Cisco Catalyst SD-WAN Multitenancy Guide, Releases 26.x and Later

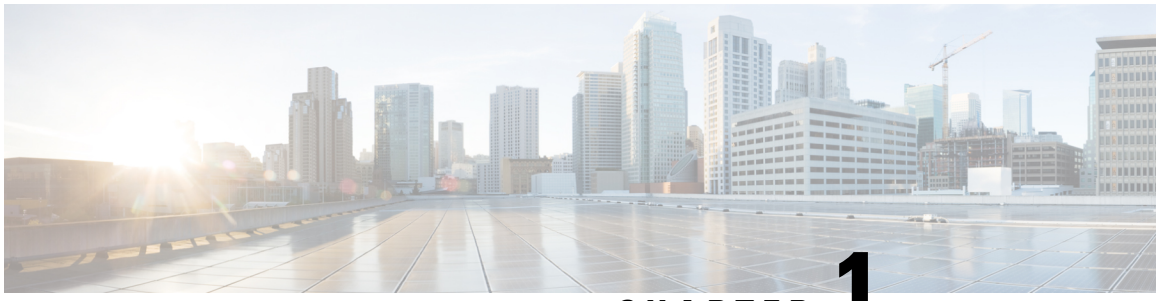
First Published: 2026-03-09

Last Modified: 2026-03-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2026 –2026 Cisco Systems, Inc. All rights reserved.

CONTENTS



CHAPTER 1

Multitenancy

Feature history for Cisco Catalyst SD WAN multitenancy

Table 1: Feature history

Feature name	Release information	Description
Multitenancy Support for Cisco Catalyst Cellular Gateways	Cisco IOS CG Release 17.14.1 Cisco Catalyst SD-WAN Control Components Release 20.14.1	Added multitenancy support for Cisco Catalyst Cellular Gateways.

Cisco Catalyst SD-WAN multitenancy

With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager.

The tenants share the same set of underlying Cisco SD-WAN Control Components:

- Cisco SD-WAN Manager
- Cisco SD-WAN Validator
- Cisco SD-WAN Controller

The tenant data is logically isolated on these shared control components.

Access to multitenancy

The service provider accesses Cisco SD-WAN Manager using a domain name mapped to the IP address of a Cisco SD-WAN Manager cluster and manages the multitenant deployment.

Each tenant is provided a subdomain to access a tenant-specific Cisco SD-WAN Manager view and manage the tenant deployment.

A service provider using the domain name managed-sp.com can assign tenants Customer1 and Customer2 the subdomains:

- customer1.managed-sp.com
- customer2.managed-sp.com

This allows the service provider to manage multiple tenants on the same set of SD-WAN Controllers instead of providing each customer a single-tenant setup with a dedicated set of SD-WAN Controllers.

Full enterprise multitenancy

Cisco Catalyst 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 Catalyst SD-WAN service offerings to their customers.

Security

Send and receive AAA traffic over management VPN 512 from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a.

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 Catalyst SD-WAN controllers can be deployed in:

- An organization data center on servers running VMware ESXi 6.7 or later, or the Kernel-based Virtual Machine (KVM) hypervisor.
- Amazon Web Services (AWS) servers hosted by Cisco CloudOps.

Tenant-specific Cisco SD-WAN Analytics

Cisco SD-WAN Analytics 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 SD-WAN Analytics insights for their overlay network by:

- Requesting a tenant-specific Cisco SD-WAN Analytics instance.
- Enabling data collection on SD-WAN Manager.

The service provider must enable cloud services on SD-WAN Manager in the provider view to facilitate the onboarding of the Cisco SD-WAN Analytics instance for the tenant overlay network.

Single tenant environments

A single tenant environment exclusively manages, and is responsible for, its own Cisco Catalyst SD-WAN Control Components and devices. All configured resources are visible to the single tenant administrator in the Cisco SD-WAN Manager interface.

Cloud-delivered Catalyst SD-WAN

Cloud-delivered Catalyst SD-WAN operates as a tenant within a multitenant environment rather than as a single tenant. Cloud-delivered Catalyst SD-WAN users do not see controller infrastructure settings in Cisco SD-WAN Manager. Their available information is limited to their own components and WAN edge devices.

For more information on Cloud-delivered Catalyst SD-WAN, see Cloud-delivered Cisco SD-WAN Getting Started Guide.

Multitenancy

- Multitenant Cisco SD-WAN Manager
- Multitenant Cisco SD-WAN Validator
- Multitenant Cisco SD-WAN Controller
- Tenant-specific WAN edge devices

Multitenant SD-WAN Manager

Defines how SD-WAN Manager is accessed and used by service providers and tenants in a multitenant deployment.

Provider view

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

In the Provider view, SD-WAN Manager:

- Provides service providers with an overall view of the SD-WAN multitenant deployment.
- Allows service providers to mange all Cisco Catalyst SD-WAN Validator and SD-WAN Controller devices.
- Enables service providers to monitor and manage each tenant deployment through the Provider-as-Tenant view.

Tenant view

In the tenant view, SD-WAN Manager allows individual tenants to:

- Monitor and manage their own deployment through a dashboard.

- Deploy and configure WAN edge devices.
- Configure custom policies on Cisco Catalyst SD-WAN Controllers.

  Cisco Catalyst SD-WAN Control Component infrastructure settings are not displayed in tenant view.

Multitenant SD-WAN Validator

Describes how SD-WAN Validator function in a multitenant environment.

SD-WAN Validators are deployed and configured by the service provider.

Only the provider can access a SD-WAN Validator through the SSH terminal.

In a multitenant deployment, SD-WAN Validators:

- Serve WAN edge devices of multiple tenants.
- Authenticate and validate WAN edge devices as they are added to the overlay network.

Multitenant SD-WAN Controllers

Explains the deployment and management of SD-WAN Controller in a multitenant environment.

SD-WAN Controllers are deployed by the service provider. Only the provider can:

- Create and attach device and feature templates to SD-WAN Controllers.
- Access a SD-WAN Controller through the SSH terminal.

Tenant assignment

- When a tenant is created, SD-WAN Manager assigns two SD-WAN Controllers for the tenant.
- The SD-WAN Controllers form an active-active cluster.
- Each tenant is assigned only two CSD-WAN Controllers.
- Before a tenant is created, two SD-WAN Controllers must be available to serve the tenant.

Controller selection

- When multiple pairs of CSD-WAN Controllers are available:
  - SD-WAN Manager assigns the pair connected to the lowest number of forecast devices.
  - If two pairs are connected to the same number of devices, the pair serving the lowest number of tenants is assigned.
- From Cisco vManage Release 20.9.1:
  - While onboarding a tenant, you can choose the pair of multitenant SD-WAN Controllers that serve the tenant.
  - After onboarding, the tenant can be migrated to a different pair if necessary.

- For more information, refer to the information about manual and automatic tenant placement in Multitenancy, on page 78.

- Each pair of SD-WAN Controllers can serve up to 24 tenants.

Tenant policy management

- Tenants can configure custom policies on their assigned SD-WAN Controllers.
- Cisco SD-WAN Manager notifies the Controllers to pull the policy templates.
- Controllers pull the templates and deploy the policy configuration for the specific tenant.

Provider access

- Only the provider can view events, audit logs, and OMP alarms for a SD-WAN Controller on SD-WAN Manager.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, a provider can view alarms and events for the sites and devices in its tenancy.

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.
- Remove the devices from the tenant network.
- Access the device through the SSH terminal.

A provider can manage the WAN edge devices only from the provider-as-tenant view. In the provider view, SD-WAN Manager does not show any WAN edge device information. Refer to SD-WAN Manager views for providers, on page 7.

SD-WAN Manager reports WAN edge device events, logs, and alarms only in the tenant and the provider-as-tenant views.

Feature availability

Some Cisco Catalyst SD-WAN features are available only in specific tenancy configurations.

Table 2: SD-WAN feature availability

Feature	Single Tenant	Multitenant	Catalyst SD-WAN Cloud
Identity Services Engine (ISE) integration	Yes	Yes (from SD-WAN Control Components 20.18.2)	Yes (for Early Adopter releases only)

Feature	Single Tenant	Multitenant	Catalyst SD-WAN Cloud
Intent-based hub and spoke topology	Yes	No	No
Controller group affinity	Yes	No	No
Cisco duo multifactor authentication (MFA) support	Yes	No	No
SD-Routing support without an SD-WAN Controller	Yes	No	No
Data stream and packet capture setting changes at tenant level	—	No, supported at provider level	No, supported at provider level

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
- Tenant role

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 SD-WAN Manager using the domain name of the service provider or by using the SD-WAN Manager 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.
- When you create a new provider user in SD-WAN Manager, including a netadmin user, by default, the user is not allowed SSH access to the SD-WAN Manager VM. To enable SSH access, configure SSH authentication using a AAA template and push the template to SD-WAN Manager. For more information on enabling SSH authentication, refer to the *Cisco Catalyst SD-WAN User Management Guide*.

SD-WAN Manager views for providers

Provider view

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

You can perform the following functions from the provider view:

- Provision and manage SD-WAN Manager, SD-WAN Validators, and SD-WAN Controllers.
- Add, modify, or delete tenants.
- Monitor the overlay network.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, view alarms and events for the sites and devices of its tenants.

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, SD-WAN Manager presents the provider-as-tenant view and displays the tenant dashboard for the selected tenant. The provider user has the same view of SD-WAN Manager 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.
- 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 SD-WAN Manager, 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, refer to the *Cisco Catalyst SD-WAN User Management Guide*.
- A tenant user can log in to SD-WAN Manager 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, SD-WAN Manager presents the tenant view and displays the tenant dashboard.

- 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 these functions:

- Provision and manage tenant routers
- Monitor overlay network of the tenant
- Create custom policies on the assigned Cisco SD-WAN Controller
- Upgrade the software on the tenant routers.
- Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, view tenant-specific information of controller connections and OMP statistics in a Cisco Catalyst SD-WAN network.

Provider and tenant remote servers and images

Cisco Catalyst SD-WAN Manager Release 20.14.1 and earlier releases

In these releases, remote servers and images operate as follows:

- Only the provider can add remote servers and images.
- The remote servers and images are visible to all tenants. Tenants can use the remote servers and images but can't edit them.

Cisco Catalyst SD-WAN Manager Release 20.15.1

In these releases, remote servers and images operate as follows:

- A tenant can add a remote server and remote image for both software images and virtual images. The remote server and image are visible only to the corresponding tenant and not to the provider or other tenants.
- The provider can add a remote server, a remote image, and a local image for both software images and virtual images in SD-WAN Manager.

Supported devices, hypervisor and persona for multitenancy

The following Cisco Catalyst SD-WAN edge devices support multitenancy.

