cisco SSM on-prem license server.
SSM Credentials **Client ID** and **Client Secret**	Client ID and client secret credentials for the Cisco SSM on-prem license server. This information is available from the administrator who manages the license server.

3. Click **Save**.

Enter Smart Account Credentials in Cisco vManage

Before You Begin

Ensure that you have configured DNS host and next-hop IP route entries for the Cisco SSM servers under VPN 0 on Cisco vManage. Without this configuration, Cisco vManage cannot communicate with Cisco SSM.

Enter Smart Account Credentials

1. From the Cisco vManage menu, choose **Administration** > **License Management**.
2. Click **Sync Licenses & Refresh Devices**.

   The **Reporting Mode** area shows the reporting mode configured on the **Administration** > **Settings** page (requires administrator permissions).
3. Click **Smart Account Credentials**.
4. In the **Smart Account Credentials** dialog box, configure the following:

Field	Description
Username	Username of the account you use to access the Smart Accounts and Virtual Accounts for which you have administrative privileges.
Password	Password for the account you use to access Smart Accounts and Virtual Accounts.

5. Click **Save**.

   Cisco vManage authenticates the Smart Account credentials, and on successful authentication, saves the credentials in the database.

Synchronize Licenses

Before You Begin

- You use this procedure to specify Smart Account and Virtual Account information, or synchronize licenses on-demand, which is useful if you have recently added licenses to your Smart Account and want to bring those licenses into Cisco vManage.
- Ensure licenses belong to the correct Smart Accounts or Virtual Accounts on Cisco SSM.

  When the selected Smart Accounts and Virtual Accounts are registered with Cisco vManage, Cisco vManage fetches and synchronizes the license information with Cisco SSM, and reports usage of the licenses in these accounts.

Synchronize Licenses

1. From the Cisco vManage menu, choose **Administration** > **License Management**.
2. Click **Sync Licenses & Refresh Devices**.
3. In the **Sync Licenses & Refresh Devices** dialog box, configure the following:

Note If these details are already configured, you can skip this step and proceed to the next step to synchronize licenses again. This is useful if you have recently added licenses to your Smart Account and want to bring those licenses into Cisco vManage.

Item	Description
Select Smart/Virtual Accounts to Fetch/Sync Licenses	Select the Smart Accounts or Virtual Accounts for which Cisco vManage must fetch licenses from the Cisco SSM. Cisco vManage also reports license usage for the licenses in these accounts. **Note** Selecting an Smart Account automatically selects all the Virtual Accounts under the Smart Account. To stop Cisco vManage from fetching and synchronizing license information with Cisco SSM for an Smart Account or Virtual Account registered earlier, deselect the Smart Account or Virtual Account. You can deregister the Smart Account or Virtual Account only if you have not assigned any licenses from the account.

Item	Description
Advanced > **Type of Licenses**	Choose the type of licenses that must be fetched by Cisco vManage from among the license types that may belong to the selected Smart Accounts and Virtual Accounts. Select one of the following: • **Prepaid** • **Postpaid** • **Mixed** (both Prepaid and Postpaid) From Cisco vManage Release 20.8.1, if you choose to synchronize postpaid licenses, the license assignment procedure enables you to select committed MSLA licenses (MSLA-C) or uncommitted MSLA licenses (MSLA-U). See Assign a License to a Device.
Advanced > **Multiple Entitlement**	Select one of the following: • **On**: You can assign more than one license to a device. • **Off**: You can assign only one license to a device. **Note** Set this setting to **On** only if you need to map more than one DNA entitlement to a single device.

4. Click **Sync**.

Assign a License to a Device

1. From the Cisco vManage menu, choose **Administration** > **License Management**.
2. Click **Device**.
3. Select the devices to which to assign a license using the check box for each device.
4. Click **Assign License/Subscription**.

   The **Assign License/Subscription** dialog box appears.
5. In the **Assign License/Subscription** dialog box, configure the following:
   - In Cisco vManage Release 20.8.1 and later, the following options appear:

Template Name	To use a new template, enter a unique name for the template. To use an existing template, do the following: **a.** Turn on the **Use existing template** toggle. **b.** Choose an existing template.
Virtual Account	Choose the virtual account from which you wish to assign a license to the device.
MSLA Type	Choose one of the following: • **MSLA-C**: MSLA licenses using the committed billing model • **MSLA-U**: MSLA licenses using the uncommitted billing model
Subscription ID	Choose the subscription ID to track the license consumption. This option appears only if both of the following are true: • The license mode is postpaid. • You have chosen an option in the **MSLA Type** field.

License	Choose license to apply to the device. If you have enabled Multiple Entitlements in the **Sync Licenses & Refresh Devices** dialog box, you can assign up to three licenses to the device. **Note** • Select a license that belongs to the Virtual Account you have selected. On Cisco SSM, you can check the licenses that are available in a Virtual Account. • Check the device license applicability matrix in the Cisco DNA Software for SD-WAN and Routing Ordering Guide to ensure that you assign a license that is applicable to the device. Different device models support different throughputs. If you apply an incompatible license, the license may have no effect on device behavior. However, Cisco vManage will record the consumption of the license. • When assigning licenses, Cisco vManage shows the throughput entitlement levels as tiers. Select the tier that matches the license you have purchased. If you purchased a license with a throughput expressed as a throughput value, find the tier that corresponds to the throughput that the license provides. For example, for a Routing DNA Advantage license, Tier 2 provides up to 1 Gbps throughput. If your DNA Advantage license provides 1 Gbps, choose Tier 2. Tier 0: 10M-15M (up to 30M aggregate) Tier 1: 25M-100M (up to 200M aggregate) Tier 2: 250M-1G (up to 2G aggregate) Tier 3: 2.5G-10G (up to 20G aggregate) The list includes the predefined licenses that Cisco vManage provides, together with the licenses in the virtual account that you have chosen, that meet the MSLA type and subscription ID criteria.

- In Cisco vManage Release 20.7.x and earlier, the following options appear:

Are you using utility-based licensing (MSLA)?	Check this check box if you wish to apply an MSLA license. By default, the check box is unchecked.
Template Name	To use a new template, enter a unique name for the template. To use an existing template, do the following: **a.** Turn on the **Use existing template** toggle. **b.** Choose an existing template.
Virtual Account	Choose the virtual account from which you wish to assign a license to the device.

License	Choose license to apply to the device. If you have enabled Multiple Entitlements in the **Sync Licenses & Refresh Devices** dialog box, you can assign up to three licenses to the device. **Note** • Select a license that belongs to the Virtual Account you have selected. On Cisco SSM, you can check the licenses that are available in a Virtual Account. • Check the device license applicability matrix in the Cisco DNA Software for SD-WAN and Routing Ordering Guide to ensure that you assign a license that is applicable to the device. Different device models support different throughputs. If you apply an incompatible license, the license may have no effect on device behavior. However, Cisco vManage will record the consumption of the license. • When assigning licenses, Cisco vManage shows the throughput entitlement levels as tiers. Select the tier that matches the license you have purchased. If you purchased a license with a throughput expressed as a throughput value, find the tier that corresponds to the throughput that the license provides. For example, for a Routing DNA Advantage license, Tier 2 provides up to 1 Gbps throughput. If your DNA Advantage license provides 1 Gbps, choose Tier 2. Tier 0: 10M-15M (up to 30M aggregate) Tier 1: 25M-100M (up to 200M aggregate) Tier 2: 250M-1G (up to 2G aggregate) Tier 3: 2.5G-10G (up to 20G aggregate)
Subscription ID	Choose the subscription ID to be used to track the license consumption. The subscription ID field is displayed only for the following conditions: • if mode is postpaid. • if mode is mixed and MSLA is true and if there are any subscriptions available.

6. Click **Save**.

The license is assigned and you are returned to **License Management** > **Device** tab. In the table listing the devices, entries are made in the following columns in accordance with the license assignment:

- Template Name: name of the template used to assign the license
- Virtual Account: name of Virtual Account to which license belongs
- MSLA:
  - True for an MSLA license
  - False for an a la carte or EA license

- License Status: subscribed
- License Type: prepaid, postpaid, or mixed based on the types of licenses assigned to the device.
- Subscription ID: The subscription ID used for billing purposes in case of a postpaid license. For a prepaid license, this column has a blank entry.

Monitor License Usage

License Management Overview

From the Cisco vManage menu, choose **Administration** > **License Management** to display the **License Management Overview**.

The **License Management Overview** page shows license information, including what percentage of devices have licenses assigned, the top types of licenses assigned to devices, license usage, license alarms, and so on.

License alarms alert you to licensing issues affecting devices in the Cisco SD-WAN network. You can click the alarm icon to display details of the problem. Issues include the following:

- A device is not licensed.
- The interval for reporting license usage to Cisco SSM has been exceeded.
  - Prepaid licenses: A report is required every three months.
  - Postpaid licenses: A report is required each month.

License Management Overview

After you have assigned at least one license, the **Overview** tab in the **Administration** > **License Management** page provides the following information:

Device Assignment Distribution	• Percentage of licensed devices • Percentage of unlicensed devices
Top 5 licenses	Lists the top 5 licenses in use and shows the usage percentage for each license.
License Usage vs Availability	The dashlet features a bar chart with stacked columns. The chart uses two stacked columns for each of the three license packages Advantage, Essentials, and Premier. For each package, the column on the left represents the count of used licenses; the column on the right represents the count of available licenses. The stacked segments in each column represent a particular license tier (such as Tier 0 or Tier 1). The segment for each tier is of a different color, as identified in the legend.

License and Devices Overview	This section provides the following details for each license assigned: • Name (for example, Routing DNA Essentials: Tier 0) • Number of Licensed Devices: Number of devices to which this license is assigned. • Number of Total Licenses: Sum of the number of licenses assigned and number of licenses available. • Last Assigned On: Date and time when the license was most recently assigned.

Enable Offline Mode

Before You Begin

Note Changing the mode from online to offline, or from offline to online causes Cisco vManage to permanently clear any license information that it is currently storing.

Enable Offline Mode, Cisco vManage Release 20.9.1 and Later

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. In the **License Reporting** area, click the **Offline** option.

Enable Offline Mode, Before Cisco vManage Release 20.9.1

1. From the Cisco vManage menu, choose **Administration** > **License Management**.
2. Click **Overview**.
3. Click **Sync Licenses & Refresh Devices**.
4. Click the **Offline** option.
5. (Optional) Click **Advanced** and select license types or configure multiple entitlement. For information about these options, see Fetch and Synchronize Licenses.
6. Click **Sync**.

Note If you are configuring offline mode for the first time, we recommend uploading a license summary file. See Generate a Cisco SSM License Summary File and Upload It into Cisco vManage.

Generate a Cisco SSM License Summary File and Upload It into Cisco vManage

Generating a license summary file in Cisco SSM and uploading the file to Cisco vManage brings all of the license information from your Cisco smart account into Cisco vManage.

1.

Note Generating a license summary file in the Cisco SSM portal is outside the scope of Cisco SD-WAN documentation and is subject to change.

In Cisco Software Central, navigate to **Manage Licenses**, then navigate to **Reports**.

