# Cisco SD-WAN Multitenancy

## Overview of Cisco SD-WAN Multitenancy

With Cisco SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco vManage. The tenants share the same set of underlying Cisco SD-WAN controllers: Cisco vManage, Cisco vBond Orchestrator, and Cisco vSmart Controller. The tenant data is logically isolated on these shared controllers.

The service provider accesses Cisco vManage using a domain name mapped to the IP address of a Cisco vManage cluster and manages the multitenant deployment. Each tenant is provided a subdomain to access a tenant-specific Cisco vManage view and manage the tenant deployment. For example, a service provider using the domain name `managed-sp.com`, can assign tenants Customer1 and Customer2 the subdomains `customer1.managed-sp.com` and `customer2.managed-sp.com` and manage them on the same set of Cisco SD-WAN controllers, instead of providing each customer a single-tenant setup with a dedicated set of Cisco SD-WAN controllers.

Following are the key features of Cisco SD-WAN multitenancy:

- Full enterprise multitenancy: Cisco SD-WAN supports multitenancy and offers enterprises the flexibility of segregated roles such as service provider and tenants. Service providers can use multitenancy to provide Cisco SD-WAN service offerings to their customers.
- Multi-tenant Cisco vManage
- Multi-tenant Cisco vBond Orchestrators
- Multi-tenant Cisco vSmart Controllers
- Tenant-specific WAN Edge Devices
- Overlapping VPN numbers: A particular VPN or a set of common VPNs is assigned to a specific tenant, with their own configurations and monitoring dashboard environment. These VPN numbers can overlap where they are used by other tenants.
- On-prem and cloud deployment models: Cisco SD-WAN controllers can be deployed in an organization data center on servers running the VMware ESXi 6.7 or later, or the Kernel-based Virtual Machine (KVM) hypervisor. Cisco SD-WAN controllers can also be hosted on Amazon Web Services (AWS) servers by Cisco CloudOps.
- Tenant-specific Cisco vAnalytics: Cisco vAnalytics is a cloud-based service that offers insights into the performance of applications and the underlying SD-WAN network infrastructure. Each tenant can obtain Cisco vAnalytics insights for their overlay network by requesting a tenant-specific Cisco vAnalytics instance and enabling data collection on Cisco vManage. The service provider must enable cloud services on Cisco vManage in the provider view to facilitate the onboarding of the Cisco vAnalytics instance for the tenant overlay network.

### Multi-tenant Cisco vManage

Cisco vManage is deployed and configured by the service provider. The provider enables multitenancy and creates a Cisco vManage cluster to serve tenants. Only the provider can access a Cisco vManage instance through the SSH terminal.

Cisco vManage offers service providers an overall view of the SD-WAN multi-tenant deployment and allows a provider to manage the shared Cisco vBond Orchestrator and Cisco vSmart Controller devices. Cisco vManage also allows service providers to monitor and manage the deployments of each tenant.

Cisco vManage allows tenants to monitor and manage their deployment. Through Cisco vManage, tenants can deploy and configure WAN edge devices. Tenants can also configure custom policies on assigned Cisco vSmart Controllers.

### Multi-tenant Cisco vBond Orchestrators

Cisco vBond Orchestrators are deployed and configured by the service provider. Only the provider can access a Cisco vBond Orchestrator through the SSH terminal.

Cisco vBond Orchestrators serve WAN edge devices of multiple tenants as the devices are added to the overlay network.

### Multi-tenant Cisco vSmart Controllers

Cisco vSmart Controllers are deployed by the service provider. Only the provider can create and attach device and feature templates to Cisco vSmart Controllers, and can access a Cisco vSmart Controller through the SSH terminal.

- When a tenant is created, Cisco vManage assigns two Cisco vSmart Controllers for the tenant. The Cisco vSmart Controllers form an active-active cluster.

  Each tenant is assigned only two Cisco vSmart Controllers. Before a tenant is created, two Cisco vSmart Controllers must be available to serve the tenant.

- When more than one pair of Cisco vSmart Controllers are available to serve a tenant, Cisco vManage assigns to the tenant the pair of Cisco vSmart Controllers connected to the lowest number of forecast devices. If two pairs of Cisco vSmart Controllers are connected to the same number of devices, Cisco vManage assigns to the tenant the pair of Cisco vSmart Controllers serving the lowest number of tenants.
- From Cisco vManage Release 20.9.1, 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. For more information, see Flexible Tenant Placement on Multitenant Cisco vSmart Controllers.
- Each pair of Cisco vSmart Controllers can serve a maximum of 24 tenants.
- Tenants can configure custom policies on the Cisco vSmart Controllers assigned to them. Cisco vManage notifies the Cisco vSmart Controllers to pull the policy templates. Cisco vSmart Controllers pull the templates and deploy the policy configuration for the specific tenant.
- Only the provider can view events, audit logs, and OMP alarms for a Cisco vSmart Controller on Cisco vManage.

### Tenant-Specific WAN Edge Devices

A tenant or the provider acting on behalf of a tenant can add WAN edge devices to the tenant network, configure the devices, and remove the devices from the tenant network, or access the device through the SSH terminal.

A provider can manage the WAN edge devices only from provider-as-tenant view. In the provider view, Cisco vManage does not show any WAN edge device information.

Cisco vManage reports WAN edge device events, logs, and alarms only in the Tenant Role and the provider-as-tenant views.

## User Roles in Multitenant Environment

A multi-tenant environment includes the service provider and tenant roles. Each role has distinct privileges, views, and functions.

### Provider Role

The provider role entitles system-wide administrative privileges. A user with the provider role has the default username **admin**. The provider user can access Cisco vManage using the domain name of the service provider or by using the Cisco vManage IP address. When using a domain name, the domain name has the format `https://managed-sp.com`.

The **admin** user is part of the user group **netadmin**. Users in this group are permitted to perform all operations on the controllers and the WAN edge devices of the tenants. You can add additional users to the **netadmin** group.

You cannot modify the privileges of the **netadmin** group. On Cisco vManage, you can view the privileges of the user group from the **Administration** > **Manage Users** > **User Groups** page.

**Note** When you create a new provider user in Cisco vManage, including a **netadmin** user, by default, the user is not allowed SSH access to the Cisco vManage VM. To enable SSH access, configure SSH authentication using a AAA template and push the template to Cisco vManage. For more information on enabling SSH authentication, see SSH Authentication using vManage on Cisco vEdge Devices.

For more information about configuring users and user groups, see Configure User Access and Authentication.

Cisco vManage offers two views to a provider:

- **Provider View**

  When a provider user logs in to multi-tenant Cisco vManage as **admin** or another **netadmin** user, Cisco vManage presents the provider view and displays the provider dashboard.

  You can perform the following functions from the provider view:

  - Provision and manage Cisco vManage, Cisco vBond Orchestrators and Cisco vSmart Controllers.
  - Add, modify, or delete tenants.
  - Monitor the overlay network.

- **Provider-as-Tenant View**

  When a provider user selects a specific tenant from the **Select Tenant** drop-down list at the top of the provider dashboard, Cisco vManage presents the provider-as-tenant view and displays the tenant dashboard for the selected tenant. The provider user has the same view of Cisco vManage as a tenant user would when logged in as **tenantadmin**. From this view, the provider can manage the tenant deployment on behalf of the tenant.

  In the provider dashboard, a table of tenants presents a status summary for each tenant. A provider user can also launch the provider-as-tenant view by clicking on a tenant name in this table.

### Tenant Role

The tenant role entitles tenant administrative privileges. A user with the tenant role has the default username **tenantadmin**. The default password is **Cisco#123@Viptela**. We recommend that you change the default password on first login. For information on changing the default password, see Hardware and Software Installation.

The **tenantadmin** user is part of the user group **tenantadmin**. Users in this group are permitted to perform all operations on the WAN edge devices of the tenants. You can add additional users to the **tenantadmin** group.

You cannot modify the privileges of the **tenantadmin** group. On Cisco vManage, you can view the privileges of the user group from the **Administration** > **Manage Users** > **User Groups** page.

For more information about configuring users and user groups, see Configure User Access and Authentication.

A tenant user can log in to Cisco vManage using a dedicated URL and the default username **tenantadmin**. For example, the dedicated URL of a tenant could be `https://customer1.managed-sp.com` for a provider using the domain name `https://managed-sp.com`. When the user logs in, Cisco vManage presents the tenant view and displays the tenant dashboard.

**Tip** If you cannot access the dedicated tenant URL, update the subdomain details in the `/etc/hosts` file on the local machine. Alternatively, if you use an external DNS server, add a DNS entry for the tenant subdomain.

A tenant user with administrative privileges can perform the following functions:

- Provision and manage tenant routers
- Monitor overlay network of the tenant
- Create custom policies on the assigned Cisco vSmart Controllers
- Upgrade the software on the tenant routers.

# Supported Devices and Controller Specifications

The following Cisco SD-WAN edge devices support multitenancy.

*Table 1: Supported Devices*

| Platform | Device Models |
|---|---|
| Cisco vEdge device | • vEdge 100, vEdge 100b, vEdge 100m, vEdge 100wm, vEdge 1000, vEdge 2000, vEdge 5000, vEdge Cloud<br>• ISR1100-6G/ISR1100-4G, ISR1100-4GLTENA, ISR1100-4GLTEGB |

The following hypervisors are supported for multitenancy:

- VMware ESXi 6.7 or later
- KVM
- AWS (cloud-hosted and managed by Cisco CloudOps)
- Microsoft Azure (cloud-hosted and managed by Cisco CloudOps)

From Cisco vManage Release 20.6.1, a multitenant Cisco vManage instance can have one of the following three personas. The personas enable a predefined set of services on the Cisco vManage instance.