Supported devices

Table 3: Supported devices

Platform	Device Models
Cisco IOS XE Catalyst SD-WAN device	• Cisco ASR 1000 Series Aggregation Services Routers • Cisco ISR 1000 Series Integrated Services Routers • Cisco ISR 4000 Series Integrated Services Routers • Cisco Catalyst 8200 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8000V Edge Software • Cisco ENCS Platforms
Cisco Catalyst Cellular Gateways	(From Cisco IOS CG Release 17.14.1 and Cisco Catalyst SD-WAN Control Components Release 20.14.1) • CG418-E • CG522-E

tit

Supported hypervisors 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)

SD-WAN Manager personas

The personas enable a predefined set of services on the Cisco SD-WAN Manager instance.

From Cisco vManage Release 20.6.1, a multitenant Cisco SD-WAN Manager instance can have one of these three personas.

Table 4: SD-WAN Manager 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

Supported hardware specifications for multitenancy

The supported hardware specifications for the SD-WAN Validator, SD-WAN Manager, and the SD-WAN Controllers are as follows:

Hardware specifications to support 50 tenants and 1000 devices

For more information on supported hardware specifications for the SD-WAN Validator, SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst 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 SD-WAN Validator, SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst 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 SD-WAN Validator, SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst 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 SD-WAN Validator SD-WAN Manager, and the Cisco SD-WAN Controllers see, Cisco Catalyst SD-WAN Controller Compatibility Matrix and Recommended Computing Resources.

Restrictions for multitenancy

Defines the limitations and unsupported configurations in a multitenant Cisco SD-WAN deployment.

- Connecting to a device by SSH

  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 SD-WAN Manager.

- IP address of the `vmanage_system` interface

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

- Launch the device SSH terminal from SD-WAN Manager and find the `vmanage_system` IP address from the first line of the log-in prompt, or
- 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, SD-WAN Manager 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 IOS XE Catalyst SD-WAN device, use the command, **request platform software sdwan software reset**.
- For Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and earlier releases, single-node SD-WAN Manager is not supported on a multitenant deployment.
  - A minimum of a 3-node SD-WAN Managercluster is required for a multitenant deployment.

- Upgrading devices during SD-WAN Controller or SD-WAN Validator upgrade

  When a SD-WAN Controller or SD-WAN Validator upgrade is in progress, upgrade of tenant edge devices is not supported.
- SD-WAN Controller group feature

  The SD-WAN Controller group feature is not supported in multitenant mode.
- Device site ID

  The WAN edge device's site ID must be different from the SD-WAN Control Components site ID when the SD-WAN Manager has different public and private IP addresses.
- Cannot change a SD-WAN Manager back to single tenant mode

  After you enable SD-WAN Manager for multitenancy, you cannot change it back to single tenant mode.

Initial setup for multitenancy

Prerequisites for Cisco Catalyst SD-WAN multitenancy

Ensure these prerequisites are met to successfully deploy and enable Cisco Catalyst SD-WAN m ultitenancy.

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

Table 5: Minimum software prerequisites for Cisco Catalyst SD-WAN multitenancy

Device	Software Version
Cisco SD-WAN Manager	Cisco vManage Release 20.6.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.6.1
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.6.1
Cisco IOS XE Catalyst SD-WAN Device	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

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.

- Ensure a new SD-WAN Manager software image is downloaded and installed instead of migrating an existing single-tenant instance to multitenant mode, even if all devices are invalidated or deleted.
- Follow the recommended hardware specifications in the Supported Devices and Hardware specifications section of this document.

Initial setup for Cisco Catalyst SD-WAN multitenancy

Follow these steps to set up Cisco Catalyst SD-WAN multitenancy.

Procedure

Step 1 Log in to SD-WAN Manager as the provider **admin** user.

Step 2 Create SD-WAN Manager cluster.

a) To support 50 tenants and 1000 devices across all tenants, create a 3-node Cisco SD-WAN Manager Multitenant cluster.

b) To support 100 tenants and 5000 devices across all tenants, create a 6-node Cisco SD-WAN Manager Multitenant cluster.

c) From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, create a 6-node Cisco SD-WAN Manager Multitenant cluster.

Step 3 Create and configure Cisco SD-WAN Validator instances. Refer to the Deploy SD-WAN Validator topic in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

While configuring Cisco SD-WAN Validator instances, configure the service provider organization name (`sp-organization-name`) and the organization name (`organization-name`). Refer to the information about configuring an organization name in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Example:

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

Step 4 Create Cisco SD-WAN Controller instances. Refer to the Deploy SD-WAN Controller topic in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

- To support 50 tenants and 1000 devices across all tenants, deploy 6 Cisco SD-WAN Controller instances.
- To support 100 tenants and 5000 devices across all tenants, deploy 10 Cisco SD-WAN Controller.

- From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy 16 Cisco SD-WAN Controllers.

Step 5 Add Cisco SD-WAN Controller to the overlay network.

Step 6 Onboard new tenants. See Add a new tenant, on page 27.

- Create a 3-node Cisco SD-WAN Manager Multitenant cluster
- Create a 6-node Cisco SD-WAN Manager Multitenant cluster
- Enable Multitenancy on Cisco SD-WAN Manager
- Add Cisco SD-WAN Controller

Create a 3-Node SD-WAN Manager multitenant cluster

To deploy and configure a 3-node SD-WAN Manager cluster to support a multitenant environment.

Procedure

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

Step 2 Create three SD-WAN Manager instances by installing the downloaded software image file. Refer to the Deploy SD-WAN Manager topic in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

- Deploy SD-WAN Manager servers with these hardware specifications: Hardware Specifications to Support 50 Tenants and 1000 Devices of this document
- Choose the Compute+Data persona for each SD-WAN Manager instance. Example: vManage1, vManange2, and vManage 3.

Step 3 Complete the following operations on the first SD-WAN Manager instance:

a) Configure the following using CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator 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
- Configure only one default route in VPN 0.

b) Enable Multitenancy on Cisco SD-WAN Manager.

c) (Optional) Using the CLI, install the Root CA certificate for the first SD-WAN Manager instance.

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

d) Complete these steps through SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.

e) Configure the cluster IP address of the SD-WAN Manager server. Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

Step 4 Complete the following operations on the second and third SD-WAN Manager instances (vManage2 and vManage 3 in the example):

a) Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator 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 the first SD-WAN Manager instance.

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

c) Complete the following through SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.

d) Log in to the SD-WAN Manager web application server. Refer to the Cisco Catalyst SD-WAN Manager How-Tos section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

e) Ping the OOB interfaces on the other two SD-WAN Manager instances and ensure they are reachable.

f) Configure the cluster IP address of the SD-WAN Manager server. Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

Enable multitenancy only on the first SD-WAN Manager instance.

Step 5 Log in to the first SD-WAN Manager instance and add the second instance to the cluster.

- The second instance reboots before being added to the cluster.
- While the second instance is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for the second instance shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding the second instance to the cluster.
- When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both the first and second instances, and their node personas.

Step 6 Repeat the previous step to add additional SD-WAN Manager instances to the cluster.

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 SD-WAN Manager multitenant cluster

To deploy and configure a 6-node SD-WAN Manager cluster to support a multitenant environment.

Procedure

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

Step 2 Create six SD-WAN Manager instances by installing the downloaded software image file. Refer to the Deploy SD-WAN Manager topic in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

- To support 100 tenants and 5000 devices across all tenants, deploy SD-WAN Manager servers having the hardware specifications in the table Hardware Specifications to Support 100 Tenants and 5000 Devices of this document.
- From Cisco IOS XE Release 17.6.3a and Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy SD-WAN Manager servers with these hardware specifications: Hardware Specifications to Support 150 Tenants and 7500 Devices
- Choose the Compute+Data persona for three SD-WAN Manager instances Example: vManage1, vManange2, and vManage 3. Choose the Data persona for the other three SD-WAN Manager instances. Example: vManage4, vManage5, and vManage6.

Step 3 Complete the following operations on the first SD-WAN Manager instance:

a) Configure the following using CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator 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
- Configure only one default route in VPN 0.

b) Enable Multitenancy on Cisco SD-WAN Manager.

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

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

d) Complete the following through SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.

e) Configure the cluster IP address of the SD-WAN Manager server. Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

Step 4 Complete the following operations on the second and third SD-WAN Manager instances (vManage2 and vManage 3 in the example):

a) Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name
- Cisco SD-WAN Validator 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.

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

c) Complete the following through the Cisco SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.

d) Log in to the SD-WAN Manager web application server. Refer to the Cisco Catalyst SD-WAN Manager How-Tos section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
e) Ping the OOB interfaces on the other two SD-WAN Manager instances and ensure they are reachable.
f) Configure the cluster IP address of the SD-WAN Manager server. Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

Do not enable multitenancy on vManage2 and vManage3.

Step 5 Log in to the first SD-WAN Manager instance and add the second instance to the cluster.

- The second instance (vManage2 in the example) reboots before being added to the cluster.
- While the second instance is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for the second instance shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding the second instance to the cluster.
- When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both the first and second instances, and their node personas.

Step 6 Repeat the previous step to add additional SD-WAN Manager instances to the cluster (vManage3 through vManage6 in the example).

Enable multitenancy on SD-WAN Manager

Administrator triggered disaster recovery is supported for multitenant clusters from Cisco vManage Release 20.6.1 or later releases.

After you enable multitenancy on SD-WAN Manager, you cannot migrate it back to single tenant mode.

SD-WAN Manager reboots in multitenant mode and when a provider user logs in to SD-WAN Manager, the provider dashboard appears.

Before you begin

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

Procedure

Step 1 Launch SD-WAN Manager using the URL https://vmanage-ip-address:port. Log in as the provider **admin** user.
Step 2 From the SD-WAN Manager menu, choose **Administration** > **Settings** > **Tenancy Mode**. If you are using SD-WAN ManagerRelease 20.12.x or earlier, click **Edit**.
Step 3 In the Tenancy field, click **Multitenant**.
Step 4 In the **Domain** field, enter the domain name of the service provider (for example, managed-sp.com).
Step 5 Enter a Cluster Id (for example, cluster-1 or 123456).

Step 6 Click **Save**. If you are using SD-WAN Manager Release 20.12.x or earlier, click **Proceed** to confirm that you want to change the tenancy mode.

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 SD-WAN Manager cluster need to be deployed. For more details on provider and tenant DNS requirements, refer to step 3d in Add a new tenant, on page 27.

Add SD-WAN Controller

Follow these steps to add SD-WAN Controller

Procedure

Step 1 Log in to SD-WAN Manager as the provider **admin** user.

Step 2 From the SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 3

Step 4 Click **Controllers**.

Step 5 Click **Add Controller**.

Step 6 In the **Add Controller** dialog box, do the following:

a) In the **Controller Management IP Address** field, enter the system IP address of the SD-WAN Controller.
b) Enter the **Username** and **Password** required to access the Cisco SD-WAN Controller.
c) Select the protocol to use for control-plane connections. The default is **DTLS**.
d) If you select **TLS**, enter the port number to use for TLS connections. The default is 23456.
e) Check the **Generate CSR** check box for SD-WAN Manager to create a Certificate Signing Request.
f) Click **Add**.

Step 7 From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.

For the newly added SD-WAN Controller, the Operation Status reads CSR Generated.

a) For the newly added SD-WAN Controller, click **More Options** icon and click **View CSR**.
b) Submit the CSR to the Certificate Authority (CA) and obtain a signed certificate.