2. Locate the option for downloading a synchronization file for device controllers. Specify Cisco vManage as the controller type, and include all virtual accounts.
3. Download the license summary file, which is in tar.gz format.
4. From the Cisco vManage menu, choose **Administration** > **License Management**.
5. Click **Overview**.
6. Click **Sync Licenses & Refresh Devices**.
7. Click the **Offline** option.
8. In the **Attach License File** area, click the option to upload a file. Browse to the license summary file and upload it.
9. Click **Sync**.

Generate a Usage Report File in Cisco vManage and Synchronize with Cisco SSM

When managing licenses with Cisco vManage in the offline mode, use manually generated files to enable Cisco vManage to provide information about license assignment to Cisco SSM.

To generate a usage report file in Cisco vManage, upload it to Cisco SSM, receive an acknowledgement file from Cisco SSM, and upload the acknowledgement file to Cisco vManage, perform the following steps.

1. From the Cisco vManage menu, choose **Administration** > **License Management**.
2. Click **Reporting**.
3. In the table, in the row with the Cisco Smart Account, click **…** and choose **Generate Report** to generate the usage report file.

   When you generate a report, the Cisco vSmart Controller starts a 48-hour timer. If you do not upload an acknowledgement file from Cisco SSM within that time, an alert appears in the **License Management Overview** dashboard.

4. In Cisco SSM, upload the usage report file.

Note The details of procedures in the Cisco SSM portal are outside the scope of this documentation and subject to change.

a. In Cisco Software Central, navigate to **Manage Licenses**.

b. Navigate to **Reports**.

c. Navigate to **Upload Usage Data** > **Select and Upload File** or the equivalent, and upload the report file generated by Cisco vManage.

d. If prompted to select a virtual account, select the desired virtual account.

Note In a scenario where you have not yet generated a license summary in Cisco SSM and uploaded it to Cisco vManage, Cisco SSM prompts you to select a virtual account. After you have generated a license summary in Cisco SSM and uploaded it to Cisco vManage, Cisco vManage has the virtual account information that it needs to associate licenses with the correct virtual account.

For information about the scenario of assigning licenses to devices before providing Smart Account details to Cisco vManage, see Information About Offline Mode

.

Cisco SSM generates an acknowledgement file.

e. When Cisco SSM finishes generating an acknowledgement file, click **Download** or the equivalent to download the file.

5. From the Cisco vManage menu, choose **Administration** > **License Management**.

6. Click **Reporting**.

7. In the table, in the row with the Cisco Smart Account, click **…** and choose **Upload Ack** to upload the acknowledgement file from Cisco SSM.

Manage HSEC Licenses

Table 94: Feature History

Feature Name	Release Information	Description
Manage HSEC Licenses	Cisco IOS XE Release 17.9.1a Cisco vManage Release 20.9.1	You can use Cisco vManage to install HSEC licenses on devices An HSEC license is required to enable devices to support encrypted traffic throughput of 250 Mbps or higher.

Synchronize HSEC Licenses, Online Mode

Before You Begin

- This procedure requires Cisco vManage to have internet access. If Cisco vManage does not have internet access, such as for security reasons, use the Synchronize HSEC Licenses, Offline Mode, on page 242 procedure.
- This procedure requires entering credentials for your Cisco Smart Account

Synchronize HSEC Licenses, Online Mode

1. From the Cisco vManage menu, choose **Workflows** > **Workflow Library**.
2. Click the **Sync and Install HSEC Devices** workflow.
3. Click **Sync Licenses** and then click **Next**.
4. Click **Online** and then click **Next**.
5. Enter the credentials for your Cisco SSM account and then click **Next**.
6. On the **HSEC Device Activation Overview** page, click **Next**.
7. On the **Select Virtual Account** page, choose a virtual account from the drop-down list. The list is populated by the Cisco SSM account that you logged into in a previous step.
8. On the **Select HSEC-Compatible Devices** page, select the devices on which you want to install an HSEC license and then click **Summary**.

Note If an HSEC-compatible device already has an HSEC license installed by Cisco vManage, then the device is not selectable.

9. Review the summary and then click **Assign** to begin the synchronization. Cisco vManage loads the requested licenses from Cisco SSM and assigns them to the devices.
10. The process of loading and assigning licenses may take several minutes. You can monitor the progress by viewing the Cisco vManage task list.
11. After the HSEC licenses have been loaded and assigned, to install them, use the Install HSEC Licenses, on page 244 procedure.

Synchronize HSEC Licenses, Offline Mode

Before You Begin

- If Cisco vManage has internet access, we recommend using the Synchronize HSEC Licenses, Online Mode, on page 242 procedure.
- Use this procedure if Cisco vManage does not have internet access, such as for security reasons.
- This procedure requires entering credentials for your Cisco SSM Account.

Synchronize HSEC Licenses, Offline Mode

1. From the Cisco vManage menu, choose **Workflows** > **Workflow Library**.
2. Click the **Sync and Install HSEC Licenses** workflow.
3. Click **Sync Licenses** and then click **Next**.
4. Click **Offline** and then click **Next**.
5. On the **HSEC Device Activation Overview** page, click **Next**.
6. Click **Download Process** and then click **Next**.
7. On the **Offline Mode - Sync Licenses Task** page, select the devices on which to install an HSEC license.
8. Click **Next**.
9. Click **Download HSEC Device File**.
10. On the summary page, click **Download** to download a file to a local location.

    The file contains the list of devices that require an HSEC license.
11. Click **Done**.
12. Click **Cisco Smart Software Manager** to open Cisco SSM.
13. Log in to Cisco SSM and complete the following two steps:

    Note The details of procedures in the Cisco SSM portal are outside the scope of this documentation and subject to change.

    a. Upload the file that you downloaded from Cisco vManage. The procedure is identical to uploading a usage report file, as described in License Management Offline Mode.

    b. Download the Acknowledgement file.

       This file contains the HSEC licenses required for the devices that you selected.
14. From the Cisco vManage menu, choose **Workflows** > **Workflow Library**.
15. Click the **Sync and Install HSEC Devices** workflow.
16. Click **Sync Licenses** and then click **Next**.
17. Click **Offline** and then click **Next**.
18. On the **HSEC Device Activation Overview** page, click **Next**.
19. Click **Upload Process** and then click **Next**.
20. On the **Upload Smart License Authorization Code File** page, upload the acknowledgement file that you downloaded from Cisco SSM.
21. Click **Summary**.

    The process of loading and assigning licenses may take several minutes. You can monitor the progress by viewing the Cisco vManage task list.

After the HSEC licenses have been loaded and assigned, to install them, use the Install HSEC Licenses, on page 244 procedure.

Install HSEC Licenses

1. From the Cisco vManage menu, choose **Workflows** > **Workflow Library**.
2. Click the **Sync and Install HSEC Licenses** workflow.
3. Click **Install Devices**.
4. Select the desired devices on which to install an HSEC license.
5. Click **Install** to install the licenses.

   You can monitor the progress by viewing the Cisco vManage task list.

Verify HSEC License Installation

1. From the Cisco vManage menu, choose **Administration** > **License Management**.
2. Above the table click **Device**. The HSEC license information appears in two columns.

Column	Description
HSEC Compatible	**Yes** or **No** indicate HSEC compatibility.
HSEC Status	• **scheduled**: An HSEC license is pending installation on the device. • **success**: An HSEC license is installed on the device.

Preview Device Configuration and View Configuration Differences

For a configuration that you have created from the CLI:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and choose the desired device template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **...**, and click **Change Device Values**.

   The right pane displays the device's configuration, and **Config Preview** is selected.
4. Click the name of a device.

5. Click **Config Diff** to view the differences between this configuration and the configuration currently running on the device, if applicable. Click **Back** to edit the variable values entered in the previous screen.
6. Click **Configure Devices** to push the configuration to the devices. The Status column displays whether the configuration was successfully pushed. Click the right angle bracket to display details of the push operation.

Reset Interfaces

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation without having to modify the device's configuration.

1. From the Cisco vManage menu, choose **Tools** > **Operational Commands**.
2. For the desired template, click **…** and choose **Reset Interface**.
3. In the **Interface Reset** dialog box, choose the desired interface.
4. Click **Reset**.

Reset a Locked User

If a user is locked out after multiple password attempts, an administrator with the required rights can update passwords for this user.

There are two ways to unlock a user account, by changing the password or by getting the user account unlocked.

Note Only a **netadmin** user or a user with the User Management Write role can perform this operation.

To reset the password of a user who has been locked out:

1. In **Users** (**Administration** > **Manage Users**), choose the user in the list whose account you want to unlock.
2. Click **. . .** and choose **Reset Locked User**.
3. Click **OK** to confirm that you want to reset the password of the locked user. Note that this operation cannot be undone.

   Alternatively, you can click **Cancel** to cancel the operation.

Steps to Bring Up the Overlay Network

Bringing Up the Overlay Network

The following table lists the tasks for bringing up the overlay network using Cisco vManage.

Table 95:

Bring-Up Task	Step-by-Step Procedure
Step 1: Start the Cisco vManage.	1. On the hypervisor, create a VM instance. 2. Boot Cisco vManage server, start the VM, and enter login information. 3. From the Cisco vManage menu, choose **Administration** > **Settings**, configure certificate authorization settings. Select Automated to allow the certificate-generation process to occur automatically when a CSR is generated for a controller device. 4. From the Cisco vManage menu, choose **Configuration** > **Certificates**, generate the CSR. 5. Check for a confirmation email from Symantec that your request has been received. 6. Check for an email from Symantec that Viptela has approved your request and the certificate is signed. 7. From the Cisco vManage menu, choose **Configuration** > **Devices**, and check if the certificate has been installed.
Step 2: Start the Cisco vBond Orchestrator.	1. On the hypervisor, create a VM instance. 2. Boot the vBond server and start the VM. 3. From the Cisco vManage menu, choose **Configuration** > **Devices** > **Controllers**, add Cisco vBond Orchestrator and generate the CSR. 4. Check for a confirmation email from Symantec that your request has been received. 5. Check for an email from Symantec that Viptela has approved your request and the certificate is signed. 6. From the Cisco vManage menu, choose **Configuration** > **Devices**, and check if the certificate has been installed. 7. From the Cisco vManage menu, choose **Configuration** > **Templates**: a. Create a configuration template for the Cisco vBond Orchestrator. b. Attach the template to Cisco vBond Orchestrator. 8. From the Cisco vManage menu, choose **Monitor** > **Overview**, and verify that the Cisco vBond Orchestrator is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Dashboard** > **Main Dashboard**, and verify that the Cisco vBond Orchestrator is operational.

Bring-Up Task	Step-by-Step Procedure
Step 3: Start the Cisco vSmart Controller.	**1.** On the hypervisor, create a VM instance. **2.** Boot the vSmart server and start the VM. **3.** From the Cisco vManage menu, choose **Configuration** > **Devices** > **Controller**, add Cisco vSmart Controller and generate the CSR. **4.** Check for a confirmation email from Symantec that your request has been received. **5.** Check for an email from Symantec that Viptela has approved your request and the certificate is signed. **6.** From the Cisco vManage menu, choose **Configuration** > **Devices**, check that the certificate has been installed. **7.** From the Cisco vManage menu, choose **Configuration** > **Templates**: **a.** Create a configuration template for Cisco vSmart Controller. **b.** Attach the template to Cisco vSmart Controller. **8.** From the Cisco vManage menu, choose **Monitor** > **Overview**, and verify that Cisco vSmart Controller is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Dashboard** > **Main Dashboard**, and verify that Cisco vSmart Controller is operational.
Step 4: Configure the router.	**1.** From the Cisco vManage menu, choose **Configuration** > **Devices** > **WAN Edge List**, upload the router authorized serial number file. **2.** From the Cisco vManage menu, choose **Configuration** > **Certificates** > **WAN Edge List**, check that the router's chassis and serial number are in the list. **3.** From the Cisco vManage menu, choose **Configuration** > **Certificates** > **WAN Edge List**, authorize each router by marking it Valid in the Validity column. **4.** From the Cisco vManage menu, choose **Configuration** > **Certificates** > **WAN Edge List**, send the WAN Edge list to the controller devices. **5.** From the Cisco vManage menu, choose **Configuration** > **Templates**: **a.** Create a configuration template for the router. **b.** Attach the template to the router.