*Table 2: Cisco vManage Personas*

| Persona | Services |
|---|---|
| Compute+Data | Cluster Oracle, Service Proxy, Messaging Service, Coordination Service, Configuration Database, Data Collection Agent, Statistics Database, and Application Server |
| Data | Cluster Oracle, Service Proxy, Application Server, Data Collection Agent, and Statistics Database |
| Compute | Cluster Oracle, Service Proxy, Messaging Service, Coordination Service, Configuration Database, and Application Server |

The supported hardware specifications for the Cisco vBond Orchestrator, Cisco vManage, and the Cisco vSmart Controllers are as follows:

### Hardware Specifications to Support 50 Tenants and 1000 Devices

For more information on supported hardware specifications for the Cisco vBond Orchestrator, Cisco vManage, and the Cisco vSmart Controllers see, Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

### Hardware Specifications to Support 75 Tenants and 2500 Devices

For more information on supported hardware specifications for the Cisco vBond Orchestrator, Cisco vManage, and the Cisco vSmart Controllers see, Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

### Hardware Specifications to Support 100 Tenants and 5000 Devices

For more information on supported hardware specifications for the Cisco vBond Orchestrator, Cisco vManage, and the Cisco vSmart Controllers see, Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

### Hardware Specifications to Support 150 Tenants and 7500 Devices

For more information on supported hardware specifications for the Cisco vBond Orchestrator, Cisco vManage, and the Cisco vSmart Controllers see, Cisco SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

# Restrictions

- Do not use a user-configured system IP address to connect to a device through SSH. Instead, use the IP address of the `vmanage_system` interface; this IP address is assigned by Cisco vManage.

  To find the IP address of the `vmanage_system` interface, use one of the following methods:

  - Launch the device SSH terminal from Cisco vManage and find the `vmanage_system` IP address from the first line of the log-in prompt.

  - Run the **show interface description** command and find the `vmanage_system` IP address from the command output.

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

- 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**.

# Initial Setup for Multitenancy

### Prerequisites

- Download and install software versions as recommended in the following table:

*Table 3: Minimum Software Prerequisites for Cisco SD-WAN Multitenancy*

| Device | Software Version |
|---|---|
| Cisco vManage | Cisco vManage Release 20.6.1 |
| Cisco vBond Orchestrator | Cisco SD-WAN Release 20.6.1 |
| Cisco vSmart Controller | Cisco SD-WAN Release 20.6.1 |
| Cisco vEdge Device | Cisco SD-WAN Release 20.6.1 |

  A configuration in which one or more controllers, or WAN edge devices, are running software versions earlier than those mentioned in the table above is not supported.

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

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

- Follow the recommended hardware specifications in the *Supported Devices and Controller Specifications* section of this document.

- Log in to Cisco vManage as the provider **admin** user.

1. Create Cisco vManage cluster.

   a. To support 50 tenants and 1000 devices across all tenants, Create a 3-Node Cisco vManage Cluster.

   b. To support 100 tenants and 5000 devices across all tenants, Create a 6-Node Cisco vManage Cluster.

c. From Cisco SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, Create a 6-Node Cisco vManage Cluster.

2. Create and configure Cisco vBond Orchestrator instances. See Deploy Cisco vBond Orchestrator.

   While configuring Cisco vBond Orchestrator instances, configure the service provider organization name (`sp-organization-name`) and the organization name (`organization-name`). See Configure Organization Name in Cisco vBond Orchestrator.

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

3. Create Cisco vSmart Controller instances. See Deploy the Cisco vSmart Controller.

   - To support 50 tenants and 1000 devices across all tenants, deploy 6 Cisco vSmart Controller instances.
   - To support 100 tenants and 5000 devices across all tenants, deploy 10 Cisco vSmart Controllers.
   - From Cisco SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy 16 Cisco vSmart Controllers.

   a. Add Cisco vSmart Controller to the overlay network.

4. Onboard new tenants. See Add a New Tenant, on page 18.

## Create a 3-Node Cisco vManage Cluster

1. Download the Cisco vManage Release 20.6.1 or later software image from Cisco Software Download.

2. Create three Cisco vManage instances (say vManage1, vManage2, and vManage3) by installing the downloaded software image file. See Deploy Cisco vManage.

**Important**

- Deploy Cisco vManage servers having the hardware specifications in the table *Hardware Specifications to Support 50 Tenants and 1000 Devices* from the *Supported Devices and Controller Specifications* section of this document.
- Choose the **Compute+Data** persona for each Cisco vManage instance.

3. Complete the following operations on vManage1:

   a. Configure the following using the CLI:

      - System IP address
      - Site ID
      - Service Provider organization name (`sp-organization-name`)
      - Organization-name
      - vBond IP address
      - VPN 0 Transport/Tunnel interface

- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
- VPN 512 Management interface

**Note** Configure only one default route in VPN 0.

b. Enable Multitenancy on Cisco vManage, on page 13.

c. (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

d. Complete the following through the Cisco vManage GUI:

1. Generate a Certificate Signing Request
2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.

e. Configure the Cluster IP Address of the Cisco vManage Server.

Before proceeding to the next step, ensure that the **vManage IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

4. Complete the following operations on vManage2 and vManage 3:

**Important** Do not enable multitenancy on vManage2 and vManage3.

a. Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- vBond IP address
- VPN 0 Transport/Tunnel interface
- VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
- VPN 512 Management interface

b. (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

c. Complete the following through the Cisco vManage GUI:

   1. Generate a Certificate Signing Request

   2. After Symantec or your enterprise root CA has signed the certificates, install signed certificate.

d. Log in to the Cisco vManage Web Application Server.

e. Ping the OOB interfaces on the other two Cisco vManage instances and ensure they are reachable.

f. Configure the Cluster IP Address of the Cisco vManage Server.

   Before proceeding to the next step, ensure that the **vManage IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

5. Log in to the vManage1 GUI and add vManage2 to the cluster.

   vManage2 reboots before being added to the cluster.

   While vManage2 is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for vManage2 shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding vManage2 to the cluster.

   When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both vManage1 and vManage2, and their node personas.

6. Repeat **Step 5** and add vManage3 to the cluster.

**Note** After rebooting, you have to select persona (non-cloud setup) from CLI and services starts running on the node according to the selected persona.

## Create a 6-Node Cisco vManage Cluster

1. Download the Cisco vManage Release 20.6.1 or later software image from Cisco Software Download.

2. Create six Cisco vManage instances by installing the downloaded software image file. See Deploy Cisco vManage.

**Important**

- To support 100 tenants and 5000 devices across all tenants, deploy Cisco vManage servers having the hardware specifications in the table *Hardware Specifications to Support 100 Tenants and 5000 Devices* from the *Supported Devices and Controller Specifications* section of this document.

  From Cisco SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy Cisco vManage servers having the hardware specifications in the table *Hardware Specifications to Support 150 Tenants and 7500 Devices* from the *Supported Devices and Controller Specifications* section of this document.

- Choose the **Compute+Data** persona for three Cisco vManage instances (say vManage1, vManange2, and vManage 3). Choose the **Data** persona for the other three Cisco vManage instances (say vManage4, vManage5, and vManage6).

3. Complete the following operations on vManage1:

   a. Configure the following using the CLI:

      - System IP address
      - Site ID
      - Service Provider organization name (`sp-organization-name`)
      - Organization-name
      - vBond IP address
      - VPN 0 Transport/Tunnel interface
      - VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
      - VPN 512 Management interface

**Note** Configure only one default route in VPN 0.

   b. Enable Multitenancy on Cisco vManage, on page 13.

   c. (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

   d. Complete the following through the Cisco vManage GUI:

      1. Generate a Certificate Signing Request
      2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.

   e. Configure the Cluster IP Address of the Cisco vManage Server.

Before proceeding to the next step, ensure that the **vManage IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

4. Complete the following operations on vManage2 through vManage6:

**Important** Do not enable multitenancy on vManage2 through vManage6.

   a. Configure the following using the CLI:

      - System IP address
      - Site ID
      - Service Provider organization name (`sp-organization-name`)
      - Organization-name
      - vBond IP address
      - VPN 0 Transport/Tunnel interface
      - VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
      - VPN 512 Management interface

   b. (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

   c. Complete the following through the Cisco vManage GUI:

      1. Generate a Certificate Signing Request
      2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.

   d. Log in to the Cisco vManage Web Application Server.

   e. Ping the OOB interfaces on the other Cisco vManage instances and ensure they are reachable.

   f. Configure the Cluster IP Address of the Cisco vManage Server.

      Before proceeding to the next step, ensure that the **vManage IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

5. Log in to the vManage1 GUI and add vManage2 to the cluster.

   vManage2 reboots before being added to the cluster.

   While vManage2 is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for vManage2 shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding vManage2 to the cluster.

When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both vManage1 and vManage2, and their node personas.

6. Repeat **Step 5** and add vManage3 through vManage6 to the cluster.

# 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

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.

# Expand a Multitenant Deployment to Support More Tenants and Tenant Devices

As a service provider, suppose you have deployed a Cisco SD-WAN multitenant overlay to support 50 tenants and 1000 devices. If you need to support more tenants or more devices, you can expand the Cisco vManage cluster and add additional Cisco vSmart Controllers to the overlay to support up to 100 tenants and 5000 devices. From Cisco SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, you can expand the Cisco vManage cluster and add additional Cisco vSmart Controllers to the overlay to support up to 150 tenants and 7500 devices.

### Prerequisites

A multitenant Cisco SD-WAN overlay that supports up to 50 tenants and 1000 devices, deployed according to the steps outlined in the *Initial Setup for Multitenancy* section of this document.

1. Expand a 3-Node Cluster to a 6-node Cluster.

2. To support up to 100 tenants and 5000 devices, you must have 10 Cisco vSmart Controllers in the overlay. So, deploy 4 Cisco vSmart Controllers in addition to the 6 existing Cisco vSmart Controllers in the overlay.

   To support up to 150 tenants and 7500 devices, you must have 16 Cisco vSmart Controllers in the overlay. So, deploy 10 Cisco vSmart Controllers in addition to the 6 existing Cisco vSmart Controllers in the overlay.

   a. Create Cisco vSmart Controller instances. See Deploy the Cisco vSmart Controller.

   b. Add Cisco vSmart Controller to the overlay network.

You can now add more tenants or allow your existing tenants to add more devices subject to the relevant limits.

## Expand a 3-Node Cluster to a 6-node Cluster

**Note** You can only expand a 3-node Cisco vManage cluster to a 6-node Cisco vManage cluster. Expansion of the 3-node cluster to other cluster sizes is not supported.

1. To support 100 tenants and 5000 devices: Upgrade the three Cisco vManage servers in the existing 3-node cluster to the hardware specifications in the table *Hardware Specifications to Support 100 Tenants and 5000 Devices* from the *Supported Devices and Controller Specifications* section of this document.