Step 8 Install certificate.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Install Certificate**.
c) In the **Install Certificate** dialog box, paste the **Certificate Text** or click **Select a file** upload the certificate file.
d) Click **Install**.

a. SD-WAN Manager installs the certificate on the SD-WAN Controller. SD-WAN Manager also sends the serial number of the certificate to other controllers.

b. On the **Configuration** > **Certificates** page, the **Operation Status** for the newly added SD-WAN Controller reads as **Validator Updated**.

c. 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.

Step 9 Change the mode of the newly added SD-WAN Controller to **Manager Mode** by attaching a template to the device.

a) From the SD-WAN Manager menu, choose **Configuration** > **Templates**.
b) Click **Device Templates**.

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 SD-WAN 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**.

1. SD-WAN Managerpushes the configuration from the template to the new controller.
2. In the **Configuration** > **Devices** page, the **Mode** for the SD-WAN Controller shows **Manager Mode**. The new SD-WAN 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 C to the overlay to support up to 100 tenants and 5000 devices. From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, you can expand the Cisco SD-WAN Manager cluster and add additional Cisco SD-WAN Controllers to the overlay to support up to 150 tenants and 7500 devices.

- Prerequisites to expand a multitenant deployment
- Restrictions for expanding a 3-node cluster to a 6-node cluster
- Expand a 3-node cluster to a 6-node cluster

Prerequisites to expand a multitenant deployment

A multitenant Cisco Catalyst 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.

- Expand the existing 3-node Cisco SD-WAN Manager cluster to a 6-node cluster.
- To support up to 100 tenants and 5000 devices, you must have 10 SD-WAN Controllers in the overlay. So, deploy 4 SD-WAN Controllers in addition to the 6 existing SD-WAN Controllers in the overlay.
- To support up to 150 tenants and 7500 devices, you must have 16 SD-WAN Controllers in the overlay. So, deploy 10 SD-WAN Controllers in addition to the 6 existing SD-WAN Controllers in the overlay.
  - Create SD-WAN Controller instances. Refer to the information about deploying an SD-WAN Controller in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
  - Add Cisco SD-WAN Controllers to the overlay network.

- You can now add more tenants or allow your existing tenants to add more devices subject to the relevant limits.
- Starting from Cisco SD-WAN Manager Release 20.13.1, you can expand a single node cluster into 3 or 6 node clusters.

Restrictions for expanding a 3-node cluster to a 6-node cluster

You can only expand a 3-node Cisco SD-WAN Manager cluster to a 6-node Cisco SD-WAN Manager cluster. Expansion of the 3-node cluster to other cluster sizes is not supported.

Expand a 3-node cluster to a 6-node cluster

- To support 100 tenants and 5000 devices: Upgrade the three SD-WAN Manager servers in the existing 3-node cluster to the hardware specifications in the table Hardware Specifications to Support 100 Tenants and 5000 Devices of this document.
- From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices: Upgrade the three SD-WAN Manager servers in the existing 3-node cluster to the hardware specifications in the table Hardware Specifications to Support 150 Tenants and 7500 Devices of this document.

Procedure

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

Step 2 Create three SD-WAN Manager instances (for example, vManage1, vManage2, and vManage3) by installing the downloaded software image file. Refer to the information about deploying an SD-WAN Manager in the Overlay Network Bring-Up Process section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

- Deploy SD-WAN Manager servers having the hardware specifications in the table Hardware Specifications to Support 100 Tenants and 5000 Devices of this document.

  From Cisco IOS XE Release 17.6.3a, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices, deploy SD-WAN Manager servers with these hardware specifications: Hardware Specifications to Support 150 Tenants and 7500 Devices of this document.

- Choose the **Data** persona for each SD-WAN Manager instance.

Step 3 Complete the following operations on the first through third SD-WAN Manager instances (vManage1 through vManage3 in the example):

a) Configure the following using the CLI:

- System IP address
- Site ID
- Service Provider organization name (`sp-organization-name`)
- Organization-name

- Cisco SD-WAN Validator 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
- Configure only one default route in VPN 0.
- Do not enable multitenancy on vManage1 through vManage3.

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

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

c) Complete these steps through the SD-WAN Manager:

1. Generate a certificate signing request. Refer to the Certificate Management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
2. After getting the certificate signed, install the certificate.
3. Log in to the SD-WAN Manager web application server. Refer to the Cisco Catalyst SD-WAN Manager How-Tos section of the *Cisco Catalyst SD-WAN Getting Started Guide*.
4. Ping the OOB interfaces on the other SD-WAN Manager instances and ensure they are reachable.
5. Configure the cluster IP address of the SD-WAN Manager server. Refer to the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

Step 4 Log in to SD-WAN Manager on the existing 3-node cluster and add an SD-WAN Manager instance to the cluster.

a. The instance reboots before being added to the cluster.

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

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

Step 5 Repeat the previous step and add the remaining SD-WAN Manager instances to the cluster.

Upgrade SD-WAN Controller and Edge Device Software

Use these steps to upgrade all Cisco SD-WAN components to the required software versions for multitenancy support.

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.

Before you begin

Minimum software requirements for SD-WAN Controllers and WAN edge devices:

Device	Software Version
SD-WAN Manager	Cisco vManage Release 20.4.1 or later
SD-WAN Validator	Cisco SD-WAN Release 20.4.1 or later
SD-WAN Controller	Cisco SD-WAN Release 20.4.1 or later
Cisco IOS XE Catalyst SD-WAN device	Cisco IOS XE Release 17.4.1 or later

Procedure

Step 1 Upgrade the software on the three SD-WAN Manager instances in the cluster to Cisco vManage Release 20.6.1 or a later release. For more information, refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

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

Step 2 After the SD-WAN Manager software is upgraded to Cisco vManage Release 20.6.1 or a later release, log in to SD-WAN Manager.

Step 3 Upload the Cisco SD-WAN Release 20.6.1 or a later release and the Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or a later release software to SD-WAN Manager. Refer to the information about adding an image to the software repository in the Manage Software and Upgrade section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 4 Upgrade the Cisco SD-WAN Validator software to Cisco SD-WAN Release 20.6.1 or a later release.

Refer to:

- Information about upgrading the software image on a device in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*
- Information about activating a new software image in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*

Step 5 Enable maintenance window on SD-WAN Manager. Refer to the information about configuring or canceling an SD-WAN Manager server maintenance window in the Basic Settings for Cisco SD-WAN Manager section of the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

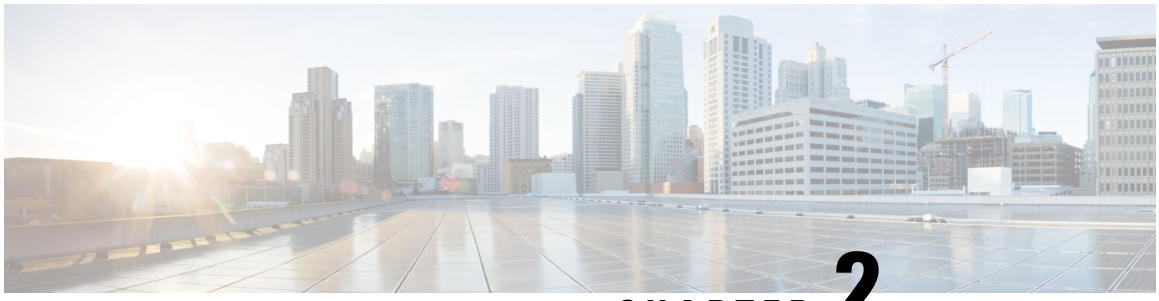
Step 6 Upgrade the SD-WAN Controller software to Cisco SD-WAN Release 20.6.1 or a later release.

Step 7 Upgrade the Cisco IOS XE Catalyst SD-WAN device software to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or a later release.

Refer to:

- Information about upgrading the software image on a device in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*

- Information about activating a new software image in the Manage Software Upgrade and Repository section of the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*



CHAPTER 2

Multitenancy: Tenant Management

Feature history for tenant management

This table describes the developments of this feature, by release.

Table 6: Feature history

Feature name	Release information	Description
Tenant Device Forecasting	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a 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 Catalyst SD-WAN controller resources efficiently.

Tenant management

A tenant or the provider acting on behalf of a tenant can:

- Add WAN edge devices to the tenant network.
- Configure the devices.
- Remove the devices from the tenant network.
- Access the device through the SSH terminal.

Tenant device forecasting

When a service provider adds a new tenant to the multitenant Cisco Catalyst SD-WAN deployment, they can forecast the number of WAN edge devices the tenant may deploy in their overlay network. Cisco SD-WAN Manager enforces this forecast limit. If the tenant tries to add devices beyond this limit, Cisco SD-WAN Manager returns an appropriate error message, and the device addition fails.

From Cisco IOS XE Release 17.6.2 and Cisco vManage Release 20.6.2, you can modify a tenant's device forecast after adding the tenant.

Benefits of tenant device forecasting

- The service provider uses Cisco Catalyst SD-WAN controller resources more efficiently.
- A multitenant deployment supports a fixed number of WAN edge devices across all tenants, depending on the configuration. By forecasting how many devices each tenant may add, the service provider assigns a quota for each tenant from the overall pool of supported edge devices.

Restrictions for tenant management

In a multitenant deployment, a tenant can only add up to 1000 devices to their overlay network.

Each pair of SD-WAN Controllers can serve a maximum of 24 tenants and 1000 tenant devices.

Prerequisites for adding a tenant

Follow these prerequisites to prevent configuration or synchronization failures when adding a tenant.

- Ensure at least two Cisco SD-WAN Controllers are operational and in Manager mode before adding a new tenant.
  - A controller enters Manager mode when a template is pushed from SD-WAN Manager.
  - SD-WAN Controllers in CLI mode cannot serve multiple tenants.
- Ensure that at least two controllers can serve the new tenant. If not, add two controllers and change their mode to Manager.
- When adding a second tenant immediately after another, SD-WAN Manager processes them sequentially, not in parallel.
- Each tenant must have a unique Virtual Account (VA) on Plug and Play Connect within Cisco Software Central. The tenant VA must belong to the same Smart Account (SA) as the provider VA.
- For on-premises deployments, create a **Validator** controller profile for the tenant on Plug and Play Connect.

Table 7: 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.

Field	Description/Value
Organization Name	Enter tenant organization in the format <SP Org Name>-<Tenant Org Name>. The organization name can contain up to 50 characters. A mismatch between the controller profile organization name and the tenant organization name causes device synchronization to fail.
Primary Controller	Enter the host details for the primary Cisco SD-WAN Validator.

- If you are using a Cisco-hosted multitenant environment, see Add a new tenant in Cisco-hosted multitenant environment

Add a new tenant

Use these steps to add a new tenant in SD-WAN Manager for multitenancy deployment.

Procedure

Step 1 Log in to SD-WAN Manager as the provider admin user.

Step 2 Navigate to **Administration** > **Tenant Management**.

Step 3 Click **Add Tenant**.

Step 4 Enter tenant information.