Bring-Up Task	Step-by-Step Procedure
Step 5: Connect AC power and boot a hardware router.	**1.** Connect AC power to the router. **2.** If needed, flip the On/Off switch on the rear of the router to the ON position. **3.** From the Cisco vManage menu, choose **Monitor** > **Overview** or choose **Monitor** > **Devices** > **Device Dashboard**, verify that the router is operational. Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Dashboard** > **Main Dashboard** or choose **Monitor** > **Network** > **Device Dashboard**, verify that the router is operational.

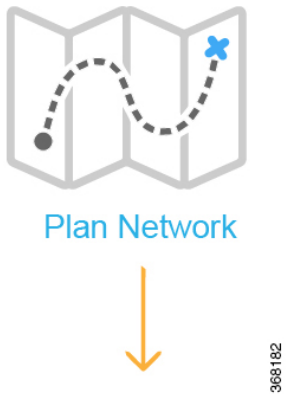
Summary of the User Portion of the Bring-Up Sequence

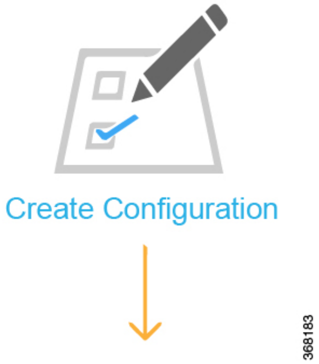
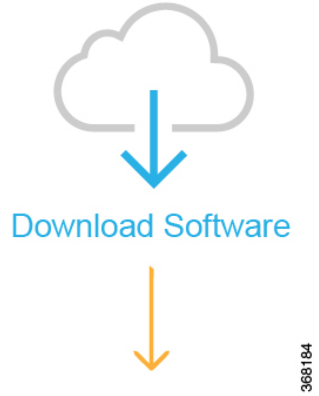
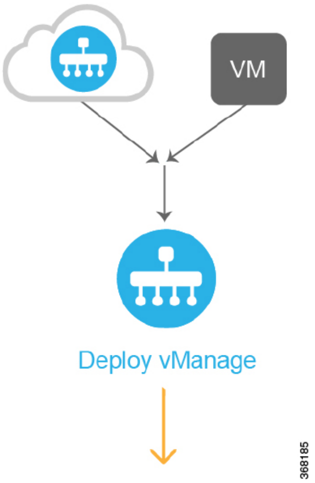
Generally, what you do to bring up the Cisco SD-WAN overlay network is what you do to bring up any network. You plan out the network, create device configurations, and then deploy the network hardware and software components. These components include all the Cisco vEdge devices, all the traditional routers that participate in the overlay network, and all the network devices that provide shared services across the overlay network, such as firewalls, load balancers, and IDP systems.

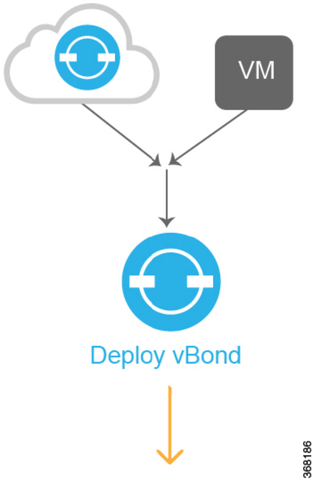
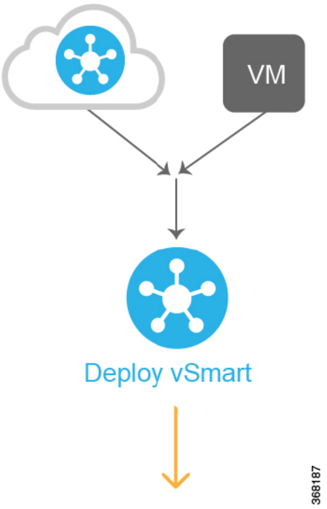
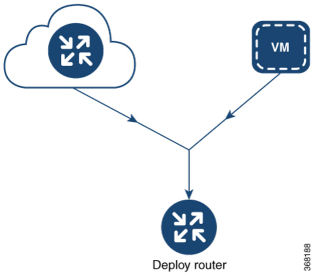
The following table summarizes the steps for the user portion of the Cisco SD-WAN overlay network bring-up sequence. The details of each step are provided in the articles that are listed in the **Procedure** column. While you can bring up the Cisco vEdge devices in any order, it is recommended that you deploy them in the order listed below, which is the functional order in which the devices verify and authenticate themselves.

If your network has firewall devices, see Firewall Ports for Cisco SD-WAN Deployments.

Table 96:

	Workflow	Procedure
1		Plan out your overlay network. See Components of the Cisco SD-WAN Solution.

	Workflow	Procedure
2		On paper, create device configurations that implement the desired architecture and functionality. See the Software documentation for your software release.
3		Download the software images.
4		Deploy Cisco vManage in the data center: **1.** Create a Cisco vManage VM instance, either on an ESXi or a KVM hypervisor. **2.** Create either a minimal or a full configuration for each Cisco vManage server. **3.** Configure certificate settings and generate a certificate for Cisco vManage. **4.** Create a Cisco vManage cluster.

	Workflow	Procedure
5		Deploy the Cisco vBond Orchestrator: 1. Create a Cisco vBond Orchestrator VM instance, either on an ESXi or a KVM hypervisor. 2. Create a minimal configuration for the Cisco vBond Orchestrator. 3. Add the Cisco vBond Orchestrator to the overlay network. During this process, you generate a certificate for the Cisco vBond Orchestrator. 4. Create a full configuration for the Cisco vBond Orchestrator.
6		Deploy the Cisco vSmart Controller in the data center: 1. Create a Cisco vSmart Controller VM instance, either on an ESXi or a KVM hypervisor. 2. Create a minimal configuration for the Cisco vSmart Controller. 3. Add the Cisco vSmart Controller to the overlay network. During this process, you generate a certificate for the Cisco vSmart Controller. 4. Create a full configuration for the Cisco vSmart Controller.
7		Deploy the Cisco vEdge routers in the overlay network: 1. For software vEdge Cloud routers, create a VM instance, either on an AWS server, or on an ESXi or a KVM hypervisor. 2. For software vEdge Cloud routers, send a certificate signing request to Symantec and then install the signed certificate on the router. 3. From Cisco vManage, send the serial numbers of all Cisco vEdge routers to the Cisco vSmart Controller and Cisco vBond Orchestrators in the overlay network. 4. Create a full configuration for the Cisco vEdge routers.

Use Variable Values in Configuration Templates

An overlay network might have multiple devices of the same type that have nearly identical configurations. This situation most commonly occurs with routers when the routers that are located in multiple stores or branch locations provide identical services, but each individual router has its own hostname, IP address, GPS location, and other site-specific properties, such as BGP neighbors. This situation also occurs in a network with redundant controller devices, such as Cisco vSmart Controllers, which must all be configured with identical policies, and Cisco vManage systems. Again, each controller has its own individual parameters, such as hostname and IP address.

To simplify the configuration process for these devices, you can create a single configuration template that contains both static configuration values and variable values. The static values are common across all the devices, and the variable values apply only to an individual device. You provide the actual values for the variables when you attach the individual device to the device configuration template.

You can configure a variable value for a parameter in a feature configuration template in two ways:

- Select the parameter scope to be Device Specific—For an individual configuration parameter, select Device Specific to mark the parameter as a variable. Each variable must be identified by a unique text string, which is called a *key*. When you select Device Specific, an Enter Key box opens and displays the default key. You can use the default key, or you can change it by typing a new string and then moving the cursor out of the Enter Key box.

- Mark a group of related parameters as optional—For some features in some feature configuration templates, you can mark the entire feature as optional. To mark the feature in this way, click Mark as Optional Row in a section of a feature configuration template. The variable parameters are then dimmed, and you cannot configure values for them in the feature configuration template.

You enter the device-specific values for the variables when you attach the device to the configuration, in one of the following ways:

- From a file—When you are attaching a template to a device, you load a file to the vManage NMS. This is an Excel file in CSV format that lists all the variables and defines the variable's value for each device.

- Manually—When you attach a device template to a device, the Cisco vManage prompts you for the values for each of device-specific parameters, and you type in the value for each parameter.

Note Cisco SD-WAN supports up to 500 variables in a template push operation.

Use a File for Variable Parameters

To load device-specific variable values from a file, you create a template variables file. This file is an Excel file in CSV format that lists all the variables in your the configurations of your devices and defines the values for each variable. You create this file offline and then import it into Cisco vManage server when you attach a device configuration to one or more devices in the overlay network.

We recommend that you create a template variables CSV file when your overlay network has more than a small number of Cisco vEdge devices.

CSV File Format

The CSV file is an Excel spreadsheet that contains one column for each variable that is required for the configuration of a device. The header row contains the variable names (one variable per column), and each row after that corresponds to a device and defines the values of the variables for that device.

You can create a single spreadsheet for all devices in the overlay network—Cisco vEdge devices, Cisco vManage systems, Cisco vSmart Controllers, and Cisco vBond Orchestrators—or you can create one spreadsheet for each device type. The system determines the device type from its serial number.

In the spreadsheet, for each device type and for each individual device, you specify values only for the required variables. When you do not need to specify a value for a variable, simply leave that cell blank.

The first three columns in the spreadsheet must be the following items and must be in the order shown:

Column	Column Heading	Description
1	csv-deviceId	Serial number of the device (used to uniquely identify the device). For Cisco vEdge devices, you receive the serial numbers in the authorized serial number file sent to you from Cisco. For other devices, the serial number is included in the signed certificate you receive from Symantec or from your root CA.
2	csv-deviceIP	System IP address of the device (used to populate the **system ip address** command).
3	csv-host-name	Hostname of the device (used to populate the **system hostname** command).

The headings for the remaining columns must be unique variable keys that are defined in the Enter Key box of a feature configuration template. These remaining columns can be in any order.

Generate a Skeleton CSV File

You can create a template variables CSV file manually, with the format described in the previous section, or you can haveCisco vManage generate a skeleton CSV file that contains all the required columns and column headings. This generated CSV file has one row for each Cisco device type, and it has the column headings for each of the variables that are required by all the feature templates included in the device configuration. The column heading text corresponds to the key string that identifies a device-specific parameter. Then you populate the rows with values for each variable.

To have Cisco vManage generate a skeleton CSV file:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and click **Add Template**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Create the required feature templates for one Cisco vEdge device router, one Cisco vSmart Controller, one Cisco vManage system, and one Cisco vBond Orchestrator.