   From Cisco SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices: Upgrade the three Cisco vManage servers in the existing 3-node cluster to the hardware specifications in the table *Hardware Specifications to Support 150 Tenants and 7500 Devices* from the *Supported Devices and Controller Specifications* section of this document.

2. Download the Cisco vManage Release 20.6.1 or a later release software image from Cisco Software Download.

3. Create three Cisco vManage instances (say vManage1, vManage2, and vManage3) by installing the downloaded software image file. See Deploy Cisco vManage.

**Important**

- Deploy Cisco vManage servers having the hardware specifications in the table *Hardware Specifications to Support 100 Tenants and 5000 Devices* from the *Supported Devices and Controller Specifications* section of this document.

  From Cisco SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices, deploy Cisco vManage servers having the hardware specifications in the table *Hardware Specifications to Support 150 Tenants and 7500 Devices* from the *Supported Devices and Controller Specifications* section of this document.

- Choose the **Data** persona for each Cisco vManage instance.

4. Complete the following operations on vManage1 through vManage3:

**Important** Do not enable multitenancy on vManage1 through vManage3.

   a. Configure the following using the CLI:

   - System IP address
   - Site ID
   - Service Provider organization name (`sp-organization-name`)
   - Organization-name
   - vBond IP address
   - VPN 0 Transport/Tunnel interface
   - VPN 0 Out-of-band (OOB) interface: Ensure that you assign a static IP address to this interface. Do not enable DHCP.
   - VPN 512 Management interface

**Note** Configure only one default route in VPN 0.

   b. (Optional) Using the CLI, install the Root CA certificate for vManage1.

**Note** Skip this step if you are using a Symantec or Cisco PKI certificate.

   c. Complete the following through the Cisco vManage GUI:

1. Generate a Certificate Signing Request
2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.

d. Log in to the Cisco vManage Web Application Server.

e. Ping the OOB interfaces on the other Cisco vManage instances and ensure they are reachable.

f. Configure the Cluster IP Address of the Cisco vManage Server.

Before proceeding to the next step, ensure that the **vManage IP Address** field on the **Administration** > **Cluster Management** page shows the OOB interface address.

5. Log in to the GUI of the existing 3-node Cisco vManage cluster and add vManage1 to the cluster.

   vManage1 reboots before being added to the cluster.

   While vManage1 is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for vManage1 shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding vManage1 to the cluster.

   When the operation is completed, on the **Administration** > **Cluster Management** page, you can view vManage1 and its node persona listed along with the three Cisco vManage instances that were part of the original 3-node cluster.

6. Repeat **Step 4** and add vManage2 and vManage3 to the cluster.

# Manage Tenants

*Table 4: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Tenant Device Forecasting | Cisco SD-WAN Release 20.6.1<br>Cisco vManage Release 20.6.1 | With this feature, a service provider can control the number of WAN edge devices a tenant can add to their overlay network. By doing so, the provider can utilize Cisco SD-WAN controller resources efficiently. |

### Tenant Device Forecasting

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.

In a multitenant deployment, a tenant can add a maximum of 1000 devices to their overlay network.

**Note** From Cisco SD-WAN Release 20.6.2, Cisco vManage Release 20.6.2, you can modify the device forecast for a tenant after the tenant is added. This modification is not supported in Cisco SD-WAN Release 20.6.1, Cisco vManage Release 20.6.1.

**Benefits:**

- The service provider can ensure that the Cisco SD-WAN controller resources are used more efficiently.
- Depending on the configuration, a multitenant deployment can support a fixed number of WAN edge devices across all tenants. By forecasting the number of devices a tenant may add, the service provider can assign a quota for each tenant from the overall pool of edge devices that the deployment can support.

# Add a New Tenant

### 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 5: 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>`.<br>**Note** The organization name can be up to 64 characters. |

| Field | Description/Value |
|---|---|
| **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, on page 27.

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**.

# Cisco vManage Dashboard for Multitenancy

After enabling Cisco vManage for multitenancy, you can view the multitenant dashboard when you log in to Cisco vManage. Cisco vManage multitenant dashboard is a portal where the provider or tenant can view and provision the underlying system.

The bar at the top of every Cisco vManage multitenant screen includes icons that allow smooth navigation.

## View Tenant Activity, Device, and Network Information

When you log in to a multitenant Cisco vManage as an administrator, the provider dashboard displays the following components. To return to the provider dashboard from other Cisco vManage screens, click **Dashboard**.

- Device pane — runs across the top of the multitenant dashboard screen. The device pane displays the number of active Cisco vSmart Controllers, Cisco vBond Orchestrators, and Cisco vManage instances, the connectivity status of devices, and information on certificates that have expired or about to expire.
- Tenants pane — displays the total number of tenants and a summary of the control status, site health, router health, and Cisco vSmart Controller status of all tenants.
- Table of tenants in the overlay network — List of individual tenants, with separate information about the control status, site health, WAN edge device health, and Cisco vSmart Controller status for each tenant.

  To display tenant-specific status summary information,

  1. Click a tenant name from the tenant list.

     A dialog box opens on the right side of the screen that provides additional information about the status of the tenant.

  2. To access the tenant dashboard for the selected tenant, click **<Tenant name> Dashboard**.

     Cisco vManage presents the provider-as-tenant view and displays the tenant dashboard. To return to the provider view, click **Provider** at the top of page.

  3. To close the dialog box, click the tenant name from the tenant list.

## View Detailed Information of a Tenant Setup

Cisco vManage displays the tenant dashboard, which provides information about a tenant deployment when

- a provider **admin** user selects a specific tenant from the **Select Tenant** drop-down list in the provider dashboard. This view is called the provider-as-tenant view.
- a **tenantadmin** user logs in to Cisco vManage. This view is called the tenant view.

### View All Network Connections in the Tenant Overlay Network

The **Device** pane runs across the top of the tenant dashboard and displays the number of control connections from Cisco vManage to the Cisco vSmart Controllers and routers in the overlay network of a tenant. For each WAN edge device, the Device pane shows

- Total number of control connections between Cisco vSmart Controllers and WAN edge devices
- Number of valid control connections between Cisco vSmart Controllers and WAN edge devices
- Number of invalid control connections between Cisco vSmart Controllers and WAN edge devices

Click a connection number, or the **Up** or **Down** arrow, to display a table with detailed information about each connection. Click the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Network** screen, or access the **Tools** > **SSH Terminal** Screen.

Click a connection number, or the **Up** or **Down** arrow, to display a table with detailed information about each connection. Click the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen, or access the **Tools** > **SSH Terminal** Screen.

**Note** InCisco vManage Release 20.6.1 and earlier releases, you can view information related to the **Monitor** > **Devices** page under the **Monitor** > **Network** page.

### View Information About Device Reboots

The **Reboot** pane displays the total number of reboots in the last 24 hours for all devices in the network. It includes soft and cold reboots and reboots that occurred as a result of power-cycling a device. For each reboot, the following information is listed:

- System IP and hostname of the device that rebooted.
- Time when the device was rebooted.
- Reason for the device reboot

If the same device reboots more than once, each reboot option is reported separately.

Click the **Reboot** pane to open the **Reboot** dialog box. In the **Reboot** dialog box, click the **Crashes** tab. For all device crashes, the following information is listed:

- System IP and hostname of the device on which the crash occurred.
- Crash index of the device
- Core time when the device crashed.
- File name of the device crash log

### View Network Connections

The **Control Status** pane displays whether Cisco vSmart Controller and WAN edge devices are connected. Each Cisco vSmart Controller must connect to all other Cisco vSmart Controllers in the network. Each WAN edge device must connect to the maximum number of configured Cisco vSmart Controllers. The **Control Status** pane displays three network connection counts:

- Control Up — total number of devices with the required number of operational control plane connections to a Cisco vSmart Controller
- Partial — total number of devices with some, but not all, operational control plane connection to Cisco vSmart Controllers.

- Control Down — total number of devices with no control plane connection to a Cisco vSmart Controller

To display a table with device details, click a row from the **Control Status** dialog box. Click the **More Actions** icon at the right of each table row to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen.

**Note** InCisco vManage Release 20.6.1 and earlier releases, you can view information related to the **Monitor** > **Devices** page under the **Monitor** > **Network** page.

### View State of Data Connections for a Site

The **Site Health** pane displays the state of data connections for a site. When a site has multiple WAN edge devices, this pane displays the state for the entire site and not for individual devices. The Site Health pane displays three connectivity states:

- Full WAN Connectivity — total number of sites where all BFD sessions on all routers are in the up state.
- Partial WAN Connectivity — total number of sites where tunnel and all BFD sessions on all routers are in the down state. These sites still have limited data plane connectivity.
- No WAN Connectivity — total number of sites where all BFD sessions on all routers are in the down state. These sites have no data plane connectivity.

To display a table with detailed information about each site, node, or tunnel, click a row from the **Site Health** dialog box. Click the **More Actions** icon at the right of each row in the table to access the **Device Dashboard** or **Real Time** view from the **Monitor** > **Devices** screen, or access the **Tools** > **SSH Terminal** screen.

**Note** InCisco vManage Release 20.6.1 and earlier releases, you can view information related to the **Monitor** > **Devices** page under the **Monitor** > **Network** page.

### View Interface Usage for WAN Edge Interfaces

The **Transport Interface Distribution** pane displays interface usage in the last 24 hours for all WAN edge interfaces in VPN 0. It includes all TLOC interfaces. Click the pane to view details of interface usage in the **Transport Interface Distribution** dialog box.

### View WAN Edge Device Counts

The **WAN Edge Inventory** pane provides four WAN edge device counts:

- Total — total number of authorized serial numbers for WAN edge devices that have been uploaded on Cisco vManage. The serial number is uploaded on the **Configuration** > **Devices** screen.
- Authorized — total number of authorized WAN edge devices in the overlay network These WAN edge devices are marked as **Valid** in the **Configuration** > **Certificates** > **WAN Edge List** screen.
- Deployed — total number of deployed WAN edge devices. These are WAN edge devices that are marked as Valid and are now operational in the network.

- Staging — total number of WAN edge devices you configure at a staging site before they are made a part of the overlay network. These routers do not take part in any routing decisions and do not affect network monitoring through Cisco vManage.