Table 8: Tenant information

Item	Description
Tenant Name	Enter a name for the tenant. The name must match the Virtual Account used for the tenant.
Tenant Description	Enter a description with up to 256 alphanumeric characters.

Item	Description
Organization Name	Enter the organization name (case-sensitive, unique per tenant). • Format: <Provider Org Name>-<Tenant Org Name> • Maximum length: 50 characters Example: If the provider organization name is 'EFT20.17-VA-Main – 841534' and the tenant organization name is 'T1', enter the organization name as **`EFT20.17-VA-Main – 841534-T1`**. The tenant organization name can be T1 for Tenant 1, T2 for Tenant 2, and so on.

Step 5 Enter the **URL Subdomain Name**.

Enter the fully qualified subdomain of the tenant.

The URL must include the service provider's domain (example: `customer1.managed-sp.com`) and follow the domain naming convention set in **Administration** > **Settings** > **Tenancy Mode**.

Step 6 Configure DNS.

a) For on-premises deployment, add the tenant's FQDN to DNS and map it to all three SD-WAN Manager cluster IPs.

Provider level:

Create DNS A record and map it to the IP addresses of the SD-WAN Manager instances running in the Cisco SD-WAN Manager cluster. The A record is derived from the domain and cluster ID created while enabling multitenancy.

For example, if domain is `sdwan.cisco.com` and Cluster ID is `vmanage123`, then configure the A record as `vmanage123.sdwan.cisco.com`.

If you do not update the DNS entries, SD-WAN Manager fails to authenticate when you log in. To verify if DNS is configured correctly, execute `nslookup vmanage123.sdwan.cisco.com`.

Tenant level:

Create a DNS CNAME record for each tenant and map it to the FQDN created at the provider level. You do not need to include the cluster ID for the CNAME record.

For example, if the domain is `sdwan.cisco.com` and the tenant name is `customer1`, configure the CNAME record as `customer1.sdwan.cisco.com`.

To verify if DNS is configured correctly, execute **`nslookup customer1.sdwan.cisco.com`**.

b) For a cloud deployment, SD-WAN Manager automatically adds the tenant's fully qualified sub-domain name (FQDN) to DNS during tenant creation. After adding the tenant, it may take up to one hour for the FQDN to resolve.

Step 7 In the **Number of Devices** field, enter the number of WAN edge devices the tenant can deploy.

Adding more devices than allowed will trigger an error.

Step 8 Click **Save**.

When you add a tenant, SD-WAN Manager automatically:

- Creates the tenant.
- Assigns two SD-WAN Controllers to the tenant and pushes a CLI template to configure tenant information on them.
- Sends the tenant and controller details to the SD-WAN Validator.

What to do next

The **Create Tenant** window 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.

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

View tenant information

From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, you can view detailed tenant information.

Use these steps to view detailed information about a tenant.

Procedure

Step 1 From Cisco SD-WAN Manager menu, click **Administration** > **Tenant Management**.

Step 2 Click **Tenant** to view detailed tenant information.

Table 9: Tenant details

Field	Description
Tenant Name	Name of the tenant.
Description	Tenant description
Controllers	SD-WAN Controllers assigned to the tenant.
Forecasted Edge Count	Predicted number of WAN edge devices.
Total Edge Count	Total number of both multitenant and single-tenant edge devices.
Multi-Tenant WAN Edge Devices	Click the non-zero number to view the number of multitenant edge devices.
Tenant-Provider VPN Mapping	Click the non-zero number to view tenant and device VPN mappings.
Service Connector	Shows the multitenant edge device that provides VXLAN connectivity to tenants.

Field	Description
Notifications	Indicates whether webhook notifications are managed by the tenant or provider.
AAA	Indicates whether remote AAA is managed by the tenant or provider.
Controller Visibility	Indicates whether controller visibility is enabled or disabled.

Restrict a tenant's access

Using this procedure, a provider admin is able to suspend or restore a tenant's access to SD-WAN Manager.

A provider administrator can control a tenant's access. They can suspend or restore SD-WAN Manager access for individual tenants. After suspension of access, there are changes in tenant's access to SD-WAN Manager.

This table lists what access is restricted or allowed after a tenant is suspended.

Table 10: Tenant's access after suspension

Post-Suspension Access	Descripton
Restricted for a tenant user	No access to the SD-WAN Manager GUI.
	No access to the SD-WAN Manager APIs.
	Cannot schedule or perform configuration or operational changes.
	Existing logged-in sessions are forcibly terminated.
Accessible for a provider-admin user	Data plane traffic continues uninterrupted.
	Monitoring data (device statistics and SD-WAN Analytics) remains available.
	Scheduled reports continue to be delivered.
	Webhook notifications, including critical alarms, continue to work.

Note After suspending a tenant access, provider-as-tenant view remains available to the provider.

Before you begin

You must have provider admintrator user access.

Follow these steps to modify a tenant’s access in SD-WAN Manager:

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admintrator user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.

Step 3 To modify user access, click **...** adjacent to the tenant and click **Edit Tenant**.
The **Edit Tenant** side panel appears.

Step 4 Toggle the **user access** button to suspend access.

The provider has access to tenant information even after suspending user access for the tenant.

What to do next

Verify that a tenant's access is suspended by reviewing the user acess column on the **Tenant Management** page.

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 34.

Use these steps to delete a tenant.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.

Step 3 In the left pane, click the name of the tenant.

The tenant information is displayed in a pane on the right.

Step 4 In the right pane, click the trash icon.

Step 5 In the Delete Tenant dialog box, enter the provider admin password and click **Save**.

Add a tenant in a Cisco-hosted multitenant environment

Use these steps to add a new tenant in a Cisco-hosted multitenant environment.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 Navigate to **Administration** > **Tenant Management**.

Step 3 Click **Add Tenant**.

Step 4 Enter tenant information.

Table 11: Tenant information

Item	Description
Tenant Name	Enter a name for the tenant.
Tenant Description	Enter a description with up to 256 alphanumeric characters.
Organization Name	Enter the organization name (case-sensitive, unique per tenant). • Format: <SP Org Name>-<Tenant Org Name> • Maximum length: 50 characters 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. Any mismatch with controller profile causes device sync failure

Step 5 Enter the sub-domain URL in FQDN format.

The sub-domain name must include `sdwan.cisco.com`.

For example, a valid sub-domain could be `Eftt1.sdwan.cisco.com`.

Ensure the sub-domain is unique by performing a nslookup or ping on the expected domain. If the domain already exists, choose a different URL.

The tenant's FQDN is automatically added to DNS during the tenant creation process. After adding the tenant, it may take up to one hour for the FQDN to resolve.

Step 6 In the **Number of Devices** field, enter the maximum number of WAN edge devices the tenant can deploy field.

Exceeding this limit will cause Cisco SD-WAN Manager to report an error and prevent additional device additions.

Step 7 Choose **Auto placement** or **manual** option for controller assignment.

Step 8 Click Save.

After tenant creation completes, Cisco SD-WAN Manager automatically generates the controller profile in the tenant's Virtual Account and creates the FQDN. You will receive an email notification once the process is finished.

Manage tenant WAN edge devices

Use these procedures to add or delete a WAN edge device from a tenant network.

- Add a WAN edge device to a tenant network
- Delete a WAN edge device from a tenant network

Add a WAN edge device to a tenant network

Register and configure a WAN edge device in SD-WAN Manager for a tenant.

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 IOS XE Catalyst SD-WAN device, use the command request platform software sdwan software reset.

Procedure

Step 1 Log in to SD-WAN Manager.

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

Step 2 Upload the file containing the device serial numbers to Cisco SD-WAN Manager.

Step 3 Validate the uploaded device and send the details to the controllers.

Step 4 Create a configuration template for the device and attach the device to the template.

Enter the organization-name in the format `<SP Org Name>-<Tenant Org Name>`.

While configuring the device, set the **Service Provider Organization Name** and the **Tenant Organization Name** as shown in the example below:

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

Step 5 Bootstrap the device using the bootstrap configuration generated through SD-WAN Manager, or manually create the initial configuration on the device.

Step 6 If using Enterprise Certificates for authentication, follow these steps:

a) Download the CSR from SD-WAN Manager.

b) Get the CSR signed by the Enterprise CA.

c) Install the certificate on SD-WAN Manager.

Delete a WAN edge device from a tenant network

Follow these steps to remove a WAN Edge device from a tenant's network in SD-WAN Manager.

Procedure

Step 1 Log in to SD-WAN Manager.

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

Step 2 Detach the device from any configuration templates.

Step 3 Delete the device.

Manage tenant data

You can back up, restore, and manage tenant configuration data in SD-WAN Manager.

- Back up tenant data
- Create data backup file
- Restore tenant data backup file
- Monitor data backup restore
- Delete tenant data backup file

Back up tenant data

You can back up configuration data for a tenant in SD-WAN Manager.

The tenant data backup solution of SD-WAN Manager multitenancy provides these functionalities:

- Create, list, and extract configuration backup files.
- Back up configuration database of a specific tenant with an option to restore it later.
- Delete back up files of a tenant stored in SD-WAN Manager.

Usage

Tenant data backup operations can be performed:

- By a tenant administrator in the tenant view.
- By a provider administrator in the provider-as-tenant view.

Allowed backup operations

At any given time, a tenant is allowed to perform only one backup operation. The operation must complete before starting a new one. These operations are supported:

- Back up a single configuration database
- Download the backup file
- Restore or import backup files
- Delete backup files
- List backup files

Limitations

Defines the limitations of provider access for backing up data.

- A provider cannot back up provider data using this solution.
- A provider can back up all tenant information at once only by backing up all tenants' configuration databases using CLI.

View back up data

The tenant data backup solution creates a task in the tenant view of SD-WAN Manager.

Tenants can monitor the progress of the operation from the task view of the tenant dashboard.

Backup and restore guidelines for tenant data

You can enable tenants to securely back up, store, and restore configuration data in Cisco SD-WAN Manager while maintaining consistency and operational limits.

Follow these guidelines for tenant backup and restore operations.

- The tenant backup file follows the format: `Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz`.
- Backup operation is read-only on the configuration database.
- To ensure data consistency, do not perform major network changes while the operation is in progress.
- Multiple tenants can perform backup and restore operations in parallel.
- A tenant cannot start other backup operations when a restore operation is in progress.
- Backup and restore operations must be performed on Cisco SD-WAN Manager instances running identical software versions.
- A tenant can store a maximum of three backup files in Cisco SD-WAN Manager.

  If three files already exist, the earliest backup file is deleted when a new backup is generated.
- Backup files can also be downloaded and stored outside the Cisco SD-WAN Manager repository.

- Ensure the following parameter values match in both the backup file and the target setup:
  - Tenant ID
  - Organization Name
  - SP Organization Name

Create data backup file

To create, verify, extract, and list tenant configuration backup files using Cisco SD-WAN Manager APIs.

Procedure

Step 1 Log in to Cisco SD-WAN Manager.

- If you are 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 are a tenant user, log in as the **tenantadmin**.

Step 2 Modify the URL path for REST API access.

In the address bar, update the URL path with `dataservice`.