In each feature template:

a. For fields that have default values, verify that you want to use that value for all devices. If you do not want to use the default, change the scope to **Global** or **Device-specific**.

b. For fields that apply to all devices, select the **Global** icon next to the field and set the desired global values.

c. For fields that are device specific, select the **Device-specific** icon next to the field and leave the field blank.

4. For each Cisco device type, create a device template.
5. From the Cisco vManage menu, choose **Configuration** > **Templates**.
6. Click **Device Templates**, and select the desired device template from the template list table.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

7. Click **…**, and click **Export CSV**.
8. Repeat Steps 7 and 8 for each device template.

Edit the exported CSV file, adding at a minimum the device serial number, device system IP address, and device hostname for each device in the overlay network. Then add values for desired device-specific variables for each device. Note that variable names cannot contain forward slashes (/), backwards slashes (\), or parentheses (( )).

If desired, you can combine the CSV files into a single file.

Import a CSV File

To use the device-specific variable values in the CSV file, import the file when you are attaching a device template to the Viptela device:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. For the desired template, click **...**, and select **Attach Devices**.
4. In the **Attach Devices** dialog box, select the desired devices in **Available Devices** and click the arrow to move them to **Selected Devices**.
5. Click **Attach**.
6. Click the Up arrow. The Upload CSV File box displays.
7. Choose the CSV file to upload, and click **Upload**.

During the attachment process, click Import file to load the Excel file. If Cisco vManage detects duplicate system IP addresses for devices in the overlay network, it displays a warning message or a pop-up window. You must correct the system IP addresses to remove any duplicates before you can continue the process of attaching device templates to Viptela devices.

Manually Enter Values for Device-Specific Variables and for Optional Rows

For parameters in a feature template that you configure as device-specific, when you attach a device template to a device, Cisco vManage prompts you for the values to use for these parameters. Entering device-specific values in this manner is useful in test or POC networks, or if you are deploying a small network. This method generally does not scale well for larger networks.

For situations in which the configuration for many devices is identical except for a few parameters, in the feature configuration template, you can specify that the parameter be an optional row in the configuration. By selecting optional row, the feature template automatically marks the parameters as device-specific, and these parameters are dimmed so that you cannot set them in the template. You do not have to individually mark the parameters as device specific. Then, when you attach a device template to a device, Cisco vManage prompts you for the values to use for these parameters. Using optional rows to enter device-specific values is useful when a group of many Cisco vEdge devices provide identical services at their branch or site, but individual routers have their own hostname, IP address, GPS location, and other site or store properties, such as BGP neighbors.

Optional rows are available for some parameters in some feature configuration templates. To treat a parameter or set of parameters as an optional row, click the **Mark as Optional Row** box. For these types of parameters, the feature configuration template has a table listing all the configured parameters. The Optional column indicates which are optional rows,

To manually enter values for device-specific variables or for variables in optional rows when you attach the template to a device:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and select the desired device template.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Attach Devices**. The **Attach Devices** dialog box opens.
4. Choose one or more devices from **Available Devices** and move them to **Selected Devices**.
5. Click **Attach**.
6. In the **Chassis Number** list, select the desired device.
7. Click **…**, and click **Edit Device Template**. The **Update Device Template** dialog box opens.
8. Enter values for the optional parameters. When you are using optional rows, if you do not want to include the parameter for the specific device, do not specify a value.
9. Click **Update**.
10. Click **Next**.

If any devices have the same system IP address, a dialog box appears or an error message is displayed when you click **Next**. Modify the system IP addresses so that there are no duplicates, and click **Save**. Then click **Next** again.

Note You need to shut down the OMP on the device, before changing the system-ip on the device.

11. In the left pane, select the device. The right pane displays the device configuration and the **Config Preview** tab in the upper right corner is selected.
12. Click **Config Diff** to preview the differences between this configuration and the configuration currently running on the device, if applicable. To edit the variable values entered in the previous screen, click **Back**.
13. Click **Configure Devices** to push the configuration to the devices.

    The Status column displays whether the configuration was successfully pushed. Click the **right angle bracket** to the left of the row to display details of the push operation.

Upgrade the Software Image on a Device

Note

- This procedure does not enable downgrading to an older software version. If you need to downgrade, see Downgrade a Cisco vEdge Device to an Older Software Image in the Cisco SD-WAN Getting Started Guide.
- If you want to perform a vManage cluster upgrade see, Upgrade Cisco vManage Cluster.
- Starting from Cisco vManage Release 20.1.1, before upgrading the configuration database, ensure that you verify the database size. We recommend that the database size is less than or equal to 5 GB. To verify the database size, use the following diagnostic command:

  request nms *configuration-db diagnostics*

To upgrade the software image on a device:

1. From the Cisco vManage menu, choose **Maintenance** > **Software Upgrade**.
2. Click **WAN Edge**, **Controller**, or **vManage** based on the type of device for which you wish to upgrade the software.
3. In the table of devices, select the devices to upgrade by selecting the check box on the far left.

   Note While upgrading Cisco vManage clusters, select all the nodes of the cluster in the table.

4. Click **Upgrade**.
5. In the **Software Upgrade** slide-in pane, do as follows:

a. Choose the server from which the device should download the image: **vManage**, **Remote Server**, or **Remote Server – vManage**.

Note

- The Remote Server option is introduced in Cisco vManage Release 20.7.1. If you chose **Remote Server**, ensure that the device can reach the remote server.
- Starting from Cisco vManage Release 20.9.1, when downloading an image from a remote server manually, ensure that only the following valid characters are used:
    - User ID: a-z, 0-9, ., _, -
    - Password: a-z, A-Z, 0-9, _, *, ., +, =, %, -
    - URL Name or Path: a-z, A-Z, 0-9, _, *, ., +, =, %, -, :, /, @, ?, ~

b. For **vManage**, choose the image version from the **Version** drop-down list.

c. For **Remote Server – vManage**, choose the **vManage OOB VPN** from the drop-down list and choose the image version from the **Version** drop-down list.

d. For **Remote Server**, configure the following:

Remote Server Name	Choose the remote server that has the image.
Image Filename	Choose the image filename from the drop-down list.

e. Check the **Activate and Reboot** check box.

If you do not check this check box, the software image is downloaded and installed on the device, but, the image is not activated, and the device is not rebooted. You must activate the image after the upgrade task is completed.

f. Click **Upgrade**.

The device restarts, using the new software version, preserving the current device configuration. The **Task View** page opens, showing the progress of the upgrade on the devices.

6. Wait for the upgrade process, which takes several minutes, to complete. When the **Status** column indicates Success, the upgrade is complete.

7. From the Cisco vManage menu, choose **Maintenance** > **Software Upgrade** and view the devices.

8. Click **WAN Edge**, **Controller**, or **vManage** based on the type of device for which you wish to upgrade the software.

9. In the table of devices, confirm that the **Current Version** column for the upgraded devices shows the new version. Confirm that the **Reachability** column says reachable.

Note

- If the control connection to Cisco vManage does not come up within the configured time limit, Cisco vManage automatically reverts the device to the previously running software image. The configured time limit for all Cisco SD-WAN devices to come up after a software upgrade is 5 minutes, except for Cisco vEdge devices, which have a default time of 12 minutes.
- If you upgrade the Cisco vEdge device software to a version higher than that running on a controller device, a warning message is displayed that software incompatibilities might occur. It is recommended that you upgrade the controller software first before upgrading the Cisco vEdge device software.
- When upgrading a Cisco CSR1000V or Cisco ISRv device to Cisco IOS XE Release 17.4.1a or later, the software upgrade also upgrades the device to a Cisco Catalyst 8000V. After the upgrade, on the Devices page, the **Chassis Number** and **Device Model** columns show the device as a Cisco CSR1000V or Cisco ISRv, but the device has actually been upgraded to a Cisco Catalyst 8000V. The reason for preserving the old name is to avoid invalidating licenses, and so on. To confirm that the device has been upgraded to a Cisco Catalyst 8000V, note that the **Current Version** column for the device indicates 17.4.1 or later.

Upload WAN Edge Router Authorized Serial Number File

The WAN eEdge router authorized serial number file contains the chassis number and the certificate serial numbers of all valid Cisco vEdge devices in the overlay network. You retrieve a serial number file from the Cisco Plug-and-Play (PnP) portal and upload it to Cisco vManage. (For more information abou Cisco PnP, see Cisco Plug and Play Support Guide for Cisco SD-WAN Products.) From Cisco vManage, you send the file to the controllers in the network. This file is required to allow the Cisco SD-WAN overlay network components to validate and authenticate each other and to allow the overlay network to become operational.

To upload the WAN edge router authorized serial number file to Cisco vManage and then download it to controllers in the network:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List**, and click **Upload WAN Edge List**.
3. Under **Upload WAN Edge List** screen:
   a. Click **Choose File** and select the WAN edge router authorized serial number file you received from Cisco PnP.
   b. To automatically validate the routers and send their chassis and serial numbers to the controllers, ensure that the **Validate the uploaded vEdge List and send to controllers** check box is selected. If you do not select this option, you must individually validate each router in **Configuration** > **Certificates** > **WAN Edge List**.
   c. Click **Upload**.

A list of routers in the network is displayed in the router table, with details about each router.

Starting from Cisco vManage Release 20.9.2, you can monitor the newly added WAN Edge devices in the **Monitor** > **Devices** page.

Upload WAN Edge Router Serial Numbers from Cisco Smart Account

To allow Cisco SD-WAN overlay network components to validate and authenticate each other and to allow the overlay network to become operational, Cisco SD-WAN requires chassis numbers of all valid Cisco vEdge devices in the overlay network.

In addition, certificate serial numbers, are required for all devices.

To upload the WAN edge router authorized serial numbers from a Cisco Smart account to the vManage NMS and then download it to all the controllers in the overlay network:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List**, and click **Sync Smart Account**.
3. In the **Sync Smart Account** window:
    a. Enter the **Username** and **Password** for your Smart account.
    b. To automatically validate the routers and send their chassis and serial numbers to the controllers, check the **Validate the Uploaded WAN Edge List and Send to Controllers** check box. If you do not select this option, you must individually validate each router in **Configuration** > **Certificates** > **WAN Edge List**.
    c. Click **Sync**.

A list of routers in the network is displayed in the router table, with details about each router.

Starting from Cisco vManage Release 20.9.2, you can monitor the newly added WAN Edge devices in the **Monitor** > **Devices** page.

View and Copy Device Configuration

View a Device's Running Configuration

Running configuration is configuration information that vManage obtains from the memory of a device. This information can be useful for troubleshooting.

To view a device's running configuration:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List** or **Controllers**, and select the device.
3. Click **…**, and click **Running Configuration**.

View a Device's Local Configuration

Local configuration is configuration that vManage has stored for a device. This information can be useful for troubleshooting or for determining how to access a device if, for example, a device is not reachable from vManage.

To view a device's local configuration created using Configuration ► Templates:

1. From the Cisco vManage menu, choose **Configuration** > **Devices**.
2. Click **WAN Edge List** or **Controllers**, and select the device.
3. Click **…**, and click **Local Configuration**.

Copy Router Configuration

When you are replacing one router at a site with another router, you copy the old router's configuration to the new router. Then you remove the old router from the network and add the new one.