  Click the pane to view hostname, system IP, site ID, and other details of each router from the **WAN Edge Inventory** dialog box.

### View Aggregated State of WAN Edge Devices

The **WAN Edge Health** pane offers an aggregated view of the state of WAN edge devices by providing a count of the number of devices in each state, therefore describing the health of the hardware nodes. The three WAN edge device states are:

- Normal — number of WAN edge devices with memory, hardware, and CPU in normal state. Using less than 70% of total memory or total CPU is classified as, normal.
- Warning — number of WAN edge devices with memory, hardware, or CPU in warning state. Using between 70% and 90% of total memory or total CPU is classified as, warning
- Error — number of WAN edge devices with memory, hardware, or CPU in error state. Using more than 90% of total memory or total CPU is classified as, error.

  Click a number or the WAN edge device state to display a table with the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms, including temperature, power supply, and PIM modules. Click the **More Actions** icon at the right of each row in the table to access the following:

  - **Hardware Environment**
  - **Real Time** view from the **Monitor** > **Network** screen

    > **Note** InCisco vManage Release 20.6.1 and earlier releases, you can view information related to the **Monitor** > **Devices** page under the **Monitor** > **Network** page.

  - **Tools** > **SSH Terminal** screen.

### View WAN Edge Device Loss, Latency, Jitter

The **Transport Health** pane displays the aggregated average loss, latency, and jitters for all links and all combinations of colors (for example, all LTE-to-LTE links, all LTE-to-3G links).

From the **Type** drop-down arrow, choose loss, latency, or jitter.

Click the ☰ icon to select a time period for which to display the transport health.

Click the ⛶ icon to open the **Transport Health** dialog box. This dialog box displays a more detailed view. To display information in a tabular format, click the **Details** tab. You can choose to change the displayed health type and time period.

### View SAIE Flow Information of WAN Edge Devices

The **Top Applications** pane displays SD-WAN Application Intelligence Engine (SAIE) flow information for traffic transiting routers in the overlay network.

**Note**

- In Cisco vManage Release 20.7.x and earlier releases, the SAIE flow is known as deep packet inspection (DPI).
- The SAIE flow information is shown only for the last 24 hours. To view SAIE flow information for a time before the last 24 hours, you must check the information for the specific device.

Click the icon to select a time period for which to display data. From the **VPN** drop-down list, select a VPN to display SAIE information for all flows in that VPN.

Click the icon to open the **Top Applications** dialog box. This dialog box displays a more detailed view of the same information. You can change the VPN and time period.

### View Tunnels Data

The **Application-Aware Routing** pane allows you to choose the following tunnel criteria from the **Type** drop-down arrow:

- Loss
- Latency
- Jitter

Based on the tunnel criteria, the pane displays the 10 worst tunnels. For example, if you choose loss, the pane shows 10 tunnels with the greatest average loss over the last 24 hours.

Click the icon against a row to display a graphical representation of the data. Select a time period for which to display data or click **Custom** to display a drop-down arrow for specifying a custom time period.

Click the icon to open the **Application-Aware Routing** dialog box. This dialog box displays the 25 worst tunnels based on criteria you choose from the **Type** drop-down arrow, the criteria being loss, latency, and jitter.

# 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.

# Tenant-Specific Policies on Cisco vSmart Controllers

A provider **admin** user (from the Cisco vManage provider-as-tenant view) or a **tenantadmin** user (from the Cisco vManage tenant view) can create and deploy tenant-specific policies on the Cisco vSmart Controllers serving the tenant. The user can configure a CLI policy or create the policy using the UI policy configuration wizard.

When you activate or deactivate a policy,

1. Cisco vManage identifies the Cisco vSmart Controllers serving the tenant.
2. Cisco vManage notifies the Cisco vSmart Controllers to pull the policy configuration.
3. Cisco vSmart Controllers pull and deploy the policy configuration.
4. Cisco vManage reports the status of the policy pull by the Cisco vSmart Controllers.

# Manage Tenant Data

## Back Up Tenant Data

The tenant data backup solution of Cisco vManage multitenancy provides the following functionalities:

- Create, Extract, and List Configuration Data Backup File.
- Back up configuration database of a specific tenant with an option to restore it later. See Restore and Delete Tenant Data Backup File.
- Delete back up files of a tenant stored in Cisco vManage. For deleting tenant data backup files, see Restore and Delete Tenant Data Backup File.

The following factors are applicable when using data backup solution:

- The tenant data backup solution operations can be performed by a tenant administrator in the tenant view and or by a provider administrator in the provider-as-tenant view. To know how to access tenant dashboard through different views, see User Roles in Multitenant Environment, on page 3.
- A tenant is allowed to perform the following backup operations at a particular time and must complete an operation before starting a new operation:
    - Back up a single configuration database
    - Download the backup file.
    - Restore or import backup files
    - Delete backup files.
    - List backup files
- A tenant backup file format is as follows:

  `Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz`
- The tenant data backup operation is a readonly operation on the configuration database. However, to ensure data consistency and prevent data loss, do not perform any major changes on the network while the operation is in progress.
- Multiple tenants can perform back-up and restore operations in parallel.
- A tenant is not allowed to perform other backup operations when the restore operation of the tenant database is in-progress. So, a tenant can perform a single backup operation and when this operation is in-progress, all new backup operation requests are rejected.

  The remaining tenants can continue with their backup operations.
- A tenant must perform backup and restore operations on Cisco vManage instances running identical Cisco vManage software versions.
- A tenant can store a maximum of three backup files in Cisco vManage and can download to store them outside Cisco vManage repository. If the tenant already has three backup files, a subsequent backup operation results in the earliest backup file being deleted and a new backup file being generated.

- Ensure that the following parameter values match in both the backup file and the setup where tenant has requested for a restore operation:
  - Tenant Id
  - Organization Name
  - SP Organization Name
- The tenant data backup solution creates a task in the tenant view of Cisco vManage. Therefore, the tenant can monitor the progress of the operation from the task view of the tenant dashboard.
- A provider cannot back up provider data using this solution. Therefore, the provider can back up all tenants information at once by backing up all tenants configuration database using CLI.

# Create, Extract, and List Configuration Data Backup File

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. In the address bar, modify the URL path with `dataservice` for the REST API connection.

   **Example:** `https://<tenant_URL>/dataservice`

3. Create a configuration backup file by using the following API:
   `https://<tenant_URL>/dataservice/tenantbackup/export.`

4. If the configuration backup file has been created successfully, Cisco vManage task view indicates that the backup file has been generated. You can view the process identifier of the created process or task.

   **Example:**

   ```
   {
      "processId": "72d69805-b987-436f-9b7a-afef2f3f9061",
   "status": "in-progress"
   }
   ```

5. Verify the task status using the obtained process identifier.

   **Example:**
   `https://<tenant_URL>/dataservice/device/action/status/72d69805-b987-436f-9b7a-afef2f3f9061`

   The verification generates the details of the task in the JSON file format.

6. After the task is completed, extract or download the backed-up file available under the **data** section of the JSON task file.

   **Example:** To extract or download the backup file, use the following API:
   `https://<tenannt_URL>/dataservice/tenantbackup/download/1570057020772/backup_1570057020772_100919-181838.tar.gz`

7. List backup files stored in Cisco vManage using the following API.

   **Example:** `https://<tenant_URL>//dataservice/tenantbackup/list`

# Restore and Delete Tenant Data Backup File

**Before you begin:**

To run the restore and delete tenant data backup files API, you can download and install Postman tool or any other alternative tool for testing http applications and services. In this document, the procedure to restore and delete tenant data backup files has been explained using the Postman tool. Postman is a software tool used as an API development environment. You can download the tool from the Postman website.

1. Open Google Chrome, or another browser, and enable developer mode on it.
2. 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**.
3. To get header information of the restore API, do as follows:
   a. On the right side of the screen, click the **Network** tab to get the network capture view.
   b. In the network capture view, click the **Name** column to sort the listed items.
   c. Search and click **index.html**.
   d. Click the **Headers** tab and expand **Request Headers**.
   e. Choose all text under **Request Headers** and copy it to the clipboard.
4. Import backup files through the Postman UI:
   a. Open the Postman UI.
   b. To disable SSL certificate verification, click **Postman** > **Preferences** > **General** > **Request**. Turn off **SSL Certificate Verification**.
   c. In the Postman UI, create a new tab.
   d. Click **Headers** and then click **Bulk Edit**.
   e. Paste the text that was copied in step 3 from the **Request Headers** block into an editable form.
   f. From the **GET** method drop-down list, choose **POST**.
   g. In the **Paste request URL** field, paste the dedicated URL of the tenant and include `dataservice/tenantbackup/import`.

      **Example:** `https://customer1.managed-sp.com/dataservice/tenantbackup/import`
   h. Click the **Body** tab and select **form-data**.
   i. Under **KEY** column, enter *bakup.tar.gz*
   j. Under **VALUE** column, click **Select Files** and select a backup file to be imported.
   k. To run the API, click **Send**.

      In the **Response** section of the Postman UI, you can view the JSON information that indicates the file that was restored.

5. Monitor the restoration of backup files in either of the following ways:

   a. Use Cisco vManage task view that indicates if backup file has been imported successfully. You can view the process identifier of the created process or task.

      **Example:**

      ```
      {"processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
          "status": "Import Successfully Submitted for tenant 1579026919487"
      }
      ```

   b. Use the following URL to get the status, `https://<tenant_URL>/dataservice/device/action/status/<processId>`

      **Example:**

      `https://customer1.managed-sp.com/dataservice/device/action/status/40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d`

6. Delete tenant data backup file through Postman UI.

   a. In the Postman UI, create a new tab.

   b. Click **Headers** and then click **Bulk Edit**.

   c. Paste the text that was copied in step 3 from the **Request Headers** block into an editable form.

   d. From the **GET** method drop-down list, choose **DELETE**.

   e. In the **Paste request URL** field, paste the dedicated URL of the tenant and include `dataservice/tenantbackup/delete?fileName='filename'`. The filename can either be name of the backup file or all.

      **Example:**

      `https://customer1.managed-sp.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz`

      **Example:** `https://customer1.managed-sp.com/dataservice/tenantbackup/delete?fileName=all`

   f. To run the API, click **Send**.

   In the **Response** section of the Postman UI, you can view the JSON information that indicates the files that were deleted.