Example:

https://<tenant_URL>/dataservice

Step 3 Create a configuration backup file by using the following API:

https://<tenant_URL>/dataservice/tenantbackup/export.

Step 4 Once the backup file is created, Cisco SD-WAN Manager task view shows the generated process ID.

Example:

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

Step 5 Verify the task status.

Use the obtained process ID with the following API, the response provides task details in JSON format.

Example:

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

Step 6 Extract or download the backup file.

After the task completes, the backup file appears under the **data** section of the JSON task file. To extract or download it, use:

`https://<tenant_URL>/dataservice/tenantbackup/download/1570057020772/backup_1570057020772_100919-181838.tar.gz`

Step 7 List available backup files.

Use the following API to list all backup files stored in Cisco SD-WAN Manager.

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

Restore tenant data backup file

Use these steps to restore tenant data backup file.

Before you begin

To run the restore API, use Postman or an equivalent API testing tool. Postman is used here as an example. You can download it from the Postman website.

Procedure

Step 1 Open Google Chrome or another browser and enable Developer Mode.

Step 2 Log in to Cisco SD-WAN Manager.

- If you're a provider user, log in as the admin and from 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.

Step 3 Get header information for the restore API:

- Click the **Network** tab to view network capture.
- In the network capture view, click the **Name** column to sort listed items.
- Search and click **index.html**.
- Click the **Headers** tab and expand **Request Headers**.
- Copy all text under Request Headers to the clipboard.

Step 4 Open Postman UI to import backup files using Postman:

a) To disable SSL certificate verification, go to **Postman** > **Preferences** > **General** > **Request** and turn off SSL Certificate Verification.
b) Create a new tab.
c) Click **Headers**, then **Bulk Edit**, and paste the copied text from Request Headers.
d) From the GET drop-down, choose **POST**.
e) In the **Request URL** field, enter the tenant URL with the restore API:

```
https://<tenant_URL>/dataservice/tenantbackup/import
```

f) Click the **Body** tab and select **form-data**.
g) Under the KEY column, enter *bakup.tar.gz*
h) Click **Send** to run the API.
i) In the Response section, view the JSON confirmation showing that the file was restored.

Example:

```
{
  "processId": "40adb6c0-eacc-4ad4-ba6c-2c2da2e96d1d",
```

```
  "status": "Import Successfully Submitted for tenant 1579026919487"
}
```

Monitor backup data restore

You can monitor the progress of the restoration in either of these ways:

- Use Cisco SD-WAN Manager task view that indicates whether the backup file is imported successfully. You can view the process identifier of the created process or task.

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

- Use the following URL with the process ID to check status directly:

```
https://<tenant_URL>/dataservice/device/action/status/<processId>
```

Example:

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

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 34.

Use these steps to delete a tenant.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.

Step 3 In the left pane, click the name of the tenant.

The tenant information is displayed in a pane on the right.

Step 4 In the right pane, click the trash icon.

Step 5 In the Delete Tenant dialog box, enter the provider admin password and click **Save**.

View tenants associated with a Cisco SD-WAN Controller

Use these steps to view tenants associated with a Cisco SD-WAN Controller.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 Click a **Controller** connection number to display a table with detailed information about each connection.

Cisco SD-WAN Manager displays a table that provides a summary of the Cisco SD-WAN Controllers and their connections.

Step 3 For a Cisco SD-WAN Controller, click **...** and click **Tenant List**.

Cisco SD-WAN Manager displays a summary of tenants associated with the Cisco SD-WAN Controller.

View OMP statistics per tenant on a Cisco SD-WAN Controller

Use these steps to view OMP statistics per tenant on a Cisco SD-WAN Controller.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the Cisco SD-WAN Managermenu, choose **Monitor** > **Devices**.

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

Step 3 In the table of devices, click on the hostname of a Cisco SD-WAN Controller.

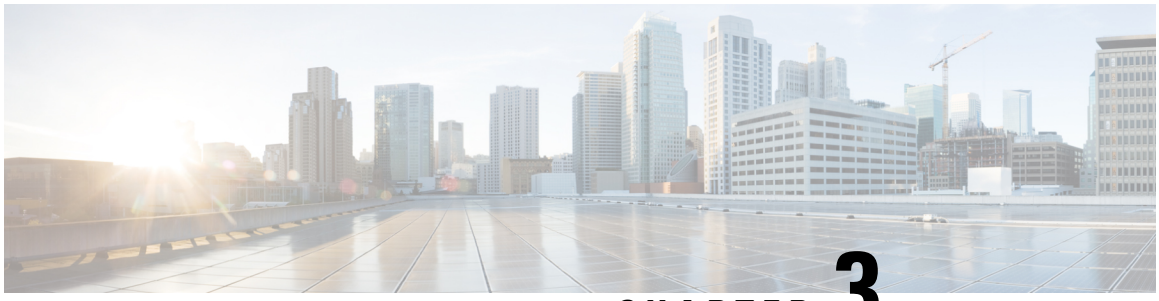
Step 4 In the left pane, click **Real Time**.

Step 5 In the **Device Options** field, enter **OMP** and select the OMP statistics you wish to view.

Step 6 In the **Select Filters** dialog box, click **Show Filters**.

Step 7 Enter the **Tenant Name** and click **Search**.

Cisco SD-WAN Manager displays the selected OMP statistics for the particular tenant.



CHAPTER 3

Multitenancy: Migration

Feature history for multitenancy migration

Table 12: Feature history

Feature name	Release information	Description
Migrate Multitenant Cisco Catalyst SD-WAN Overlay	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature enables you to migrate a multitenant Cisco Catalyst SD-WAN overlay comprising shared Cisco SD-WAN Manager instances and Cisco SD-WAN Validator, and tenant-specific Cisco SD-WAN Controllers to a multitenant overlay comprising shared Cisco SD-WAN Manager instances, Cisco SD-WAN Validator, and Cisco SD-WAN Controllers.

Feature name	Release information	Description
Migration of a tenant from a multitenant overlay to a single-tenant deployment	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature supports the migration of a tenant from a multitenant overlay to a single-tenant deployment. To migrate a tenant between two Cisco Catalyst SD-WAN deployments, move the tenant configurations, statistical data, and WAN edge devices from one deployment to another.

Tenant migration in a multitenant deployment

The tenant migration involves

- export of tenant data from the source Cisco SD-WAN Manager instance, and
- and import of data to the destination Cisco SD-WAN Manager instance.

After the data migration is complete, the tenant WAN edge devices with active control connections with the source Cisco SD-WAN Manager migrate and form connections with the destination Cisco SD-WAN Manager.

Availability

- From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and Cisco vManage Release 20.6.1, migration of a single-tenant overlay to a multitenant deployment is supported only with Cisco Catalyst SD-WAN controllers deployed on-premises.
- From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1, migration of a tenant from a multitenant overlay to a single-tenant deployment is supported.

Restrictions for migration of a tenant from a multitenant overlay to a single-tenant deployment

Defines the restrictions during tenant migration in Cisco Catalyst SD-WAN deployments.

- Change in the tenant organization name is not supported when the tenant moves from the Cisco Catalyst SD-WAN source to destination deployment.
- Tenant migration with multitenant WAN edge devices is not supported.
- Data traffic loss is expected during migration as devices are migrating from one set of SD-WAN Controllers to another.
- All user passwords are set to the default Cisco password on the destination overlay. The default password is `Cisco#123@Viptela`.
- Statistical data of the tenant that can be relearned by destination SD-WAN Manager is not migrated.

- The migration procedure does not support multiple imports on the same destination SD-WAN Manager. Reinitialize the destination SD-WAN Manager to allow import again.

Migrate single-tenant Cisco Catalyst SD-WAN overlay to multitenant Cisco Catalyst SD-WAN deployment

Prerequisites to migrate single-tenant SD-WAN overlay to multitenant SD-WAN deployment

Follow these prerequistes to ensure a successful migration.

- Ensure that the edge devices in the single-tenant deployment can reach the SD-WAN Validator in the multitenant deployment
- Ensure that the template, routing, and policy configuration on the edge devices is synchronized with the current configuration on SD-WAN Manager.
- Configure a maintenance window for the single-tenant overlay before performing this procedure. Refer to the information about configuring an SD-WAN Manager server maintenance window in the *Cisco Catalyst SD-WAN Control Components and Device Management Guide.*
- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.
- The software versions of the SD-WAN Controllers and WAN edge devices must be identical in both the single-tenant and multitenant deployments.

Minimum software requirements for to migrate a single-tenant overlay

Table 13: Software requirements

Device	Software version
Cisco SD-WAN Manager	Cisco vManage Release 20.6.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.6.1
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.6.1
Cisco IOS XE Catalyst SD-WAN device	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

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

Table 14: Software requirements

Device	Software version
Cisco SD-WAN Manager	Cisco vManage Release 20.6.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.6.1
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.6.1
Cisco IOS XE Catalyst SD-WAN device	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a

Migrate single-tenant SD-WAN overlay to multitenant SD-WAN deployment

Migration of a single-tenant overlay to a multitenant deployment is only supported with the SD-WAN Controllers deployed on-premises. Migration is yet to be supported with cloud-hosted SD-WAN Controllers.

Procedure

Step 1 Export the single-tenant deployment and configuration data from a SD-WAN Controller instance controlling the overlay.

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

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

Body	Required Format: Raw JSON `{ "desc": <tenant_description>, "name": <tenant_name>, "subdomain": <tenant_name>.<domain>, "orgName": <tenant_orgname > }` Field Description: • `desc`: A description of the tenant. The description can be up to 256 characters and can contain only alphanumeric characters. • `name`: Unique name for the tenant in the multitenant deployment. • `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`. • `orgName`: Name of the tenant organization. The organization name is case-sensitive.
Response	Format: JSON `{ "processId": <vManage_process_ID>, }`

Step 2 Check the status of the data export task in SD-WAN Manager.

When the task succeeds, download the data using the URL
`https://ST-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz`

Step 3 Import the data exported from the single-tenant overlay, on a multitenant SD-WAN Manager instance.

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

Method	`POST`
URL	`https://MT-vManage-IP-address`
Endpoint	`/dataservice/tenantmigration/import`
Authorization	Provider admin user credentials.

Body	**Required** Format: form-data Key Type: File Value: `default.tar.gz`

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

Step 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.

Step 5 On the single-tenant SD-WAN Manager 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** Format: Raw text Content: Migration token obtained in Step 4.

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

As part of the migration task, the address of the multitenant Cisco SD-WAN Validator, 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.

What to do next

In SD-WAN Manager, check the status of the migration task.

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 SD-WAN Validator IP address and the Organization name to match the configuration of the multitenant deployment.

In the single-tenant deployment, if Cisco SD-WAN Manager-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 SD-WAN Manager. If enterprise certificates are installed on the cloud-based WAN edge devices, the certificates are not affected by the migration.

Migrate a tenant from a multitenant Cisco Catalyst SD-WAN overlay to single-Tenant Cisco Catalyst SD-WAN deployment

Prerequisites to migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment

Ensure these prerequisites are met for a successful migration.