To copy the configuration from the old router to the new router:

1. From the Cisco vManage menu, choose **Configuration** > **Certificates**.
2. Mark the new Cisco vEdge device as invalid.
3. From the Cisco vManage menu, choose **Configuration** > **Devices**.
4. Under **WAN Edge List**, select the old router.
5. Click **…**, and click **Copy Configuration**.
6. In the **Copy Configuration** window, select the new router.
7. To confirm the copy of the configuration, click **Update**.

After you have copied the configuration to the new router, you can add the new router to the network. First, delete the old router from the network, as described below. Then add the new router to the network:

1. From the Cisco vManage menu, choose **Configuration** > **Certificates**.
2. Mark the new router as valid.
3. Click **Send to Controller**.

View Device Templates

View a Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** or **Feature Templates**, and select a template you wish to view.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**, and **Feature Templates** is titled **Feature**.

3. Click **…**, and then click **View**.

View Device Templates Attached to a Feature Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**, and select a template you wish to view.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **…**, and click **Show Attached Device Templates**.

   Device Templates dailog box opens, displaying the names of the device templates to which the feature template is attached.

View Devices Attached to a Device Template

For a device template that you created from feature templates:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and select a template you wish to view.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and click **Attach Devices**.
4. From **Attach Devices**, click **Attached Devices**.

For a device template that you created from a CLI template:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**, and select a template you wish to view.

Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. Click **…**, and then click **Show Attached Devices**.

Web Server Certificate for Cisco vManage

To establish a secure connection between your web browser and the Cisco vManage server using authentication certificates, you must generate a CSR to create a certificate, have it signed by a root CA, and then install it. You must install a separate certificate on each Cisco vManage server in a cluster by performing the following steps for each server:

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. In the **Web Server Certificate** area, click **CSR**.

3. In the **Common Name** field, enter the domain name or IP address of the Cisco vManage server. For example, the fully-qualified domain name of Cisco vManage could be vmanage.org.local.
4. In the **Organizational Unit** field, enter the unit name within your organization — for example, Network Engineering.
5. In the **Organization** field, enter the exact name of your organization as specified by your root CA — for example, Viptela Inc.
6. In the **City** field, enter the name of the city where your organization is located — for example, San Jose.
7. In the **State** field, enter the state in which your city is located — for example, California.
8. In the **2-Letter Country Code** field, enter the two-letter code for the country in which your state is located. For example, the two-letter country code for the United States of America is US.
9. Click **Validity** and choose the validity period for the certificate.
10. Optionally, in the **Subject Alternative Name (SAN) DNS Names** field, enter the names of DNS severs to which the certificate trust should be extended. If you enter more than one DNS server name, separate each name with a space or a comma.

Note Cisco SD-WAN supports SAN DNS names, from Cisco IOS XE SD-WAN release 16.11 and Cisco SD-WAN release 19.1.

11. Optionally, in the **Subject Alternative Name (SAN) URIs** field, enter the URIs of resources to which the certificate trust should be extended. If you enter more than one URI, separate each URI with a space or a comma.

    Enter each URI in *scheme***:***value* format, where *scheme* is the protocol for accessing the resource and *value* is the resource. For example, **`https://example.example.com`** or **`scp://example.example.com`**.

Note Cisco SD-WAN supports SAN URIs beginning with Cisco IOS XE SD-WAN release 16.11 and Cisco SD-WAN release 19.1.

12. Click **Generate** to generate the CSR.
13. Send the CSR to your CA server to have it signed.
14. When you receive the signed certificate, click **Certificate** near the **Web Server Certificate** bar to install the new certificate. The **View** box displays the current certificate on the Cisco vManage server.
15. Copy and paste the new certificate in the box. Alternatively, click **Import** and **Select a File** to download the new certificate file.
16. Restart the application server and log in to Cisco vManage.

View Web Server Certificate Expiration Date

When you establish a secure connection between your web browser and the Cisco vManage server using authentication certificates, configure the time period for which the certification is valid (in Step 8 in the previous section). At the end of this time period, the certificate expires. The **Web Server Certificate** bar shows the expiration date and time.

Starting 60 days before the certificate expires, the Cisco vManage dashboard displays a notification indicating that the certificate will expire soon. This notification is then displayed again 30, 15, and 7 days before the expiration date, and then daily.

Workflow to Configure IPv4 Static Route Tracking

Table 97: Feature History

Feature Name	Release Information	Description
Static Route Tracker for Service VPNs for Cisco vEdge Devices	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	To configure Static Route Tracking on Cisco vManage, configure an endpoint tracker using Cisco System template, and Configure a static route using the Cisco VPN template.
TCP/UDP Endpoint Tracker and Dual Endpoint Static Route Tracker for Cisco vEdge devices	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	You can now configure static route tracker with TCP/UDP endpoint using Cisco system template, and configure a static route using the Cisco VPN template. You can then add the configured dual trackers in a tracker group using **New Endpoint Tracker Groups** option.

1. Configure an endpoint tracker using the System template.
2. Configure a static route using the VPN template.
3. Apply the tracker to the next-hop address.

Create a Static Route Tracker

Use the **System Template** to create a tracker for static routes.

1. From Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Navigate to the **Cisco System** template for the device.

Note For information about creating a System template, see Create System Template.

4. Click **Tracker**. Click **New Endpoint Tracker** to configure the tracker parameters.

Table 98: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
Threshold	Wait time for the probe to return a response before declaring that the configured endpoint is down. Range is from 100 to 1000 milliseconds. Default is 300 milliseconds.
Interval	Time interval between probes to determine the status of the configured endpoint. Default is 60 seconds (1 minute). Range is from 10 to 600 seconds.
Multiplier	Number of times probes are sent before declaring that the endpoint is down. Range is from 1 to 10. Default is 3.
Tracker Type	From the drop-down, choose Global. From the Tracker Type field drop-down, choose Static Route. From Cisco SD-WAN Release 20.7.1, you can configure a tracker group with dual endpoints on Cisco vEdge devices and associate this tracker group to a static route.
Endpoint Type	Choose endpoint type IP Address.
End-Point Type: IP Address	IP address of the static route end point. This is the destination on the internet to which the router sends probes to determine the status of the route.

5. Click **Add**.

6. Click **Save**.

7. To create a tracker group, click **New Endpoint Tracker**.

   From the **Tracker Type** drop-down list, choose **tracker-group** and configure the tracker group parameters.

Note Ensure that you have created two trackers to form a tracker group.

Table 99: Tracker Group Parameters

Fields	Description
Name	Name of the tracker group.

Fields	Description
Tracker Type	From the drop-down, choose **Global**. From the Tracker Type field drop-down, choose **Static Route**. From Cisco SD-WAN Release 20.7.1, you can configure a tracker group with dual endpoints on Cisco vEdge devices and associate this tracker group to a static route.
Tracker Elements	This field is displayed only if you chose **Tracker-group** as the tracker type. Add the existing interface tracker names (separated by a space). When you add this tracker to the template, the tracker group is associated with these individual trackers, and you can then associate the tracker group to a static route.
Tracker Boolean	From the drop-down list, choose **Global**. This field is displayed only if you chose **tracker-group** as the **Tracker Type**. By default, the **OR** option is selected. Choose **AND** or **OR**. **OR** ensures that the static route status is reported as active if either one of the associated trackers of the tracker group report that the route is active. If you select **AND**, the static route status is reported as active if both the associated trackers of the tracker group report that the route is active.

8. Click **Add**.
9. Click **Save**.

Note Complete all the mandatory actions before you save the template.

Configure a Next Hop Static Route with Tracker

Use the **VPN** template to associate a tracker to a static route next hop.

Note You can apply only one tracker per static route next hop.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Navigate to the **Cisco VPN Template** for the device.

Note For information about creating a VPN template, see Create VPN Template.

4. Enter **Template Name** and **Description** as required.
5. In Basic Configuration, by default, VPN is set to 0. Set a VPN value within (1–511, 513–65530) range for service VPNs, for service-side data traffic on Cisco IOS XE SD-WAN devices.

Note You can configure static route tracker only on service VPNs.

6. Click **IPv4 Route**.
7. Click **New IPv4 Route**.
8. In the **IPv4 Prefix** field, enter a value.
9. Click **Next Hop**.
10. Click **Add Next Hop** and enter values for the fields listed in the table.

Parameter Name	Description
Address	Specify the next-hop IPv4 address.
Distance	Specify the administrative distance for the route.
Tracker	Enter the name of the gateway tracker to determine whether the next hop is reachable before adding that route to the route table of the device.
Add Next Hop	Enter the name of the gateway tracker with the next hop address to determine whether the next hop is reachable before adding that route to the route table of the device.

11. Click **Add** to create the static route with the next-hop tracker.

Note Configuring a static route with a next-hop 'X.X.X.255' is not supported.

Cisco vEdge device does not implement RFC 3021.

12. Click **Save**.

Note You need to fill all the mandatory fields in the form to save the VPN template.

Monitor Static Route Tracker Configuration

View Static Route Tracker

To view information about a static tracker on a transport interface:

1. From the Cisco vManage menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor** > **Network**.

2. Choose a device from the list of devices.
3. Click **Real Time**.
4. From the **Device Options** drop-down list, choose **Static Route Tracker Info**.

Verify Static Route Tracking Configuration Using CLI

Command Verification

Use the following command to verify if the configuration is committed. The following sample configuration shows tracker definition for a static route tracker and it's application to an IPv4 static route:

```
Device# show running-config system tracker
system
 tracker tracker1
 endpoint-ip 10.1.1.1
 interval 60
 multiplier 5
 tracker-type static-route

 tracker tracker2
 endpoint-ip 10.1.1.12
 interval 40
 multiplier 2
 tracker-type static-route
```

Use the following command to verify the IPv4 route:

```
Device# show running-config vpn 1 ip route

vpn 1
 ip route 10.20.30.0/24 10.20.30.1
 ip route 192.168.2.0/16 10.20.24.16 100
 ip route 192.168.2.0/16 10.20.24.17 tracker tracker1
!
```

The following is a sample output from the **show tracker static-route** command displaying individual static route tracker status:

```
Device#  show tracker static-route
TRACKER                RTT IN
NAME      VPN  STATUS  MSEC
--------------------------------
tcp-10001  1    UP      0
udp-10002  1    UP      0
```

The following is a sample output from the **show tracker static-route-group** command displaying tracker group status:

```
Device# show tracker static-route-group
                                                 TRACKER     TRACKER  TRACKER
                                                 ELEMENT     ELEMENT  ELEMENT
TRACKER NAME                VPN  BOOLEAN  STATUS  NAME       STATUS   RTT
----------------------------------------------------------------------------------
group-tcp-10001-udp-10002    1    and      UP     tcp-10001    UP       0
                                                  udp-10002    UP       0
```

The following is a sample output from the **show ip route static** command:

```
Device# show ip route static
 Codes Proto-sub-type:
  IA -> ospf-intra-area, IE -> ospf-inter-area,
  E1 -> ospf-external1, E2 -> ospf-external2,
  N1 -> ospf-nssa-external1, N2 -> ospf-nssa-external2,
  e -> bgp-external, i -> bgp-internal
Codes Status flags:
  F -> fib, S -> selected, I -> inactive,
  B -> blackhole, R -> recursive, L -> import

                                         PROTOCOL  NEXTHOP      NEXTHOP   NEXTHOP

VPN  PREFIX          PROTOCOL  SUB TYPE  IF NAME     ADDR        VPN      TLOC IP   COLOR
 ENCAP  STATUS
------------------------------------------------------------------------------------------
1    192.168.2.0/16  STATIC      -         ge0/4   10.20.24.17    -        -        -
 -      F,S
1    192.168.2.0/16  STATIC      -         ge0/4   10.20.24.16    -        -        -
 -      F,S
```

Workflow to Configure RBAC for Policies

Table 100: Feature History

Feature Name	Release Information	Description
Role-Based Access Control By Resource Group	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	You can configure role-based access control (RBAC) based on sites or resource groups in Cisco vManage.
RBAC for Policies	Cisco vManage Release 20.6.1 Cisco SD-WAN Release 20.6.1	Configure RBAC for policies in Cisco vManage.
Co-Management: Granular Role-Based Access Control for Feature Templates	Cisco vManage Release 20.7.1	This feature introduces greater granularity in assigning RBAC permissions for template use. This enables you to give a tenant self-management of network configuration tasks. Network administrators and managed service providers can use this feature to assign permissions to their end customers.