   **Example:**

   ```
   {
       "Deleted": [
           "bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz"
       ]
   }
   ```

# 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.

# Migrate Single-Tenant Cisco SD-WAN Overlay to Multitenant Cisco SD-WAN Deployment

### Before You Begin

- Before you begin the migration,
  - Migration of a single-tenant overlay to a multitenant deployment is only supported with the Cisco SD-WAN controllers deployed on-premises. Migration is yet to be supported with cloud-hosted Cisco SD-WAN controllers.
  - Ensure that the edge devices in the single-tenant deployment can reach the Cisco vBond Orchestrator in the multitenant deployment
  - Ensure that the template, routing, and policy configuration on the edge devices is synchronized with the current configuration on Cisco vManage
  - Configure a maintenance window for the single-tenant overlay before performing this procedure. See Configure or Cancel vManage Server Maintenance Window.
- Minimum software requirements for the single-tenant overlay to be migrated:

| Device | Software Version |
|---|---|
| Cisco vManage | Cisco vManage Release 20.6.1 |
| Cisco vBond Orchestrator | Cisco SD-WAN Release 20.6.1 |
| Cisco vSmart Controller | Cisco SD-WAN Release 20.6.1 |

| Device | Software Version |
|---|---|
| Cisco vEdge Device | Cisco SD-WAN Release 20.6.1 |

- Minimum software requirements for the multitenant deployment to which the single-tenant overlay must be migrated:

| Device | Software Version |
|---|---|
| Cisco vManage | Cisco vManage Release 20.6.1 |
| Cisco vBond Orchestrator | Cisco SD-WAN Release 20.6.1 |
| Cisco vSmart Controller | Cisco SD-WAN Release 20.6.1 |
| Cisco vEdge Device | Cisco SD-WAN Release 20.6.1 |

- The software versions of the Cisco SD-WAN controllers and WAN edge devices must be identical in both the single-tenant and multitenant deployments.

- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.

### Migration Procedure

1. Export the single-tenant deployment and configuration data from a Cisco vManage instance controlling the overlay.

| | |
|---|---|
| Method | `POST` |
| URL | `https://`*`ST-vManage-IP-address`* |
| Endpoint | `/dataservice/tenantmigration/export` |
| Authorization | Admin user credentials. |

| | |
|---|---|
| Body | Required<br>Format: Raw JSON<br>`{`<br>`    "desc": <tenant_description>,`<br>`    "name": <tenant_name>,`<br>`    "subdomain": <tenant_name>.<domain>,`<br>`    "orgName":  <tenant_orgname >`<br>` }`<br>Field Description:<br>• `desc`: A description of the tenant. The description can be up to 256 characters and can contain only alphanumeric characters.<br>• `name`: Unique name for the tenant in the multitenant deployment.<br>• `subdomain`: Fully qualified sub-domain name of the tenant. The sub-domain name must include the domain name of the service provider. For example, if `managed-sp.com` is the domain name of service provider, and the tenant name is `Customer1`, the tenant sub-domain name would be `customer1.managed-sp.com`.<br>• `orgName`: Name of the tenant organization. The organization name is case-sensitive. |
| Response | Format: JSON<br>`{`<br>`    "processId": <vManage_process_ID>,`<br>`}` |

While exporting the data, Cisco vManage attempts to detach any CLI templates from the edge devices in preparation for the migration to the multitenant deployment. If prompted by Cisco vManage, detach CLI templates from the edge devices and execute the export API call again.

2. Check the status of the data export task in Cisco vManage. When the task succeeds, download the data using the URL `https://ST-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz`

3. On a multitenant Cisco vManage instance, import the data exported from the single-tenant overlay.

| | |
|---|---|
| Method | `POST` |
| URL | `https://MT-vManage-IP-address` |
| Endpoint | `/dataservice/tenantmigration/import` |
| Authorization | Provider Admin user credentials. |
| Body | Required<br>Format: form-data<br>Key Type: File<br>Value: `default.tar.gz` |

| | |
|---|---|
| Response | `Format: JSON`<br>`{`<br>`    "processId": <vManage_process_ID>,`<br>`    "migrationTokenURL": <token_URL>,`<br>`}` |

When the task succeeds, on the multitenant Cisco vManage, you can view the devices, templates, and policies imported from the single-tenant overlay.

4. Obtain the migration token using the token URL obtained in response to the API call in **Step 3**.

| | |
|---|---|
| Method | `GET` |
| URL | `https://`*`MT-vManage-IP-address`* |
| Endpoint | `migrationTokenURL` obtained in **Step 3**. |
| Authorization | Provider Admin user credentials. |
| Response | The migration token as a large blob of encoded text. |

5. On the single-tenant Cisco vManage instance, initiate the migration of the overlay to the multitenant deployment.

| | |
|---|---|
| Method | `POST` |
| URL | `https://`*`ST-vManage-IP-address`* |
| Endpoint | `dataservice/tenantmigration/networkMigration` |
| Authorization | Admin user credentials. |
| Body | Required<br>Format: Raw text<br>Content: Migration token obtained in **Step 4**. |
| Response | Format: JSON<br>`{`<br>`    "processId": <vManage_process_ID>,`<br>`}` |

In Cisco vManage, check the status of the migration task. As part of the migration task, the address of the multitenant vBond Orchestrator, and the service provider and tenant organization names are pushed to the WAN edge devices of the single-tenant overlay. If the task succeeds, WAN edge devices form control connections to controllers in the multitenant deployment; the WAN edge devices are no longer connected to the controllers of the single-tenant overlay.

Attach any CLI templates detached from the edge devices (in Step 1) after migration to the multitenant deployment. Before you attach the templates, update the Cisco vBond Orchestrator IP address and the Organization name to match the configuration of the multitenant deployment.

**Note** In the single-tenant deployment, if Cisco vManage-signed certificates are installed on cloud-based WAN edge devices, the certificates are cleared when the devices are migrated to the multitenant deployment. You must re-certify the devices on the multitenant Cisco vManage. If enterprise certificates are installed on the cloud-based WAN edge devices, the certificates are not affected by the migration. For more information, see Enterprise Certificates.

# Migrate Multitenant Cisco SD-WAN Overlay

*Table 6: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Migrate Multitenant Cisco SD-WAN Overlay | Cisco SD-WAN Release 20.6.1<br>Cisco vManage Release 20.6.1 | This feature enables you to migrate a multitenant Cisco SD-WAN overlay comprising shared Cisco vManage instances and Cisco vBond Orchestrators, and tenant-specific Cisco vSmart Controllers to a multitenant overlay comprising shared Cisco vManage instances, Cisco vBond Orchestrators, and Cisco vSmart Controllers. |

### Prerequisites

Minimum software requirements for Cisco SD-WAN controllers and WAN edge devices in the multitenant overlay to be migrated:

| Device | Software Version |
|---|---|
| Cisco vManage | Cisco vManage Release 20.3.3 |
| Cisco vBond Orchestrator | Cisco SD-WAN Release 20.3.3 |
| Cisco vSmart Controller | Cisco SD-WAN Release 20.3.3 |
| Cisco vEdge Device | Cisco SD-WAN Release 20.3.3 |

### Restrictions

- This migration procedures applies only to Cisco SD-WAN controllers deployed on premises.
- The multitenant overlay can only be migrated to a setup in which Cisco vManage instances run Cisco vManage Release 20.6.1 software and Cisco SD-WAN controllers run Cisco SD-WAN Release 20.6.1 software.
- This migration procedure cannot be used to merge two or more multitenant overlays. Only one multitenant overlay can be migrated to the new setup at a time.

### Migration Procedure

1. Upgrade the software on the three Cisco vManage instances in the cluster to Cisco vManage Release 20.6.1. For more information, see Upgrade Cisco vManage Cluster.

   **Note** Run the command **request nms configuration-db upgrade** on only one of the Cisco vManage instances.

2. After the Cisco vManage software is upgraded to Cisco vManage Release 20.6.1, log in to the Cisco vManage GUI.

   You're prompted to set a new password.

   a. Enter a new password that adheres to the password guidelines.

3. Upload the Cisco SD-WAN Release 20.6.1 software to Cisco vManage. For more information, see Add an Image to the Software Repository.

4. Upgrade the Cisco vBond Orchestrator software to Cisco SD-WAN Release 20.6.1. For more information, see Upgrade the Software Image on a Device.

5. Create two Cisco vSmart Controller instances running Cisco SD-WAN Release 20.6.1 software. See Deploy the Cisco vSmart Controller.

   **Note** With two Cisco vSmart Controller instances, you can support up to 24 tenants. To support up to 50 tenants, create six Cisco vSmart Controller instances.

   a. Add Cisco vSmart Controller to the overlay network.

   The **Provider Dashboard** shows the new Cisco vSmart Controllers running Cisco SD-WAN Release 20.6.1 software. The **Tenant Dashboard** shows the older Cisco vSmart Controllers running Cisco SD-WAN Release 20.3.3 software.

6. Enable maintenance window on Cisco vManage. For more information, see Configure or Cancel vManage Server Maintenance Window.

   A maintenance window of 3 to 4 hours is recommended.

7. Migrate the tenant configuration from the older tenant-specific Cisco vSmart Controllers running Cisco SD-WAN Release 20.3.3 software to the new shared Cisco vSmart Controllers running Cisco SD-WAN Release 20.6.1 software.

| | |
|---|---|
| Method | `POST` |
| URL | `https://<vmanageip>:<port>` |
| Endpoint | `dataservice/tenant/vsmart-mt/migrate` |
| Authorization | Provider **admin** user credentials. |
| Body | Required<br>Format: Raw JSON<br>`{}` |

| | |
|---|---|
| Response | Format: JSON<br>`{`<br>`    "processId": <vManage_process_ID>,`<br>`}` |

In Cisco vManage, check the status of the migration task using the `processId` from the API response. During the migration task, the following changes are effected:

a. The older Cisco vSmart Controllers are invalidated and deleted from the overlay network.

b. In the tenant view, the older Cisco vSmart Controllers are removed from the **Tenant Dashboard**, and the **Devices** and the **Certificates** page.

c. The tenant WAN edge devices are connected to the new Cisco vSmart Controllers.

8. (Optional) Upgrade the Cisco vEdge device software to Cisco SD-WAN Release 20.6.1. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.