- Manually migrate the serial number of the WAN edge device associated to a virtual account on the source Cisco SD-WAN Manager overlay in Cisco PNP to the destination virtual account.
- Ensure that you manually create the controller profile on the destination virtual account for on-prem to on-prem or cloud to on-prem deployments.
- Ensure that the source and destination Cisco SD-WAN Manager instances use the same Certificate Authority (CA) and software release; a mismatch can block tenant data import and cause migration failure.
- Ensure that you check the CPU, memory, and disk size requirements of the destination overlay Cisco SD-WAN Controller before the migration to meet the WAN edge forecast requirements.
- Ensure that there is no overlap between the configured system IP addresses of edge devices and the destination overlay controllers.
- Ensure that all devices in a tenant have connectivity to the Cisco SD-WAN Validator in the destination single-tenant overlay. The migration procedure supports a Cisco SD-WAN Validator on the single-tenant deployment configured either with IP or DNS.

  Push any required static route configuration to the devices before initiating any of the migration steps.
- Ensure that there are valid control connections from Cisco SD-WAN Manager to the WAN edge devices in the source overlay.

Configuration

- Ensure that the destination single-tenant Cisco SD-WAN Manager does not have any configurations before migration. You can configure only mandatory admin settings and all other configurations can be done after data import.
- Configure a maintenance window for the multitenant overlay before performing this procedure. Refer to the information about configuring a maintenance window in the basic settings section of the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.
- Ensure that the WAN edge devices that are configured using CLI, device template, or configuration groups, have an IP host mapping to the Cisco SD-WAN Validator in the destination single-tenant overlay.
- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.

Migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment

Use these steps to migrate a tenant from a multitenant SD-WAN overlay to single-tenant SD-WAN deployment.

Procedure

Step 1 Export the multitenant deployment configuration and statistical data from a Cisco SD-WAN Manager instance controlling the source overlay.

Method	`POST`
URL	`https://MT-vManage-IP-address`
Endpoint	`/dataservice/tenantmigration/export`
Authorization	Administrator user credentials.

Body	Required Format: Raw JSON Example: `{ "name": "tenant1", "desc": "This is tenant1", "orgName": "vIPtela Inc MT to ST Migration Regression-Tenant1 Inc", "subDomain": "tenant1.mtreg.com", "wanEdgeForecast": 100, "migrationKey="tenant1TenantMigrationKey123", "isDestinationOverlayMT": false }` Field descriptions: **Note** Ensure that the `name`, `desc`, `orgName`, `subdomain`, and `wanEdgeForecast` match the tenant you wish to migrate. • `name`: Unique name for the tenant in the multitenant deployment. The name should be between 8-32 characters and can contain only alphanumeric characters. • `desc`: Description of the tenant. The description can be up to 256 characters and can contain only alphanumeric characters. • `orgName`: Name of the tenant organization. The organization name is case-sensitive. • `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`. • `wanEdgeForecast`: Number of WAN edge devices that the tenant can deploy. • `migrationKey`: Migration key which is used to encrypt sensitive data during migration. The migration key should be between 8-32 characters and can contain only alphanumeric characters. • `isDestinationOverlayMT`: Boolean variable which speficies if the migration is happening to a mutitenant overlay or not.
Response	Format: JSON `{ "processId": <vManage_process_ID>, }`

Step 2 Check the status of the data export task in SD-WAN Manager When the task is successfully complete, download the data from the following URL: `https://MT-vManage-IP-address/dataservice/tenantmigration/download/default.tar.gz`

Step 3 Import the data to the single-tenant instance, as follows:

a) Execute the following API:

Method	`POST`
URL	`https://ST-vManage-IP-address`

Endpoint	`/dataservice/tenantmigration/import/{migrationKey}` Use the same migration key specified earlier.
Authorization	Provider administrator user credentials.
Body	Required Format: form-data Key Type: File Value: `default.tar.gz`

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

b) When the task is complete, on the single-tenant SD-WAN Manager you can view the devices, templates, and policies imported from the multitenant overlay.

Step 4 After the import, update information related to the device templates, policies, and other deployment-specific parameters.

a) Check and update the administrator settings as some of the administrator settings specific to the source overlay are not exported. The import does not override the administrator settings that are already configured in destination SD-WAN Manager.

Step 5 If a centralized policy is present on the source tenant, the migration copies the policy to the destination overlay.

We recommend creating Cisco SD-WAN Controller templates and attaching them to the devices. Apply the centralized policy to devices in the destination overlay before proceeding.

Step 6 Obtain the migration token using the token URL from the previous step.

Method	`GET`
URL	`https://ST-vManage-IP-address`
Endpoint	`migrationTokenURL` obtained in the previous step.
Authorization	Provider administrator user credentials.
Response	The migration token as a large encoded text.

Step 7 On the multitenant SD-WAN Manager instance, initiate the migration of the overlay to the single-tenant deployment.

Method	`POST`
URL	`https://MT-vManage-IP-address`
Endpoint	`dataservice/tenantmigration/networkMigration`
Authorization	Administrator user credentials.
Body	Required Format: Raw text Content: Migration token obtained in the previous step.

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

When the task succeeds, WAN edge devices form control connections to controllers in the single-tenant deployment; the WAN edge devices are no longer connected to the controllers of the multitenant overlay.

What to do next

In SD-WAN Manager, check the status of the migration task.

After the migration is successfully complete, perform the following tasks:

- If WAN edge devices have SD-WAN Manager signed certificates in the source setup, the certificates are cleared from the device during migration and control connections are lost. Recertify the devices in the destination.
- The passwords are updated to the default password in the destination overlay for users created on a tenant in the source overlay. Make any configuration changes specific to the destination overlay.
- Delete the tenant on the source overlay after migration and verification is complete.

Migrate multitenant Cisco Catalyst SD-WAN overlay

Restrictions for migrating multitenant Cisco Catalyst SD-WAN overlay

Defines restrictions for migrating a multitenant Cisco Catalyst SD-WAN overlay.

- This migration procedure applies only to SD-WAN Controllers deployed on premises.
- The multitenant overlay can only be migrated to a setup in which Cisco SD-WAN Manager instances run Cisco vManage Release 20.6.1 software and 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.

Migrate multitenant Cisco Catalyst SD-WAN overlay

Before you begin

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

Device	Software version
Cisco SD-WAN Manager	Cisco vManage Release 20.3.3
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.3.3
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.3.3
Cisco IOS XE Catalyst SD-WAN device	Cisco IOS XE Release 17.3.3

Procedure

Step 1 Upgrade the software on the three SD-WAN Manager instances in the cluster to Cisco vManage Release 20.6.1.

Refer to the cluster management section of the *Cisco Catalyst SD-WAN Getting Started Guide*.

Run the **`request nms configuration-db upgrade`** command on only one of the SD-WAN Manager instances.

Step 2 After the SD-WAN Manager software is upgraded to Cisco vManage Release 20.6.1, log in to the SD-WAN Manager.

You're prompted to set a new password. Enter a new password that adheres to the password guidelines.

Step 3 Upload the Cisco SD-WAN Release 20.6.1 software to SD-WAN Manager.

Refer to the information about adding an image to the software repository in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 4 Upgrade the Cisco SD-WAN Validator software to Cisco SD-WAN Release 20.6.1.

Refer to the information about upgrading the software image of a device in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Step 5 Create two SD-WAN Controllers instances running Cisco SD-WAN Release 20.6.1 software.

Refer to the information about deploying an SD-WAN Controller in the *Cisco Catalyst SD-WAN Getting Started Guide*.

With two SD-WAN Controller instances, you can support up to 24 tenants. To support up to 50 tenants, create six SD-WAN Controller instances.

Step 6 Add Cisco SD-WAN Controllers to the overlay network.

The Provider Dashboard shows the new SD-WAN Controller running Cisco SD-WAN Release 20.6.1 software.

The Tenant Dashboard shows the older SD-WAN Controller running Cisco SD-WAN Release 20.3.3 software.

Step 7 Enable the maintenance window on SD-WAN Manager. For more information, see Configure or Cancel SD-WAN Manager Server Maintenance Window.

Refer to the information about configuring a maintenance window in the basic settings section of the *Cisco Catalyst SD-WAN Control Components and Device Management Guide*.

A maintenance window of 3 to 4 hours is recommended.

Step 8 Migrate the tenant configuration from the older tenant-specific SD-WAN Controller running Cisco SD-WAN Release 20.3.3 software to the new shared SD-WAN Controller 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 Format: Raw JSON `{}`
Response	Format: JSON `{ "processId": <vManage_process_ID>, }`

Step 9 Upgrade the Cisco IOS XE Catalyst SD-WAN device software to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

Refer to the information about upgrading the software image on a device, and about activating a new software image, in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

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.

During the migration task, the following changes are affected:

1. The older SD-WAN Controllers are invalidated and deleted from the overlay network.
2. In the tenant view, the older SD-WAN Controllers are removed from the Tenant Dashboard, and the Devices and the Certificates page.
3. The tenant WAN edge devices are connected to the new SD-WAN Controller.

What to do next

In SD-WAN Manager check the status of the migration task using the `processId` from the API response.

Verify the migration

Use these steps to verify multitenant migration.

Procedure

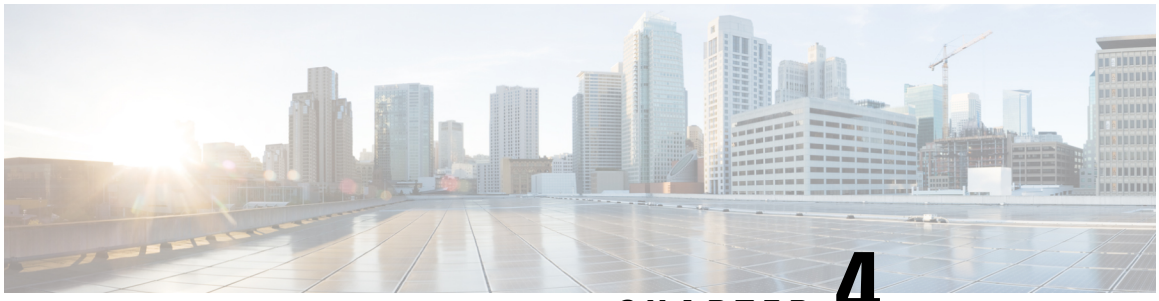
Step 1 In the provider view, perform these checks:

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

b) View tenants associated with a Cisco SD-WAN Controller, on page 38.

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

Step 2 In the provider-as-tenant view, verify whether the multitenant SD-WAN Controllers appear on the **Tenant Dashboard**.



CHAPTER 4

Multitenancy: Disaster Recovery

Disaster recovery for a multitenant Cisco SD-WAN Manager cluster

Summary

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

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Managercluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active CSD-WAN Manager cluster from the overlay network.

4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.

What's next

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

Prerequisites for a multitenant disaster recovery

Follow these prerequisites for a successful migration.