Feature Name	Release Information	Description
Co-Management: Improved Granular Configuration Task Permissions	Cisco vManage Release 20.9.1	To enable a user to self-manage specific configuration tasks, you can assign the user permissions to perform specific configuration tasks while excluding other tasks. This feature introduces numerous new permission options, enabling fine granularity in determining which configuration task permissions to provide to a user. .
RBAC for Security Operations and Network Operations Default User Groups	Cisco vManage Release 20.9.1	This feature provides the following default user groups: • network_operations user group for non-security policies • security_operations user group for security policies RBAC for policies allows you to create users and user groups with the required read and write permissions for security and non-security policies. Users can perform configuration and monitoring actions only for the authorized policy type.

Minimum supported releases: Cisco SD-WAN Release 20.6.1 and Cisco vManage Release 20.6.1

To configure RBAC for policies, use the following workflow:

1. Create user groups with required Read or Write (R/W) access to selected control or data policies. For details on creating user groups, refer Create User Groups .
2. Create users and assign them to required user groups. Refer Create Users.
3. Create or modify or view policy configurations as required. For information about configuring policies, see Configure Centralized Policies Using Cisco vManage.

Manage Users

From the Cisco vManage menu, choose **Administration** > **Manage Users** to add, edit, view, or delete users and user groups.

Please note the following:

- Only a user logged in as the **admin** user or a user who has Manage Users write permission can add, edit, or delete users and user groups from Cisco vManage.
- Each user group can have read or write permission for the features listed in this section. Write permission includes Read permission.
- All user groups, regardless of the read or write permissions selected, can view the information displayed in the Cisco vManage Dashboard.

Table 101: User Group Permissions: Cisco IOS XE SD-WAN devices

Feature	Read Permission	Write Permission
Alarms	Set alarm filters and view the alarms generated on the devices on the **Monitor** > **Logs** > **Alarms** page. Cisco vManage Release 20.6.x and earlier: Set alarm filters and view the alarms generated on the devices on the **Monitor** > **Alarms** page.	No additional permissions.
Audit Log	Set audit log filters and view a log of all the activities on the devices on the **Monitor** > **Logs** > **Alarms** page and the **Monitor** > **Logs** > **Audit Log** page. Cisco vManage Release 20.6.x and earlier: Set audit log filters and view a log of all the activities on the devices on the **Monitor** > **Alarms** page and the **Monitor** > **Audit Log** page.	No additional permissions.
Certificates	View a list of the devices in the overlay network under **Configuration** > **Certificates** > **WAN Edge List**. View a certificate signing request (CSR) and certificate on the **Configuration** > **Certificates** > **Controllers** window.	Validate and invalidate a device, stage a device, and send the serial number of valid controller devices to the Cisco vBond Orchestrator on the **Configuration** > **Certificates** > **WAN Edge List** window. Generate a CSR, install a signed certificate, reset the RSA key pair, and invalidate a controller device on the **Configuration** > **Certificates** > **Controllers** window.
CLI Add-On Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the CLI add-on feature template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a CLI add-on feature template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Cloud OnRamp	View the cloud applications on the**Configuration** > **Cloud OnRamp for SaaS** and **Configuration** > **Cloud OnRamp for IaaS** window.	No additional permissions.
Cluster	View information about the services running on Cisco vManage, a list of devices connected to a Cisco vManage server, and the services that are available and running on all the Cisco vManage servers in the cluster on the **Administration** > **Cluster Management** window.	Change the IP address of the current Cisco vManage, add a Cisco vManage server to the cluster, configure the statistics database, edit, and remove a Cisco vManage server from the cluster on the **Administration** > **Cluster Management** window.
Colocation	View the cloud applications on the **Configuration** > **Cloud OnRamp for Colocation** window.	No additional permissions.
Config Group > **Device** > **Deploy** (Minimum supported release: Cisco vManage Release 20.9.1)	This permission does not provide any functionality.	Deploy a configuration onto Cisco IOS XE SD-WAN devices. **Note** To edit an existing feature configuration requires write permission for **Template Configuration**.
Device CLI Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the device CLI template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a device CLI template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Device Inventory	View the running and local configuration of devices, a log of template activities, and the status of attaching configuration templates to devices on the **Configuration** > **Devices** > **WAN Edge List** window. View the running and local configuration of the devices and the status of attaching configuration templates to controller devices on the **Configuration** > **Devices** > **Controllers** window.	Upload a device's authorized serial number file to Cisco vManage, toggle a device from Cisco vManage configuration mode to CLI mode, copy a device configuration, and delete the device from the network on the **Configuration** > **Devices** > **WAN Edge List** window. Add and delete controller devices from the overlay network, and edit the IP address and login credentials of a controller device on the **Configuration** > **Devices** > **Controllers** window.

Feature	Read Permission	Write Permission
Device Monitoring	View the geographic location of the devices on the **Monitor** > **Geography** window. View events that have occurred on the devices on the **Monitor** > **Logs** > **Events** page. Cisco vManage Release 20.6.x and earlier: View events that have occurred on the devices on the **Monitor** > **Events** page. View a list of devices in the network, along with device status summary, SD-WAN Application Intelligence Engine (SAIE) and Cflowd flow information, transport location (TLOC) loss, latency, and jitter information, control and tunnel connections, system status, and events on the **Monitor** > **Devices** page (only when a device is selected). **Note** In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow. Cisco vManage Release 20.6.x and earlier: Device information is available in the **Monitor** > **Network** page.	Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the **Monitor** > **Devices** page (only when a device is selected).
Device Reboot	View the list of devices on which the reboot operation can be performed on the **Maintenance** > **Device Reboot** window.	Reboot one or more devices on the **Maintenance** > **Device Reboot** window.
Disaster Recovery	View information about active and standby clusters running on Cisco vManage on the **Administration** > **Disaster Recovery** window.	No additional permissions.

Feature	Read Permission	Write Permission
Events	View the geographic location of the devices on the **Monitor** > **Logs** > **Events** page. View the geographic location of the devices on the **Monitor** > **Events** page.	Ping a device, run a traceroute, and analyze the traffic path for an IP packet on the **Monitor** > **Logs** > **Events** page (only when a device is selected).
Feature Profile > **Other** > **Thousandeyes** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **ThousandEyes** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Other Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **ThousandEyes** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Other Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Dhcp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **DHCP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **DHCP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Lan/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **LAN/VPN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **LAN/VPN** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Lan/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Ethernet Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Ethernet Interface** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Service** > **Lan/Vpn/Interface/Svi** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **SVI Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **SVI Interface** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Routing/Bgp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Routing/BGP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Routing/BGP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Routing/Ospf** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Routing/OSPF** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Routing/OSPF** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Service** > **Switchport** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Switchport** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Switchport** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Service** > **Wirelesslan** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wireless LAN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Service Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wireless LAN** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **Service Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Interface/Ethernet** > **Aaa** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **AAA** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **AAA** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Interface/Ethernet** > **Banner** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Banner** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Banner** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Basic** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Basic** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Basic** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **System** > **Bfd** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **BFD** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **BFD** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Global** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Global** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Global** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Logging** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Logging** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Logging** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Ntp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **NTP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **NTP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **System** > **Omp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **OMP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **OMP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **System** > **Snmp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **SNMP** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **System Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **SNMP** settings on the **Configuration** > **Templates** > **(Add or edit configuration group)** page, in the **System Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Cellular Controller** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Cellular Controller** settings on the **Configuration** > **Templates** > **(View a configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cellular Controller** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Cellular Profile** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Cellular Profile** settings on the **Configuration** > **Templates** > **(View a configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Cellular Profile** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Transport** > **Management/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Management VPN** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Management VPN** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Management/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Management Ethernet Interface** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Management VPN and Management Internet Interface** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Routing/Bgp** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **BGP Routing** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **BGP Routing** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Tracker** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Tracker** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Tracker** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.

Feature	Read Permission	Write Permission
Feature Profile > **Transport** > **Wan/Vpn** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Wan/Vpn/Interface/Cellular** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn/Interface/Cellular** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn/Interface/Cellular** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Feature Profile > **Transport** > **Wan/Vpn/Interface/Ethernet** (Minimum supported release: Cisco vManage Release 20.9.1)	View the **Wan/Vpn/Interface/Ethernet** settings on the **Configuration** > **Templates** > **(View configuration group)** page, in the **Transport & Management Profile** section. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, and delete the **Wan/Vpn/Interface/Ethernet** settings on the **Configuration** > **Templates** > **(Add or edit a configuration group)** page, in the **Transport & Management Profile** section. **Note** These operations require write permission for **Template Configuration**.
Integration Management	View information about controllers running on Cisco vManage, on the **Administration** > **Integration Management** window.	No additional permissions.
License Management	View license information of devices running on Cisco vManage, on the **Administration** > **License Management** window.	On the **Administration** > **License Management** page, configure use of a Cisco Smart Account, choose licenses to manage, and synchronize license information between Cisco vManage and the license server.

Feature	Read Permission	Write Permission
Interface	View information about the interfaces on a device on the **Monitor** > **Devices** > **Interface** page. Cisco vManage Release 20.6.x and earlier: View information about the interfaces on a device on the **Monitor** > **Network** > **Interface** page	Edit **Chart Options** to select the type of data to display, and edit the time period for which to display data on the **Monitor** > **Devices** > **Interface** page.
Manage Users	View users and user groups on the **Administration** > **Manage Users** window.	Add, edit, and delete users and user groups from Cisco vManage, and edit user group privileges on the **Administration** > **Manage Users** window.
Other Feature Templates (Minimum supported release: Cisco vManage Release 20.7.1)	View all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy all feature templates except the SIG feature template, SIG credential template, and CLI add-on feature template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**.
Policy	View the common policies for all Cisco vSmart Controllers or devices in the network on the **Configuration** > **Policies** window.	Create, edit, and delete the common policies for all Cisco vSmart Controllers or devices in the network on the **Configuration** > **Policies** window.
Policy Configuration	View the list of policies created and details about them on the **Configuration** > **Policies** window.	Create, edit, and delete the common policies for all theCisco vSmart Controllers and devices in the network on the **Configuration** > **Policies** window.
Policy Deploy	View the current status of the Cisco vSmart Controllers to which a policy is being applied on the **Configuration** > **Policies** window.	Activate and deactivate the common policies for all Cisco vManage servers in the network on the **Configuration** > **Policies** window.