**Tip** It is not necessary to upgrade the tenant WAN edge device software in the same maintenance window in which you migrate the multitenant overlay. However, we recommend that you upgrade the tenant WAN edge device software within a few weeks of the migration.

### Verify the Migration

1. In the provider view, perform the following checks:

   a. From the **Main Dashboard** page, verify whether the tenant WAN edge devices are connected to the new multitenant Cisco vSmart Controllers.

   b. View Tenants Associated with a Cisco vSmart Controller, on page 32.

   c. On the Cisco vSmart Controller CLI, run the command **show control connections**. In the command output, verify that control connections are established between the Cisco vSmart Controller and the tenant WAN edge devices.

2. In the provider-as-tenant view, verify whether the multitenant Cisco vSmart Controllers appear on the **Tenant Dashboard**.

# Upgrade Cisco SD-WAN Controller and Edge Device Software

### Prerequisites

Minimum software requirements for Cisco SD-WAN controllers and WAN edge devices:

| Device | Software Version |
|---|---|
| Cisco vManage | Cisco vManage Release 20.4.1 or later |
| Cisco vBond Orchestrator | Cisco SD-WAN Release 20.4.1 or later |

| Device | Software Version |
|---|---|
| Cisco vSmart Controller | Cisco SD-WAN Release 20.4.1 or later |
| Cisco vEdge Device | Cisco SD-WAN Release 20.4.1 or later |

### Upgrade Procedure

1. Upgrade the software on the three Cisco vManage instances in the cluster to Cisco vManage Release 20.6.1 or a later release. For more information, see Upgrade Cisco vManage Cluster.

   **Note** Skip the step to upgrade the configuration-db service using the command **request nms configuration-db upgrade**.

2. After the Cisco vManage software is upgraded to Cisco vManage Release 20.6.1 or a later release, log in to the Cisco vManage GUI.
3. Upload the Cisco SD-WAN Release 20.6.1 or a later release software to Cisco vManage. For more information, see Add an Image to the Software Repository.
4. Upgrade the Cisco vBond Orchestrator software to Cisco SD-WAN Release 20.6.1 or a later release. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.
5. Enable maintenance window on Cisco vManage. For more information, see Configure or Cancel vManage Server Maintenance Window.
6. Upgrade the Cisco vSmart Controller software to Cisco SD-WAN Release 20.6.1 or a later release. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.
7. Upgrade the Cisco vEdge device software to Cisco SD-WAN Release 20.6.1 or a later release. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.

   **Tip** We recommend that you upgrade the WAN edge device software in the same maintenance window. If the WAN edge device software is not upgraded within the OMP graceful restart window, traffic may be lost.

# Multitenant Cisco vManage: Disaster Recovery

If a Multitenant Cisco vManage cluster or the data center hosting the Cisco vManage nodes in the cluster fail, you can recover from the failure by activating a standby Cisco vManage cluster. You can perform disaster recovery as follows:

1. Deploy and configure a standby Cisco vManage cluster.

   The standby Cisco vManage cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active Cisco vManage cluster periodically.

   Choose a Cisco vManage node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active Cisco vManage cluster fails, restore the most recent configuration database on the standby Cisco vManage cluster, activate the standby Cisco vManage cluster, and remove the previously active Cisco vManage cluster from the overlay network.

   Choose a Cisco vManage node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active Cisco vManage cluster.

To test disaster recovery, you can simulate a scenario in which the active Cisco vManage cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

### Prerequisites

- The number of Cisco vManage nodes in the active and standby clusters must be identical.
- Each Cisco vManage node in the active and standby clusters must run the same Cisco vManage software release.
- Each Cisco vManage node in the active and standby clusters must be able to connect to the WAN transport IP address of the Cisco vBond Orchestrators in the overlay network.
- Initially, the tunnel interfaces of the Cisco vManage nodes in the standby cluster must be disabled.
- The Cisco vManage nodes in the standby cluster must be certified.
- The clock of every Cisco vManage node in the standby cluster must be synchronized with the clocks of the Cisco SD-WAN controllers and WAN edge devices in the overlay network. If NTP is configured on the overlay, configure the same on the standby Cisco vManage nodes.
- The Cisco vManage nodes in the active and standby clusters should use identical neo4j credentials.

### Restrictions

- Do not interrupt any active processes while backing up the configuration database.
- If you wish to enable SD-AVC, you must do so before the restoring the configuration database on standby Cisco vManage node.

### Configure a Standby Cisco vManage Cluster

1. Configure the standby Cisco vManage nodes with a similar running configuration as the active Cisco vManage nodes. Install local certificates on the standby Cisco vManage nodes.

**Note** The running configuration on a standby Cisco vManage is usually identical to that of an active Cisco vManage node. However, you must ensure that settings such as the system IP address and the tunnel interface IP address are unique.

2. On the standby Cisco vManage nodes, shut down the transport interface in VPN 0: On the CLI, include the **shutdown** command in the transport interface configuration.
3. Create a standby cluster using the standby Cisco vManage nodes.

With the standby Cisco vManage nodes configured in this manner, the overlay network is not aware of the standby Cisco vManage cluster.

### Back Up the Active Cisco vManage Cluster Configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active Cisco vManage virtual machines.

1. Choose an active Cisco vManage node that hosts the configuration database service and export a backup the configuration database. On the CLI of the Cisco vManage node, run the following command: **request nms configuration-db backup path** *file-path*

   The command backs up the configuration database in a `.tar.gz` file and saves the file in the specified *file-path*.

   In the following example, the database is backed up to a file named `db_backup.tar.gz` in the `/home/admin/` directory.

   ```
   Active-vManage# request nms configuration-db backup path /home/admin/db_backup
   Successfully saved database to /home/admin/db_backup.tar.gz
   ```

2. Choose a standby Cisco vManage node that hosts the configuration database service and copy the configuration database backup to this node.

   In the following example, `db_backup.tar.gz` is copied from the active Cisco vManage node to the `/home/admin/` directory of a standby Cisco vManage node.

   ```
   Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
   admin@10.126.93.92:/home/admin
   The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
   ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
   viptela 18.4.5

   admin@10.126.93.92's password:
   db_backup.tar.gz                                100%  399KB   4.4MB/s   00:00
   ```

### Restore Cisco vManage Cluster Using the Configuration Database Backup

Restore the most recent backup of the configuration database from the active Cisco vManage cluster on the standby Cisco vManage node to which you copied this backup.

**Note**

- The restore operation does not restore all the information included in the configuration database. Cisco vManage configurations such as users and repositories must be configured on the standby Cisco vManage node after the configuration database is restored using the backup.
- When you complete the steps that follow, the previously active Cisco vManage nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

1. On the CLI of the standby Cisco vManage node, run the following command: **request nms configuration-db restore path** *file-path*

   In the following example, the configuration database is restored using the backup file `db_backup.tar.gz`.

   ```
   Standby-vManage# request nms configuration-db restore path /home/admin/db_backup.tar.gz
   Configuration database is running in a standalone mode
   Importing database...Successfully restored database
   ```

2. Verify that the appropriate services are running on the standby Cisco vManage nodes: On the CLI of each standby Cisco vManage node, run the **request nms all status** command. From the command output, verify the services running on the node.

3. Verify that every standby Cisco vManage node has a list of all the active and standby Cisco vManage nodes.

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

   b. Verify that the page displays all active and standby Cisco vManage nodes.

4. On the standby Cisco vManage nodes, enable the transport interface on VPN 0.

   Use one of the following two methods:

   a. Enable the transport interface in VPN 0: On the CLI of each standby Cisco vManage node, run the **no shutdown** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   Active-vManage(config-interface)# no shutdown
   Active-vManage(config-interface)# commit and-quit
   ```

   b. Activate the tunnel interface in VPN 0: On the CLI of each standby Cisco vManage node, run the **tunnel-interface** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   Active-vManage(config-interface)# tunnel-interface
   Active-vManage(config-interface)# commit and-quit
   ```

5. Add each standby Cisco vManage node to the overlay network.

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

   b. Click **Controllers**.

   c. For a Cisco vBond Orchestrator, click **...** and click **Edit**.

   d. In the **Edit** dialog box, enter the following details of the Cisco vBond Orchestrator: WAN transport IP address, username, and password.

   e. Repeat **Step 5c** and **Step 5d** for every Cisco vBond Orchestrator.

6. Disconnect the active Cisco vManage nodes from the overlay network.

   **Note** In a lab environment, where you are simulating a disaster scenario, you can perform this step. However, if you cannot reach Cisco vManage instances in an actual disaster scenario, you may not be able to perform this step and can omit the step.

   Use one of the following two methods:

   a. Shut down the transport interface in VPN 0: On the CLI of each active Cisco vManage node, run the **shutdown** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   ```

```
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

**b.** Deactivate the tunnel interface in VPN 0: On the CLI of each active Cisco vManage node, run the **no tunnel-interface** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

**7.** From the standby Cisco vManage, send the updated controller and device list to the Cisco vBond Orchestrators.

Send the list of controllers:

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

**b.** Click **Controllers**.

**c.** Click **Send to vBond**.

Wait for the configuration task to complete. When the task is complete,

- The standby Cisco vManage nodes become the active Cisco vManage nodes.
- The previously active Cisco vManage nodes are no longer part of the overlay network.
- The active Cisco vManage nodes have the configuration from the most recent configuration database backup.
- Every controller establishes connection with the other controllers in the network.

**d.** Click **WAN Edge List**.

**e.** Click **Send to Controllers**.

**8.** Verify that the following are intact:

- Policies
- Templates
- Controller and WAN edge device lists

**9.** Verify the valid Cisco vManage nodes.

**a.** Log in to the CLI of each Cisco vBond Orchestrator and run the **show orchestrator valid-vmanage-id** command.

In the command output, verify that the chassis numbers of the active and previously active Cisco vManage nodes are listed.

**b.** Log in to the CLI of a WAN edge device and run the **show control valid-vmanage-id** command.

In the command output, verify that the chassis numbers of the active and previously active Cisco vManage nodes are listed. Also, check whether the device is connected to the active Cisco vManage nodes and the Cisco vSmart Controllers.

**10.** Invalidate the previously active Cisco vManage nodes.

**Note** After you invalidate the Cisco vManage nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

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

   b. Click **Controllers**.

   c. For each previously active Cisco vManage node, click **...** and click **Invalidate**.

11. Verify the valid Cisco vManage nodes.

   a. Log in to the CLI of each Cisco vBond Orchestrator and run the **show orchestrator valid-vmanage-id** command.

      In the command output, verify that the chassis numbers of only the active Cisco vManage nodes are listed.

   b. Log in to the CLI of WAN edge device and run the **show control valid-vmanage-id** command.

      In the command output, verify that the chassis numbers of only the active Cisco vManage nodes are listed. Also, check whether the device is connected to the active Cisco vManage nodes and the Cisco vSmart Controllers.

The Cisco vManage cluster that was initially the standby cluster is now the active Cisco vManage cluster.

# Multitenant Cisco vManage: Disaster Recovery in an Overlay Network with Virtual Routers

If a Multitenant Cisco vManage cluster or the data center hosting the Cisco vManage nodes in the cluster fail, you can recover from the failure by activating a standby Cisco vManage cluster. You can perform disaster recovery as follows:

1. Deploy and configure a standby Cisco vManage cluster.

   The standby Cisco vManage cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active Cisco vManage cluster periodically.

   Choose a Cisco vManage node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active Cisco vManage cluster fails, restore the most recent configuration database on the standby Cisco vManage cluster, activate the standby Cisco vManage cluster, and remove the previously active Cisco vManage cluster from the overlay network.

   Choose a Cisco vManage node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active Cisco vManage cluster.

To test disaster recovery, you can simulate a scenario in which the active Cisco vManage cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

The following disaster recovery procedure applies to an overlay network in which Cisco vEdge Cloud routers are deployed at branch locations.

### Prerequisites

- The number of Cisco vManage nodes in the active and standby clusters must be identical.
- Each Cisco vManage node in the active and standby clusters must run the same Cisco vManage software release.
- Each Cisco vManage node in the active and standby clusters must be able to connect to the WAN transport IP address of the Cisco vBond Orchestrators in the overlay network.
- Initially, the tunnel interfaces of the Cisco vManage nodes in the standby cluster must be disabled.
- The Cisco vManage nodes in the standby cluster must be certified.
- The clock of every Cisco vManage node in the standby cluster must be synchronized with the clocks of the Cisco SD-WAN controllers and WAN edge devices in the overlay network. If NTP is configured on the overlay, configure the same on the standby Cisco vManage nodes.
- The Cisco vManage nodes in the active and standby clusters should use identical neo4j credentials.

### Restrictions

- Do not interrupt any active processes while backing up the configuration database.
- If you wish to enable SD-AVC, you must do so before the restoring the configuration database on standby Cisco vManage node.

### Configure a Standby Cisco vManage Cluster

1. Configure the standby Cisco vManage nodes with a similar running configuration as the active Cisco vManage nodes. Install local certificates on the standby Cisco vManage nodes.

**Note** The running configuration on a standby Cisco vManage is usually identical to that of an active Cisco vManage node. However, you must ensure that settings such as the system IP address and the tunnel interface IP address are unique.

2. On the standby Cisco vManage nodes, shut down the transport interface in VPN 0: On the CLI, include the **shutdown** command in the transport interface configuration.
3. Create a standby cluster using the standby Cisco vManage nodes.

With the standby Cisco vManage nodes configured in this manner, the overlay network is not aware of the standby Cisco vManage cluster.

### Back Up the Active Cisco vManage Cluster Configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active Cisco vManage virtual machines.

1. Choose an active Cisco vManage node that hosts the configuration database service and export a backup the configuration database. On the CLI of the Cisco vManage node, run the following command: **request nms configuration-db backup path** *file-path*

   The command backs up the configuration database in a `.tar.gz` file and saves the file in the specified *file-path*.

   In the following example, the database is backed up to a file named `db_backup.tar.gz` in the `/home/admin/` directory.

   ```
   Active-vManage# request nms configuration-db backup path /home/admin/db_backup
   Successfully saved database to /home/admin/db_backup.tar.gz
   ```

2. Choose a standby Cisco vManage node that hosts the configuration database service and copy the configuration database backup to this node.

   In the following example, `db_backup.tar.gz` is copied from the active Cisco vManage node to the `/home/admin/` directory of a standby Cisco vManage node.

   ```
   Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
   admin@10.126.93.92:/home/admin
   The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
   ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
   viptela 18.4.5

   admin@10.126.93.92's password:
   db_backup.tar.gz                                100%  399KB   4.4MB/s   00:00
   ```

### Restore Cisco vManage Cluster Using the Configuration Database Backup

Restore the most recent backup of the configuration database from the active Cisco vManage cluster on the standby Cisco vManage node to which you copied this backup.

**Note**

- The restore operation does not restore all the information included in the configuration database. Cisco vManage configurations such as users and repositories must be configured on the standby Cisco vManage node after the configuration database is restored using the backup.
- When you complete the steps that follow, the previously active Cisco vManage nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

1. On the CLI of the standby Cisco vManage node, run the following command: **request nms configuration-db restore path** *file-path*

   In the following example, the configuration database is restored using the backup file `db_backup.tar.gz`.

   ```
   Standby-vManage# request nms configuration-db restore path /home/admin/db_backup.tar.gz
   Configuration database is running in a standalone mode
   Importing database...Successfully restored database
   ```

2. Verify that the appropriate services are running on the standby Cisco vManage nodes: On the CLI of each standby Cisco vManage node, run the **request nms all status** command. From the command output, verify the services running on the node.

3. Verify that every standby Cisco vManage node has a list of all the active and standby Cisco vManage nodes.

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

   b. Verify that the page displays all active and standby Cisco vManage nodes.

4. Log in to the CLI of each Cisco vBond Orchestrator and run the **show orchestrator valid-vmanage-id** command.

   In the command output, verify that the chassis numbers of the active and previously active Cisco vManage nodes are listed.

5. Log in to the CLI of Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.

   In the command output, verify that the chassis numbers of the active and previously active Cisco vManage nodes are listed.

6. On the standby Cisco vManage nodes, enable the transport interface on VPN 0.

   Use one of the following two methods:

   a. Enable the transport interface in VPN 0: On the CLI of each standby Cisco vManage node, run the **no shutdown** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   Active-vManage(config-interface)# no shutdown
   Active-vManage(config-interface)# commit and-quit
   ```

   b. Activate the tunnel interface in VPN 0: On the CLI of each standby Cisco vManage node, run the **tunnel-interface** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   Active-vManage(config-interface)# tunnel-interface
   Active-vManage(config-interface)# commit and-quit
   ```

7. Add each standby Cisco vManage node to the overlay network.

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

   b. Click **Controllers**.

   c. For a Cisco vBond Orchestrator, click **...** and click **Edit**.

   d. In the **Edit** dialog box, enter the following details of the Cisco vBond Orchestrator: WAN transport IP address, username, and password.

   e. Repeat **Step 7c** and **Step 7d** for every Cisco vBond Orchestrator.

8. Disconnect the active Cisco vManage nodes from the overlay network.

**Note** In a lab environment, where you are simulating a disaster scenario, you can perform this step. However, if you cannot reach Cisco vManage instances in an actual disaster scenario, you may not be able to perform this step and can omit this step.

Use one of the following two methods:

a. Shut down the transport interface in VPN 0: On the CLI of each active Cisco vManage node, run the **shutdown** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

b. Deactivate the tunnel interface in VPN 0: On the CLI of each active Cisco vManage node, run the **no tunnel-interface** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

9. From the standby Cisco vManage, send the updated controller and device list to the Cisco vBond Orchestrators.

   Send the list of controllers:

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

   b. Click **Controllers**.

   c. Click **Send to vBond**.

      Wait for the configuration task to complete. When the task is complete,

      - The standby Cisco vManage nodes become the active Cisco vManage nodes.
      - The previously active Cisco vManage nodes are no longer part of the overlay network.
      - The active Cisco vManage nodes have the configuration from the most recent configuration database backup.
      - Every controller establishes connection with the other controllers in the network.

   d. Click **WAN Edge List**.

   e. Click **Send to Controllers**.

10. Verify that the following are intact:

    - Policies
    - Templates
    - Controller and WAN edge device lists

11. Verify the valid Cisco vManage nodes.

    a. Log in to the CLI of each Cisco vBond Orchestrator and run the **show orchestrator valid-vmanage-id** command.

       In the command output, verify that the chassis numbers of the active and previously active Cisco vManage nodes are listed.

b. Log in to the CLI of a Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.

   In the command output, verify that the chassis numbers of the active and previously active Cisco vManage nodes are listed. Also, check whether the device is connected to the active Cisco vManage nodes and the Cisco vSmart Controllers.

12. Invalidate the previously active Cisco vManage nodes.

    The previously active Cisco vManage is the certificate issuer for the cloud WAN edge devices. The active Cisco vManage issues certificates to the cloud WAN edge devices only after the previously active Cisco vManage nodes are invalidated.

**Note**

- After you invalidate the Cisco vManage nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.
- When you invalidate the previously active Cisco vManage nodes, Cisco vManage marks the nodes as invalid and sends an update to all controllers. However, Cisco vManage does not send an updated list of valid Cisco vManage UUIDs to Cisco vBond Orchestrators immediately because the previously active Cisco vManage is the CA for the cloud WAN edge devices. So, the output of the **show orchestrator valid-vmanage-id** command on a Cisco vBond Orchestrator includes the UUIDs of the invalidated Cisco vManage nodes.

  Cisco vManage has a scheduled task that runs every 24 hours and checks to see if all the cloud WAN edges have been moved to the active Cisco vManage. Cisco vManage sends the updated list of valid Cisco vManage UUIDs to Cisco vBond Orchestrator only after the cloud WAN edge devices have been moved to the active Cisco vManage. After this list is received, the output of the **show orchestrator valid-vmanage-id** command on a Cisco vBond Orchestrator does not include the UUIDs of the invalidated Cisco vManage nodes.

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

b. Click **Controllers**.

c. For each previously active Cisco vManage node, click **...** and click **Invalidate**.

13. Verify the valid Cisco vManage nodes after 24 hours.

a. Log in to the CLI of each Cisco vBond Orchestrator and run the **show orchestrator valid-vmanage-id** command.

   In the command output, verify that the chassis numbers of only the active Cisco vManage nodes are listed.

b. Log in to the CLI of WAN edge device and run the **show control valid-vmanage-id** command.

   In the command output, verify that the chassis numbers of only the active Cisco vManage nodes are listed. Also, check whether the device is connected to the active Cisco vManage nodes and the Cisco vSmart Controllers.

The Cisco vManage cluster that was initially the standby cluster is now the active Cisco vManage cluster.

# Multitenant Cisco vManage: Disaster Recovery After a Failed Data Center Becomes Operational

If a Multitenant Cisco vManage cluster or the data center hosting the Cisco vManage nodes in the cluster fail, you can recover from the failure by activating a standby Cisco vManage cluster. You can perform disaster recovery as follows:

1. Deploy and configure a standby Cisco vManage cluster.

   The standby Cisco vManage cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active Cisco vManage cluster periodically.

   Choose a Cisco vManage node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active Cisco vManage cluster fails, restore the most recent configuration database on the standby Cisco vManage cluster, activate the standby Cisco vManage cluster, and remove the previously active Cisco vManage cluster from the overlay network.

   Choose a Cisco vManage node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active Cisco vManage cluster.

To test disaster recovery, you can simulate a scenario in which the active Cisco vManage cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

The following procedure applies to a scenario in which an initially active Cisco vManage cluster or the data center hosting the cluster failed and the standby Cisco vManage cluster was configured to be the active Cisco vManage cluster. If the cluster that was initially active becomes operational again, it serves as a standby cluster. By completing the following procedure, you can turn this standby cluster into the active cluster.

### Check the Configuration of the Standby vManage NMS

1. Check whether the running configuration of the standby Cisco vManage nodes is similar to the running configuration of the active Cisco vManage nodes. Local certificates must be installed on the standby Cisco vManage nodes.

**Note** The running configuration on a standby Cisco vManage is usually identical to that of an active Cisco vManage node. However, you must ensure that settings such as the system IP address and the tunnel interface IP address are unique.

2. On the standby Cisco vManage nodes, shut down the transport interface in VPN 0: On the CLI, include the **shutdown** command in the transport interface configuration.

With the standby Cisco vManage nodes configured in this manner, the overlay network is not aware of the standby Cisco vManage cluster.

### Back Up the Active Cisco vManage Cluster Configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active Cisco vManage virtual machines.

1. Choose an active Cisco vManage node that hosts the configuration database service and export a backup the configuration database. On the CLI of the Cisco vManage node, run the following command: **request nms configuration-db backup path** *file-path*

   The command backs up the configuration database in a `.tar.gz` file and saves the file in the specified *file-path*.

   In the following example, the database is backed up to a file named `db_backup.tar.gz` in the `/home/admin/` directory.

   ```
   Active-vManage# request nms configuration-db backup path /home/admin/db_backup
   Successfully saved database to /home/admin/db_backup.tar.gz
   ```

2. Choose a standby Cisco vManage node that hosts the configuration database service and copy the configuration database backup to this node.

   In the following example, `db_backup.tar.gz` is copied from the active Cisco vManage node to the `/home/admin/` directory of a standby Cisco vManage node.

   ```
   Active-vManage# request execute vpn 512 scp /home/admin/db_backup.tar.gz
   admin@10.126.93.92:/home/admin
   The authenticity of host '10.126.93.92 (10.126.93.92)' can't be established.
   ECDSA key fingerprint is SHA256:jTjJWQ0UNHvlrBUxWzNjd8mUz819gPf51MeopsgDlAc.
   Are you sure you want to continue connecting (yes/no)? yes
   Warning: Permanently added '10.126.93.92' (ECDSA) to the list of known hosts.
   viptela 18.4.5