Feature	Read Permission	Write Permission
RBAC VPN	View the VPN groups and segments based on roles on the **Monitor** > **VPN** page. Cisco vManage Release 20.6.x and earlier: View the VPN groups and segments based on roles on the **Dashboard** > **VPN Dashboard** page.	Add, edit, and delete VPNs and VPN groups from Cisco vManage, and edit VPN group privileges on the **Administration** > **VPN Groups** window.
Routing	View real-time routing information for a device on the **Monitor** > **Devices** > **Real-Time** page. Cisco vManage Release 20.6.x and earlier: View real-time routing information for a device on the **Monitor** > **Network** > **Real-Time** page.	Add command filters to speed up the display of information on the **Monitor** > **Devices** > **Real-Time** page.
Security	View the current status of the Cisco vSmart Controllers to which a security policy is being applied on the **Configuration** > **Security** window.	Activate and deactivate the security policies for all Cisco vManage servers in the network on the **Configuration** > **Security** window.
Security Policy Configuration	Activate and deactivate the common policies for all Cisco vManage servers in the network on the **Configuration** > **Security** > **Add Security Policy** window.	Activate and deactivate the security policies for all Cisco vManage servers in the network on the **Configuration** > **Security** > **Add Security Policy** window.
Session Management	View user sessions on the **Administration** > **Manage Users** > **User Sessions** window.	Add, edit, and delete users and user groups from Cisco vManage, and edit user sessions on the **Administration** > **Manage Users** > **User Sessions** window.
Settings	View the organization name, Cisco vBond Orchestrator DNS or IP address, certificate authorization settings, software version enforced on a device, custom banner on the Cisco vManage login page, and the current settings for collecting statistics on the **Administration** > **Settings** window.	Edit the organization name, Cisco vBond Orchestrator DNS or IP address, certificate authorization settings, software version enforced on a device, custom banner on the Cisco vManage login page, current settings for collecting statistics, generate a certificate signing request (CSR) for a web server certificate, and install a certificate on the **Administration** > **Settings** window.

Feature	Read Permission	Write Permission
SIG Template (Minimum supported release: Cisco vManage Release 20.7.1)	View the SIG feature template and SIG credential template on the **Configuration** > **Templates** window. **Note** This operation requires read permission for **Template Configuration**.	Create, edit, delete, and copy a SIG feature template and SIG credential template on the **Configuration** > **Templates** window. **Note** These operations require write permission for **Template Configuration**.
Software Upgrade	View a list of devices,the custom banner on Cisco vManage on which a software upgrade can be performed, and the current software version running on a device on the **Maintenance** > **Software Upgrade** window.	Upload new software images on devices, upgrade, activate, and delete a software image on a device, and set a software image to be the default image on devices on the **Maintenance** > **Software Upgrade** window.
System	View system-wide parameters configured using Cisco vManage templates on the **Configuration** > **Templates** > **Device Templates** window. **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.	Configure system-wide parameters using Cisco vManage templates on the **Configuration** > **Templates** > **Device Templates** window. **Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is called **Device**.
Template Configuration	View feature and device templates on the **Configuration** > **Templates** window.	Create, edit, delete, and copy a feature or device template on the **Configuration** > **Templates** window. **Note** Beginning with Cisco vManage Release 20.7.1, to create, edit, or delete a template that is already attached to a device, the user requires write permission for the Template Deploy option.
Template Deploy	View the devices attached to a device template on the **Configuration** > **Templates** window.	Attach a device to a device template on the **Configuration** > **Templates** window.

Feature	Read Permission	Write Permission
Tools	Use the **admin tech** command to collect the system status information for a device on the **Tools** > **Operational Commands** window.	Use the **admin tech** command to collect the system status information for a device, and use the **interface reset** command to shut down and then restart an interface on a device in a single operation on the **Tools** > **Operational Commands** window. Rediscover the network to locate new devices and synchronize them with Cisco vManage on the **Tools** > **Operational Commands** window. Establish an SSH session to the devices and issue CLI commands on the **Tools** > **Operational Commands** window.
vAnalytics	Launch vAnalytics on **Cisco vManage** > **vAnalytics** window.	No additional permissions.
Workflows	Launch workflow library from **Cisco vManage** > **Workflows** window.	No additional permissions.

RBAC User Group in Multitenant Environment

The following is the list of user group permissions for role-based access control (RBAC) in a multitenant environment:

- R stands for read permission.
- W stands for write permission.

Table 102: RBAC User Group in Multitenant Environment

Feature	Provider Admin	Provider Operator	Tenant Admin	Tenant Operator
Cloud OnRamp	RW	R	RW	R
Colocation	RW	R	RW	R
RBAC VPN	RW	R	RW	R
Security	RW	R	RW	R
Security Policy Configuration	RW	R	RW	R
vAnalytics	RW	R	RW	R

Add User

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**.
2. By default **Users** is selected. The table displays the list of users configured in the device.
3. To edit, delete, or change password for an existing user, click **…** and click **Edit**, **Delete**, or **Change Password** respectively.
4. To add a new user, click **Add User**.
5. Add **Full Name**, **Username**, **Password**, and **Confirm Password** details.
6. In the **User Groups** drop-down list, select the user group where you want to add a user.
7. In the **Resource Group** drop-down list, select the resource group.

Note This field is available from Cisco SD-WAN Release 20.5.1.

8. Click **Add**.

Delete a User

If a user no longer needs access to devices, you can delete the user. Deleting a user does not log out the user if the user is logged in.

To delete a user:

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**.
2. For the user you wish to delete, click **...**, and click **Delete**.
3. To confirm the deletion of the user, click **OK**.

Edit User Details

You can update login information for a user, and add or remove a user from a user group. If you edit the details of a user who is logged in, the changes take effect after the user logs out.

To edit user details:

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**.
2. For the user you wish to edit, click **...**, and click **Edit**.
3. Edit the user details.

   You can also add or remove the user from user groups.
4. Click **Update**.

Change User Password

You can update passwords for users, as needed. We recommend that you use strong passwords.

Before You Begin

If you are changing the password for an admin user, detach device templates from all Cisco vManage instances in the cluster before you perform this procedure. You can reattach the device templates after you complete this procedure.

To change a password for a user:

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**.
2. For the user you wish to change the password, click **...** and click **Change Password**.
3. Enter the new password, and then confirm it.

Note Note that the user, if logged in, is logged out.

4. Click **Done**.

Check Users Logged In to a Device Using SSH Sessions

1. From the Cisco vManage menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor** > **Network**.
2. Select the device you want to use under the **Hostname** column.
3. Click **Real Time**.
4. From **Device Options**, choose **AAA users** for Cisco IOS XE SD-WAN devices or **Users** for Cisco vEdge devices.

   A list of users logged in to this device is displayed.

Check Users Logged In to a Device Using HTTP Sessions

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**.
2. Click **User Sessions**.

   A list of all the active HTTP sessions within Cisco vManage is displayed, including, username, domain, source IP address, and so on.

Manage a User Group

Users are placed in groups, which define the specific configuration and operational commands that the users are authorized to view and modify. A single user can be in one or more groups. Cisco SD-WAN software provides standard user groups, and you can create custom user groups, as needed:

- **basic**: Includes users who have permission to view interface and system information.
- **netadmin**: Includes the admin user, by default, who can perform all operations on the Cisco vManage. You can add other users to this group.
- **operator**: Includes users who have permission only to view information.
- Minimum supported release: Cisco vManage Release 20.9.1

network_operations: Includes users who can perform non-security operations on Cisco vManage, such as viewing and modifying non-security policies, attaching and detaching device templates, and monitoring non-security data.

- Minimum supported release: Cisco vManage Release 20.9.1

  security_operations: Includes users who can perform security operations on Cisco vManage, such as viewing and modifying security policies, and monitoring security data.

Note: All user groups, regardless of the read or write permissions selected, can view the information displayed on the Cisco vManage Dashboard screen.

Delete a User Group

You can delete a user group when it is no longer needed. For example, you might delete a user group that you created for a specific project when that project ends.

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.
3. Click the name of the user group you wish to delete.

Note You cannot delete any of the default user groups—basic, netadmin, operator, network_operations, and security_operations.

4. Click **Trash** icon.
5. To confirm the deletion of the user group, click **OK**.

Edit User Group Privileges

You can edit group privileges for an existing user group. This procedure lets you change configured feature read and write permissions for the user group needed.

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**.
2. Click **User Groups**.
3. Select the name of the user group whose privileges you wish to edit.

Note You cannot edit privileges for the any of the default user groups—basic, netadmin, operator, network_operations, and security_operations.

4. Click **Edit**, and edit privileges as needed.
5. Click **Save**.

If an **admin** user changes the privileges of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

Managing Resource Groups

Minimum supported releases: Cisco IOS XE Release 17.5.1a and Cisco vManage Release 20.5.1

To configure Resource Groups:

1. From the Cisco vManage menu, choose **Administration** > **Resource Groups**. The table dispalys a list of resource groups that are configured in Cisco vManage.
2. To edit or delete a resource group, click **...**, and click **Edit** or **Delete**.
3. To add new resource group, click **Add Resource Group**.
4. Enter **Resource Group Name** and the **Description**.
5. Under **Site ID**, enter **Range** or **Select ID(S)** from the drop-down list to include in the resource group.
6. To add the resource group to a device, click **Add**.

To add Users:

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**. The Manage Users screen appears.
2. By default **Users** is selected. The table displays the list of users configured in the device.
3. To edit, delete, or change password for an existing user, click **...**, and click **Edit**, **Delete**, or **Change Password** respectively.
4. To add a new user, click **Add User**.
5. Add **Full Name**, **Username**, **Password**, and **Confirm Password** details.
6. From the **User Groups** drop-down list, select the user group where you want to add a user.
7. From the **Resource Group** drop-down list, select the resource group.

Note This field is available from Cisco SD-WAN Release 20.5.1.

8. Click **Add**.

Modify Policy Configurations

Minimum supported releases: Cisco SD-WAN Release 20.6.1 and Cisco vManage Release 20.6.1

1. Login to Cisco vManage with the new user details.
2. You can modify or update the configurations based on the requirement.

When you login to Cisco vManage with new user details, you can view only the user group components that are assigned to you. For more details on configuring policies, see Policies Configuration Guide for vEdge Routers

Assign Users to Configure RBAC for Policies

Minimum supported releases: Cisco SD-WAN Release 20.6.1 and Cisco vManage Release 20.6.1

To Assign User to Create or Modify a CFlowd Data Policy

To create a CFlowd user group:

1. From the Cisco vManage, choose **Administration** > **Manage Users**.
2. Click **User Groups** and **Add User Group**.
3. Enter **User Group Name**.

   For example, cflowd-policy-only.
4. Check the Read or Write check box against the CFlowD Policy feature that you want to assign to a user group.
5. Click **Add**.
6. You can view the new user group in the left navigation path. Click **Edit** to edit the existing read or write rules.
7. Click **Save**.

To create a CFlowd user:

1. In Cisco vManage, choose **Administration** > **Manage Users**.
2. Click **Users**.
3. Click **Add User**.
4. In the Add New User page, enter **Full Name**, **Username**, **Password**, and **Confirm Password** details.
5. Choose **cflowd-policy-only** from the **User Groups** drop-down.

   Allow the **Resource Group** to select the default resource group.
6. Click **Add**. You can view the new user in the Users window.
7. To edit the existing read or write rules for a user, click **Edit**.