   admin@10.126.93.92's password:
   db_backup.tar.gz                                100%  399KB   4.4MB/s   00:00
   ```

### Restore Cisco vManage Cluster Using the Configuration Database Backup

Restore the most recent backup of the configuration database from the active Cisco vManage cluster on the standby Cisco vManage node to which you copied this backup.

**Note**

- The restore operation does not restore all the information included in the configuration database. Cisco vManage configurations such as users and repositories must be configured on the standby Cisco vManage node after the configuration database is restored using the backup.
- When you complete the steps that follow, the previously active Cisco vManage nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

1. On the CLI of the standby Cisco vManage node, run the following command: **request nms configuration-db restore path** *file-path*

   In the following example, the configuration database is restored using the backup file `db_backup.tar.gz`.

   ```
   Standby-vManage# request nms configuration-db restore path /home/admin/db_backup.tar.gz
   Configuration database is running in a standalone mode
   Importing database...Successfully restored database
   ```

2. Verify that the appropriate services are running on the standby Cisco vManage nodes: On the CLI of each standby Cisco vManage node, run the **request nms all status** command. From the command output, verify the services running on the node.

3. Verify that every standby Cisco vManage node has a list of all the active and standby Cisco vManage nodes.

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

   b. Verify that the page displays all active and standby Cisco vManage nodes.

4. On the standby Cisco vManage nodes, enable the transport interface on VPN 0.

   Use one of the following two methods:

   a. Enable the transport interface in VPN 0: On the CLI of each standby Cisco vManage node, run the **no shutdown** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   Active-vManage(config-interface)# no shutdown
   Active-vManage(config-interface)# commit and-quit
   ```

   b. Activate the tunnel interface in VPN 0: On the CLI of each standby Cisco vManage node, run the **tunnel-interface** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   Active-vManage(config-interface)# tunnel-interface
   Active-vManage(config-interface)# commit and-quit
   ```

5. Add each standby Cisco vManage node to the overlay network.

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

   b. Click **Controllers**.

   c. For a Cisco vBond Orchestrator, click **...** and click **Edit**.

   d. In the **Edit** dialog box, enter the following details of the Cisco vBond Orchestrator: WAN transport IP address, username, and password.

   e. Repeat **Step 5c** and **Step 5d** for every Cisco vBond Orchestrator.

6. Disconnect the active Cisco vManage nodes from the overlay network.

   **Note** In a lab environment, where you are simulating a disaster scenario, you can perform this step. However, if you cannot reach Cisco vManage instances in an actual disaster scenario, you may not be able to perform this step and can omit the step.

   Use one of the following two methods:

   a. Shut down the transport interface in VPN 0: On the CLI of each active Cisco vManage node, run the **shutdown** command.

   ```
   Active-vManage# config
   Active-vManage(config)# vpn 0 interface interface-name
   ```

```
Active-vManage(config-interface)# shutdown
Active-vManage(config-interface)# commit and-quit
```

b. Deactivate the tunnel interface in VPN 0: On the CLI of each active Cisco vManage node, run the **no tunnel-interface** command.

```
Active-vManage# config
Active-vManage(config)# vpn 0 interface interface-name
Active-vManage(config-interface)# no tunnel-interface
Active-vManage(config-interface)# commit and-quit
```

7. From the standby Cisco vManage, send the updated controller and device list to the Cisco vBond Orchestrators.

   Send the list of controllers:

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

   b. Click **Controllers**.

   c. Click **Send to vBond**.

      Wait for the configuration task to complete. When the task is complete,

      - The standby Cisco vManage nodes become the active Cisco vManage nodes.
      - The previously active Cisco vManage nodes are no longer part of the overlay network.
      - The active Cisco vManage nodes have the configuration from the most recent configuration database backup.
      - Every controller establishes connection with the other controllers in the network.

   d. Click **WAN Edge List**.

   e. Click **Send to Controllers**.

8. Verify that the following are intact:

   - Policies
   - Templates
   - Controller and WAN edge device lists

9. Verify the valid Cisco vManage nodes.

   a. Log in to the CLI of each Cisco vBond Orchestrator and run the **show orchestrator valid-vmanage-id** command.

      In the command output, verify that the chassis numbers of the active and previously active Cisco vManage nodes are listed.

   b. Log in to the CLI of a WAN edge device and run the **show control valid-vmanage-id** command.

      In the command output, verify that the chassis numbers of the active and previously active Cisco vManage nodes are listed. Also, check whether the device is connected to the active Cisco vManage nodes and the Cisco vSmart Controllers.

10. Invalidate the previously active Cisco vManage nodes.

**Note** After you invalidate the Cisco vManage nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

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

b. Click **Controllers**.

c. For each previously active Cisco vManage node, click **...** and click **Invalidate**.

11. Verify the valid Cisco vManage nodes.

    a. Log in to the CLI of each Cisco vBond Orchestrator and run the **show orchestrator valid-vmanage-id** command.

    In the command output, verify that the chassis numbers of only the active Cisco vManage nodes are listed.

    b. Log in to the CLI of WAN edge device and run the **show control valid-vmanage-id** command.

    In the command output, verify that the chassis numbers of only the active Cisco vManage nodes are listed. Also, check whether the device is connected to the active Cisco vManage nodes and the Cisco vSmart Controllers.

The Cisco vManage cluster that was initially the standby cluster is now the active Cisco vManage cluster.

# Replace Faulty Cisco vSmart Controller

To replace a faulty Cisco vSmart Controller with a new instance, follow these steps:

1. Create a Cisco vSmart Controller instance. See Deploy the Cisco vSmart Controller.
2. Add Cisco vSmart Controller to the overlay network.
3. From the Cisco vManage menu, choose **Configuration** > **Devices**.
4. Click **Controllers**.
5. For the faulty Cisco vSmart Controllers, click **...** and click **Invalidate**.

   The **Invalidate** dialog box appears.

**Note** If you have not added a new Cisco vSmart Controller that can replace the faulty Cisco vSmart Controller, Cisco vManage indicates this through an error message. Click **Cancel** in the **Invalidate** dialog box and add a new Cisco vSmart Controller before invalidating the faulty instance.

6. In the **Invalidate** dialog box, do the following:

   a. Check the **Replace vSmart** check box.

   b. From the **Select vSmart** drop-down list, choose the new Cisco vSmart Controller that should replace the faulty instance.

c. Click **Invalidate**.

Cisco vManage launches the **Invalidate Device** and **Push CLI Tempalte Configuration** task. When these tasks are completed, the faulty Cisco vSmart Controller is invalidated and removed from the overlay network. The tenants that were served by the faulty Cisco vSmart Controller are now served by the new Cisco vSmart Controller that you chose as the replacement.