To modify a Cflowd policy:

1. Login to Cisco vManage with the new user credentials.

   You can view access only to CFlowd Policies as your login is assigend to **cflowd-policy-only** user group.
2. You can create, modify, or update the configurations based on the requirement.

Verify Granular RBAC Permissions

Minimum supported release: Cisco vManage Release 20.7.1

Use this procedure to verify the permissions that you have configured for a user group.

1. From the Cisco vManage menu, choose **Administration** > **Manage Users**.

2. Click **User Groups**.
3. In the pane that displays the user groups, select a user group to display the read and write permissions assigned to the user group.
4. Scroll to the permissions that control template access to verify your configuration for the user group.

Workflow to Configure Route Leaking Using Cisco vManage

Table 103: Feature History

Feature Name	Release Information	Description
Route Leaking Between Transport VPN and Service VPNs	Cisco SD-WAN Release 20.3.1 Cisco vManage Release 20.3.1	You can configure route leaking between transport VPN and service VPNs using the **Global Route Leak** option under the VPN feature template.
Route Manipulation for Leaked Routes with OMP Administrative Distance	Cisco vManage Release 20.6.1 Cisco SD-WAN Release 20.6.1	You can configure route redistribution between the transport VPN and service VPNs using the **Global Route Leak** option under the VPN feature template.
Route Leaking between Inter-Service VPN	Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	You can configure to leak routes between the service VPNs at the same site using the **Route Leak** option in the Cisco vManage.

1. Configure and enable the Localized Policy and attach the Route Policy.
2. Configure and enable the Route Leaking feature between Global and Service VPN.
3. Configure and enable the Route Leaking feature between Service VPNs.
4. Attach the Service Side VPN Feature Template to the Device Template.

Configure Localized Route Policy

Configure Route Policy

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. Select **Localized Policy**.
3. From the **Custom Options** drop-down, under Localized Policy, select **Route Policy**.
4. Click **Add Route Policy**, and select **Create New**.
5. Enter a name and description for the route policy.
6. In the left pane, click **Add Sequence Type**.

7. In the right pane, click **Add Sequence Rule** to create a single sequence in the policy. Match is selected by default.
8. Select a desired protocol from the **Protocol** drop-down list. The options are: IPv4, IPv6, or both.
9. Click a match condition.
10. On the left, enter the values for the match condition.
11. On the right enter the action or actions to take if the policy matches.
12. Click **Save Match and Actions** to save a sequence rule.
13. If no packets match any of the route policy sequence rules, the default action is to drop the packets. To change the default action:
    a. Click **Default Action** in the left pane.
    b. Click the **Pencil** icon.
    c. Change the default action to **Accept**.
    d. Click **Save Match and Actions**.
14. Click **Save Route Policy**.

Add the Route Policy

1. From the Cisco vManage menu, choose **Configuration** > **Policies**.
2. Choose the **Localized Policy**.
3. Click **Add Policy**.
4. Click **Next** in the Local Policy Wizard until you arrive at the **Configure Route Policy** option.
5. Click **Add Route Policy** and choose **Import Existing**.
6. From the **Policy** drop-down choose the route policy that is created. Click **Import**.
7. Click **Next**.
8. Enter the **Policy Name** and **Description**.
9. Click **Preview** to view the policy configurations in CLI format.
10. Click **Save Policy**.

Attach the Localized Policy to the Device Template

Note The first step in utilizing the Localized Policy that was created previously is to attach it to the device template.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Device Templates** and select the desired template.

3. Click **…**, and click **Edit**.
4. Click **Additional Templates**.
5. From the **Policy** drop-down, choose the **Localized Policy** that is created.
6. Click **Update**.

Note Once the localized policy has been added to the device template, selecting the **Update** option immediately pushes a configuration change to all of the devices that are attached to this device template. If more than one device is attached to the device template, you will receive a warning that they are changing multiple devices.

7. Click **Next** and then **Configure Devices**.
8. Wait for the validation process and push configuration from Cisco vManage to the device.

Configure and Enable Route Leaking between Global and Service VPNs

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. To configure route leaking, click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is called **Feature**.

Do one of the following:

- To create a feature template:

  a. Click **Add Template**. Choose a device from the list of devices. The templates available for the selected device display in the right pane.

  b. Choose the **VPN** template from the right pane.

Note Route leaking can be configured on service VPNs only. Therefore, ensure that the number you enter in the **VPN** field under **Basic Configuration** is one of the following: 1—511 or 513—65530.

  For details on configuring various VPN parameters such as basic configuration, DNS, Virtual Router Redundancy Protocol (VRRP) tracking, and so on, see Configure a VPN Template. For details specific to the route leaking feature, proceed to Step c.

  c. Enter Template Name and Description for the feature template.

  d. Click **Global Route Leak** below the **Description** field.

  e. To leak routes from the transport VPN, click **Add New Route Leak from Global VPN to Service VPN**.

1. In the **Route Protocol Leak from Global to Service** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.

2. In the **Route Policy Leak from Global to Service** drop-down list, choose **Global**. Next, choose one of the available route policies from the drop-down list.

3. Click **Add**.

f. To leak routes from the service VPNs to the transport VPN, click **Add New Route Leak from Service VPN to Global VPN**.

1. In the **Route Protocol Leak from Service to Global** drop-down list, choose **Global** to choose a protocol. Otherwise, choose **Device-Specific** to use a device-specific value.

2. In the **Route Policy Leak from Service to Global** drop-down list, choose **Global**. Next, choose one of the available route policies from the drop-down list.

3. Click **Add**.

g. Click **Save/Update**. The configuration does not take effect till the feature template is attached to the device template.

h. To redistribute the leaked static routes to BGP or OSPF protocols, see one of the following:

- Configure BGP
- Configure OSPF

- To modify an existing feature template:

a. Choose a feature template you wish to modify.

b. Click **...** next to the row in the table, and click **Edit**.

c. Perform all operations from Step c of creating a feature template.

Note

- The configuration does not take effect till the Service VPN feature template is attached to the device template.

Attach the Service Side VPN Feature Template to the Device Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.

2. Click **Device Templates** and select the desired template.

3. Click **…**, and click **Edit**.

4. Click **Service VPN**.

5. Click **Add VPN**. Select the Service VPN feature template listed in the Available VPN Templates pane. Click right-shift arrow and add the template to Selected VPN Templates list.

6. Click **Next** once it moves from the left (Available VPN Templates) to the right side (Selected VPN Templates).
7. Click **Add**.
8. Click **Update**.
9. Click **Next** and then **Configure Devices**.
10. Finally, wait for the validation process and push configuration from Cisco vManage to the device.

Workflow to Configure VRRP Tracking

Table 104: Feature History

Feature Name	Release Information	Description
VRRP Interface Tracking for Cisco vEdge Devices	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	This feature enables VRRP to set the edge as active or standby based on the WAN Interface or SIG tracker events and increase the TLOC preference value on a new VRRP active to ensure traffic symmetry, for Cisco vEdge Devices.
VRRP Interface Tracking for Cisco vEdge Devices.	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	Starting this release, you can configure VRRP interface tracking through Cisco vManage feature template on Cisco vEdge Device.

1. Configure an object tracker. For more information, see Configure an Object Tracker, on page 293.
2. Configure VRRP for a VPN Interface template and associate the object tracker with the template. For more information, see Configure VRRP for a VPN Interface Template and Associate Interface Object Tracker, on page 294.

Configure an Object Tracker

Use the **System** template to configure an object tracker.

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature**.
3. Navigate to the **System** template for the device.

Note To create a **System** template, see Create System Template

4. Click **Tracker**, and click **New Object Tracker** to configure the tracker parameters.

Table 105: Tracker Parameters

Field	Description
Tracker Type	Choose Interface or SIG to configure the Object tracker.
Tracker List	Enter the name of the tracker list.
Interface	Choose global or device-specific tracker interface name.

5. Click **Add**.
6. Click **Save**.

Configure VRRP for a VPN Interface Template and Associate Interface Object Tracker

To configure VRRP for a **VPN** template, do the following:

1. From the Cisco vManage menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled **Feature**.

3. Navigate to the **VPN Interface Ethernet** template for the device.

Note For information about creating a new **VPN Interface Ethernet** template, see Configure VPN Ethernet Interface.

4. Click **VRRP** and choose **IPv4**.
5. Click **New VRRP** to create a new VRRP or edit the existing VRRP and configure the following parameters:

Parameter Name	Description
TLOC Preference Change	(Optional) Choose **On** or **Off** to set whether the TLOC preference can be changed or not.

6. Click the **Add Tracking Object** link, and in the **Tracking Object** dialog box that is displayed, click **Add Tracking Object**.
7. In the **Tracker Name** field, enter the name of the tracker.
8. From the **Action** drop-down list, choose **Decrement** and enter the **Decrement Value**.
9. Click **Add**.

10. Click **Add** to save the VRRP details.

11. Click **Save**.

Configure VRRP Tracking Using CLI Templates

You can configure VRRP tracking using the CLI add-on feature templates and CLI device templates. For more information, see CLI Templates.

VRRP Object Tracking Using CLI

Configure Track List Interface

Use the following configuration to add an interface to a track list using Cisco vManage device CLI tempale:

```
Device# config terminal
Device(config)# system
Device(config-system)# track-list zs1 interface ge0/1 gre1 ipsec1
Device(config-track-list-zs1)# commit
Device(config-system-tracker-list-zs1)# exit
Device(config-system)# exit
```

Configure Interface Tracking and Priority Decrement

```
Device(config)# vpn 1
Device(config-vpn-1)# name vpn-name
Device(config- vpn-1)# interface ge0/2
Device(config-interface-ge0/2)# ip address 172.16.10.1/24
Device(config-interface-ge0/2)# no shutdown
Device(config-interface-ge0/2)# vrrp 100
Device(config-vrrp-100)# track zs1 decrement 10
Device(config-vrrp-track-zs1)# exit
Device(config-vrrp-100)# ipv4 172.16.10.100
Device(config-vrrp-100)# tloc-change-pref
```

SIG Container Tracking

The following example shows how to configure a track list and tracking for SIG containers using the Cisco vManage device CLI template.

Note In SIG Object Tracking, you can only set *global* as the variable for Service Name.

Configure Track List for SIG Container

```
Device# config terminal
Device(config)# system
Device(config-system)# track-list SIG sig-container global
Device(config-system-tracker-list-SIG)# exit
Device(config-system)# exit
```

Configure SIG Container Tracking and Priority Decrement

```
Device(config)# vpn 1
Device(config-vpn-1)# name vpn-name
Device(config- vpn-1)# interface ge0/2
Device(config-interface-ge0/2)# ip address 172.16.10.1/24
Device(config-interface-ge0/2)# no shutdown
Device(config-interface-ge0/2)# vrrp 100
Device(config-vrrp-100)# track SIG decrement 10
Device(config-vrrp-track-zs1)# exit
Device(config-vrrp-100)# ipv4 172.16.10.100
Device(config-vrrp-100)# tloc-change-pref
```

Configure SIG Container Tracking for VRRP Group

```
Device(config-vpn-1)# int ge0/4
Device(config-interface-ge0/4)# vrrp 10
Device(config-vrrp-10)# track SIG decrement 10
Device(config-track-SIG)# commit
Commit complete.
Device(config-track-SIG)#
```