- The number of SD-WAN Manager nodes in the active and standby clusters must match.
- Each SD-WAN Manager node in the active and standby clusters must run the same SD-WAN Manager software release.
- Each SD-WAN Manager node in the active and standby clusters must connect to the WAN transport IP address of the SD-WAN Validator in the overlay network.
- Initially, disable the tunnel interfaces of the SD-WAN Manager nodes in the standby cluster.
- Certify the SD-WAN Manager nodes in the standby cluster.
- Synchronize the clock of every SD-WAN Manager node in the standby cluster with the clocks of the SD-WAN Controller and WAN edge devices in the overlay network. If NTP is configured on the overlay, configure the same on the standby SD-WAN Manager nodes.
- Use identical Neo4j credentials on the SD-WAN Manager nodes in the active and standby clusters.

Restrictions for a multitenant disaster recover

Defines restrictions to backup and restore process during disaster recovery of a SD-WAN Manager cluster.

- Do not interrupt any active processes while backing up the configuration database.
- Enable SD-AVC before restoring the configuration database on the standby SD-WAN Manager node.

Configure a standby SD-WAN Manager cluster

To prepare standby SD-WAN Manager nodes with a unique yet synchronized configuration for disaster recovery without impacting the active overlay network.

Procedure

Step 1 Configure the standby SD-WAN Manager nodes with a running configuration similar to the active SD-WAN Manager nodes and install local certificates.

The running configuration on a standby node is usually identical to an active node, but ensure settings such as system IP address and tunnel interface IP address are unique.

Step 2 On the standby nodes, shut down the transport interface in VPN 0 using the CLI shutdown command in the transport interface configuration.

Step 3 Create a standby cluster using the configured standby SD-WAN Manager nodes.

Step 4 With this configuration, the overlay network remains unaware of the standby SD-WAN Manager cluster.

Back up the active SD-WAN Manager cluster configuration

Back up the full configuration database of the active Cisco vManange cluster periodically. Additionally, take snapshots of the active SD-WAN Manager virtual machines.

Procedure

Step 1 Choose an active SD-WAN Manager node that hosts the configuration database service.

Step 2 On the CLI of the selected node, run the following command to back up the configuration database: **request nms configuration-db backup path <file-path>**

The command saves the configuration database as a `.tar.gz` file in the specified file path.

Example:

In the example below, 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
```

Step 3 Choose a standby SD-WAN Manager node that hosts the configuration database service and copy the configuration database backup to this node.

Example:

In the following example, db_backup.tar.gz is copied from the active SD-WAN Managernode to the /home/admin/ directory of a standby SD-WAN Manager 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 SD-WAN Manager cluster using the configuration database backup

Restore the most recent backup of the configuration database from the active SD-WAN Manager cluster on the standby SD-WAN Manager node to which the backup was copied.

- The restore operation does not restore all configuration details. Settings such as users and repositories must be configured on the standby SD-WAN Manager node after restoring the backup.
- When you complete the steps that follow, the previously active SD-WAN Manager nodes cannot be reused. To reuse the nodes, you must perform additional steps that are beyond the scope of this document.

Procedure

Step 1 On the CLI of the standby SD-WAN Manager node, run the following command: r**equest nms configuration-db restore path** *file-path*.

Example:

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
```

Step 2 Verify standby SD-WAN Manager nodes.

a) Verify that all appropriate services are running on each standby SD-WAN Manager node.

On the CLI of each standby node, run: **request nms all status**

From the command output, confirm that the necessary services are active.

b) Verify that every standby node maintains a list of all active and standby SD-WAN Manager nodes:

1. From the SD-WAN Manager, navigate to **Configuration** > **Devices** > **Controllers**.
2. Confirm that the page displays all active and standby SD-WAN Manager nodes.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed **Control Components** to align with Cisco Catalyst SD-WAN rebranding.

Step 3 On the standby SD-WAN Manager nodes, enable the transport interface on VPN 0 using one of these two methods:

a) Enable the transport interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **no shutdown** command.

Example:

```
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 SD-WAN Manager node, run the **tunnel-interface** command.

Example:

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

Step 4 Add each standby SD-WAN Manager node to the overlay network.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > > **Devices**.
b) Click **Controllers**.
c) For a SD-WAN Validator, click **...** and click **Edit**.
d) In the **Edit** dialog box, enter the following details of the SD-WAN Validator: WAN transport IP address, username, and password.

e) Repeat **Step 4c** and **Step 4d** for every SD-WAN Validator.

Step 5 Disconnect the active SD-WAN Manager nodes from the overlay network using one of these methods.

a) Shut down the transport interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **shutdown** command.

Example:

```
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 SD-WAN Manager node, run the **no tunnel-interface** command.ste

Example:

```
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
```

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

Step 6 From the standby SD-WAN Manager send the updated controller and device list to the SD-WAN Validator, including the list of controllers:

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) Click **Send to Validator**.

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

- The standby SD-WAN Manager nodes become the active Cisco SD-WAN Manager nodes.
- The previously active SD-WAN Manager nodes are no longer part of the overlay network.
- The active SD-WAN Manager 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**.

Step 7 Verify configuration and connectivity

a) Verify that policies, templates, and the controller and WAN edge device lists are intact.
b) Verify valid SD-WAN Manager nodes:

1. On each SD-WAN Validator, log in to the CLI and run: **show orchestrator** *valid-vmanage-id*.
2. Confirm that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed.
3. On a WAN edge device, log in to the CLI and run: **show control** *valid-vmanage-id*.
4. Confirm that the chassis numbers of the active and previously active SD-WAN Manager nodes are listed.

5. Check that the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Step 8 Invalidate the previously active SD-WAN Manager nodes.

After you invalidate the SD-WAN Manager, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) For each previously active SD-WAN Manager node, click **...** and click **Invalidate**.

Verify the valid SD-WAN Manager nodes

Procedure

Step 1 Log in to the CLI of each SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

In the command output, verify that the chassis numbers of only the active SD-WAN Manager nodes are listed.

Step 2 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 SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Disaster recovery in an overlay network with virtual routers

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

Summary

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

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Manager cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active SD-WAN Manager cluster from the overlay network.
4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.
5. To test disaster recovery, you can simulate a scenario in which the active SD-WAN Manager cluster fails. One way to simulate such a failure would be by disabling the tunnel interface as described in this document.

What's next

See these sections, before you proceed.

- Restrictions for a multitenant disaster recover
- Prerequisites for a multitenant disaster recovery
- Configure a standby SD-WAN Manager cluster
- Back up the active SD-WAN Manager cluster configuration

Restore SD-WAN Manager cluster using the configuration database backup

Restore the most recent backup of the configuration database from the active SD-WAN Manager cluster on the standby SD-WAN Manager node to which you copied this backup.

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

Procedure

Step 1 On the CLI of the standby SD-WAN Manager node, run the following command: **request nms configuration-db restore path** *file-path*

Example:

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
```

Step 2 Verify services and node list on the standby SD-WAN Manager nodes

a) Verify that the appropriate services are running on the standby SD-WAN Manager nodes: On the CLI of each standby SD-WAN Manager node, run the **request nms all status** command.

From the command output, verify the services running on the node.

b) Verify that every standby SD-WAN Manager node has a list of all the active and standby SD-WAN Manager nodes.

1. From the SD-WAN Manager menu, choose **Configuration** > **Devices** > **Controllers**.
2. Verify that the page displays all active and standby SD-WAN Manager nodes.

Step 3 Run the these commands:

a) Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.

b) 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 SD-WAN Manager nodes are listed.

Step 4 Enable the transport interface on VPN 0 on the standby SD-WAN Manager nodes using either of the following methods:

a) Enable the transport interface in VPN 0: On the CLI of each standby SD-WAN Manager node, run the **no shutdown** command.

Example:

```
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 SD-WAN Manager node, run the **tunnel-interface** command.

Example:

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

Step 5 Add each standby SD-WAN Manager node to the overlay network.

a) From the SD-WAN Manager menu, choose **Configuration** > > **Devices**.

b) Click **Controllers**.

c) For a Cisco SD-WAN Validator, click **...** and click **Edit**.

a) In the **Edit** dialog box, enter the following details of the Cisco SD-WAN Validator: WAN transport IP address, username, and password.

b) Repeat **Step 5c** and **Step 5d** for every Cisco SD-WAN Validator.

Step 6 Disconnect the active SD-WAN Manager nodes from the overlay network using one of the following two methods.

a) Shut down the transport interface in VPN 0: On the CLI of each active SD-WAN Manager node, run the **shutdown** command.

Example:

```
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 SD-WAN Manager node, run the **no tunnel-interface** command.

Example:

```
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
```

Step 7 From the standby SD-WAN Manager, send the updated controller and device list to the Cisco SD-WAN Validator.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates** .
b) Click **Controllers**.
c) Click **Send to Validator**.

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

- The standby SD-WAN Manager nodes become the active SD-WAN Manager nodes.
- The previously active SD-WAN Manager nodes are no longer part of the overlay network.
- The active SD-WAN Manager 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**.

Step 8 Verify configuration and connectivity.

a) Verify that policies, templates, and the controller and WAN edge device lists are intact.
b) Verify valid SD-WAN Manager nodes:

1. Log in to the CLI of each Cisco SD-WAN Validator and run the **show orchestrator valid-vmanage-id** command.
2. Log in to the CLI of a Cisco vEdge Cloud router and run the **show control valid-vmanage-id** command.
3. In the command output, verify that the chassis numbers of the active and previously active SD-WAN Manager nodes are listed.
4. Check whether the device is connected to the active SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

Step 9 Invalidate the previously active SD-WAN Manager nodes.

a) From the SD-WAN Manager menu, choose **Configuration** > **Certificates**.
b) Click **Controllers**.
c) For each previously active SD-WAN Manager node, click **...** and click **Invalidate**.

a. The previously active SD-WAN Manager is the certificate issuer for the cloud WAN edge devices. The active SD-WAN Manager issues certificates to the cloud WAN edge devices only after the previously active SD-WAN Manager nodes are invalidated.

b. After you invalidate the SD-WAN Manager nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.

c. When you invalidate the previously active SD-WAN Manager nodes, SD-WAN Manager marks the nodes as invalid and sends an update to all controllers. However, SD-WAN Manager does not send an updated list of valid SD-WAN Manager UUIDs to Cisco SD-WAN Validator immediately because the previously active SD-WAN Manager is the CA for the cloud WAN edge devices. So, the output of the **show orchestrator valid-vmanage-id** command on a Cisco SD-WAN Validator includes the UUIDs of the invalidated SD-WAN Manager nodes.

d. SD-WAN Manager 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 SD-WAN Manager. SD-WAN Manager sends the updated list of valid SD-WAN Manager UUIDs to Cisco SD-WAN Validator only after the cloud WAN edge devices have been moved to the active SD-WAN Manager. After this list is received, the output of the **show orchestrator valid-vmanage-id** command on a Cisco SD-WAN Validator does not include the UUIDs of the invalidated SD-WAN Manager nodes.

What to do next

To verify SD-WAN Manager nodes, see Verify the valid SD-WAN Manager nodes.

Disaster recovery after a failed data center becomes operational

This procedure applies to a scenario in which an initially active SD-WAN Manager cluster or the data center hosting the cluster failed and the standby SD-WAN Manager cluster was configured to be the active SD-WAN Manager 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.

Summary

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

Workflow

1. Deploy and configure a standby SD-WAN Manager cluster.

   The standby SD-WAN Manager cluster is not part of the overlay network and is not active.

2. Back up the configuration database of the active SD-WAN Manager cluster periodically.

   Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and back up the configuration database.

3. If the active SD-WAN Manager cluster fails, restore the most recent configuration database on the standby SD-WAN Manager cluster, activate the standby SD-WAN Manager cluster, and remove the previously active SD-WAN Manager cluster from the overlay network.

4. Choose a SD-WAN Manager node in the cluster that hosts the configuration database service and restore the configuration database backed up from the previously active SD-WAN Manager cluster.

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

What's next

- Back Up the Active Cisco SD-WAN Manager Cluster Configuration
- Restore Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

Replace faulty SD-WAN Controller

To replace a faulty SD-WAN Controller with a new instance, follow these steps:

Procedure

Step 1 Create a SD-WAN Controller instance.

Step 2 Add the SD-WAN Controller to the overlay network.

Step 3 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.

Step 4 Click **Controllers**.

Step 5 For the faulty SD-WAN Controller, click **...** and click **Invalidate**.

The **Invalidate** dialog box appears.

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

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

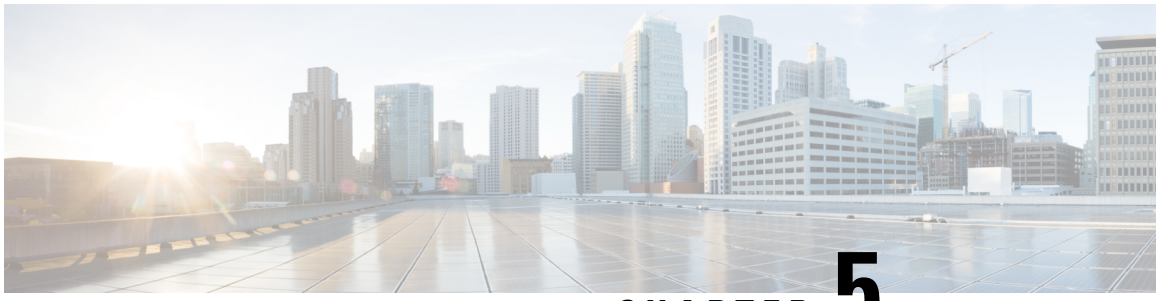
a) Check the **Replace Controller** check box.

b) From the **Select Controller** drop-down list, choose the new SD-WAN Controller that should replace the faulty instance.

c) Click **Invalidate**.

SD-WAN Manager launches the Invalidate Device and Push CLI Tempalte Configuration task. When these tasks are completed, the faulty SD-WAN Controller is invalidated and removed from the overlay network.

The tenants that were served by the faulty SD-WAN Controller are now served by the new SD-WAN Controller that you chose as the replacement.



CHAPTER 5

Multitenancy: Dashboard

Cisco SD-WAN Manager dashboard for multitenancy

Cisco SD-WAN Manager multitenant dashboard is a portal where the provider or tenant can view and provision the underlying system.

After enabling SD-WAN Manager for multitenancy, you can view the multitenant dashboard when you log in to SD-WAN Manager, under **Monitor** > **Overview**.

In Cisco vManage Release 20.6.1 and earlier, information related to the **Monitor** > **Devices** page can be viewed under the **Monitor** > **Network** page.

The bar at the top of every SD-WAN Manager multitenant screen includes icons that allow smooth navigation.

View Cisco SD-WAN Validator health dashlet

You can view the state of each Cisco SD-WAN Validator in the **Validator Health** dashlet on the **Monitor Overview** dashboard. This dashlet displays the cumulative state of the Cisco Catalyst SD-WAN Validators within a selected time window, along with the number of Validators in each state.

You can filter the dashlet view based on health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices**, as well as for **CPU Load**.

You can use the **View Details** option to access a detailed table view of device health on the **Monitor** > **Devices** page.

View Cisco SD-WAN Manager health dashlet

You can view the state of the SD-WAN Manager in the **Manager Health** dashlet on the **Monitor Overview** dashboard. This dashlet displays the health status of the SD-WAN Manager.

You can filter the dashlet view based on health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices**, as well as for **CPU Load**.

You can use the **View Details** option to access a detailed table view of device health on the **Monitor** > **Devices** page.

View Cisco SD-WAN Controller health dashlet

You can view the list of tenants hosted on a particular device by clicking the **Controller bar**.

You can view the state of each SD-WAN Controller in the **Controller Health** dashlet on the **Monitor Overview** dashboard. This dashlet displays the cumulative state of the SD-WAN Controller within a selected time window, along with the number of controllers in each state.

You can filter the dashlet view based on health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices**, as well as for **CPU Load**.

You can use the **View Details** option to access a detailed table view of device health on the **Monitor** > **Devices** page.

View multitenant WAN edge health dashlet

You can view the state of each WAN edge device in the **Multi Tenant WAN Edge Health** dashlet on the **Monitor Overview** dashboard. This dashlet displays the cumulative state of the devices within a selected time window, along with the number of WAN edge devices in each state.

You can view the list of tenants hosted on a particular device by clicking the multi-tenant WAN edge device bar. You can filter the dashlet view based on health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices**, as well as for **CPU Load**.

You can use the **View Details** option to access a detailed table view of device health on the **Monitor** > **Devices** page.

View tenant activity, device, and network information

To provide administrators with an overview and detailed insights into tenant, device, and network status in a multitenant Cisco SD-WAN environment.

When you log in to a multitenant SD-WAN Manager as an administrator, the Provider Dashboard displays the following components.

- Device pane: Runs across the top of the multitenant dashboard screen. It displays the number of active SD-WAN Controllers, SD-WAN Validators, and SD-WAN Manager instances, along with the connectivity status of devices and information on certificates that have expired or are about to expire.
- Tenants pane: Displays the total number of tenants and a summary of the control status, site health, router health, and SD-WAN Controller status for all tenants.
- Table of tenants in the overlay network: Lists individual tenants with separate information on control status, site health, WAN edge device health, and SD-WAN Controller status for each tenant.

Use these steps to display tenant specific status summary information:

To return to the provider dashboard from other SD-WAN Manager screens, click **Dashboard**.

Procedure

Step 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.

Step 2 Click **Tenant name** > **Dashboard**, to access the tenant dashboard.

SD-WAN Manager switches to the provider-as-tenant view and displays the tenant dashboard.

Step 3 Click **Provider** at the top of the page, to return to the provider view.

Step 4 Click the tenant name from the tenant list, to close the dialog box.

Step 5 To return to the provider dashboard from other SD-WAN Manager screens, click **Dashboard**.

View detailed information of a tenant setup

Cisco SD-WAN Manager displays the tenant dashboard, which provides information about a tenant deployment in the following scenarios:

- When a **provider admin** user selects a specific tenant from the **Select Tenant** drop-down list in the provider dashboard. This view is referred to as the provider-as-tenant view.
- When a **tenantadmin** user logs in to SD-WAN Manager. This view is referred to as 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 SD-WAN Manager to the SD-WAN Controllers and routers in a tenant's overlay network.

For each WAN edge device, the device pane shows:

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

You can use a connection number or the Up/Down arrow to view a table with detailed information about each connection, and use the **More Actions** icon at the right of each table row to access additional options.

You can also use 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 the **Tools** > **SSH Terminal** screen.

View information about device reboots

The **Reboot pane** displays the total number of device reboots in the last 24 hours for all devices in the network. It includes soft and cold reboots, as well as reboots caused by power-cycling a device.

For each reboot, the following information is listed:

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

If the same device reboots multiple times, each reboot is reported separately.

You can use the **Reboot pane** opens the **Reboot** dialog box. In the dialog box, the **Crashes** tab lists information for all device crashes, including:

- 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 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 SD-WAN Manager to the SD-WAN Controllers and routers in a tenant's overlay network.

For each WAN edge device, the device pane shows:

- Total number of control connections between SD-WAN Controllers and WAN edge devices

- Number of valid control connections between SD-WAN Controllers and WAN edge devices
- Number of invalid control connections between SD-WAN Controllers and WAN edge devices

You can use a connection number or the Up/Down arrow to view a table with detailed information about each connection, and use the **More Actions** icon at the right of each table row to access additional options.

You can also use 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 the **Tools** > **SSH Terminal** screen.

View state of data connections for a site

The **Site Health** pane displays the state of data connections for a site. For sites with multiple WAN edge devices, the pane shows the state for the entire site rather than individual devices.

he Site Health pane includes 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 some tunnels or BFD sessions on routers are down, but limited data plane connectivity remains.
- No WAN Connectivity: Total number of sites where all BFD sessions on all routers are down, resulting in no data plane connectivity.

You can view a table with detailed information about each site, node, or tunnel in the **Site Health** dialog box.

The **More Actions** icon at the right of each table row provides access to the **Device Dashboard**, or **Real Time view** from the **Monitor** > **Devices** screen, or the **Tools** > **SSH Terminal** screen.

View interface usage for WAN edge interfaces

The **Transport Interface Distribution** pane displays interface usage for the last 24 hours for all WAN edge interfaces in VPN 0, including all TLOC interfaces.

You can view detailed interface usage information 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 uploaded on SD-WAN Manager. The serial number is uploaded on the **Configuration** > **Devices** screen.
- Authorized: Total number of authorized WAN edge devices in the overlay network. These devices are marked as 'Valid' in the **Configuration** > **Certificates** > **WAN Edge List** screen.
- Deployed: Total number of deployed WAN edge devices. These devices are marked as 'Valid' and are operational in the network.

- Staging: Total number of WAN edge devices configured at a staging site before they become part of the overlay network. These devices do not participate in routing decisions and do not affect network monitoring through SD-WAN Manager.

You can view hostname, system IP, site ID, and other details of each router in the **WAN Edge Inventory** dialog box.

View aggregated state of WAN edge devices

The **WAN Edge Health** pane provides an aggregated view of the state of WAN edge devices by showing the number of devices in each state, reflecting the overall health of the hardware nodes.

The three WAN edge device states are:

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

You can view a table displaying the last 12 or 24 hours of memory usage, CPU utilization, and hardware-related alarms (such as temperature, power supply, and PIM modules) by selecting a number or device state in the pane.

Use 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.

  Tools > **SSH Terminal** screen.

View WAN edge device loss, latency, and jitter

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

You can use the **Type** drop-down arrow to select **loss**, **latency**, or **jitter**, and adjust the time period to display the relevant transport health data.

The **Transport Health** dialog box provides a more detailed view, with the **Details** tab displaying the information in a tabular format. You can also change the displayed health type and time period from this dialog box.

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.

SAIE flow information is available for the last 24 hours. To view data beyond this period, you must check the information for the specific device.

You can select a time period and a VPN from the respective drop-down lists to display SAIE flow information for all flows in that VPN. The **Top Applications** dialog box provides a more detailed view of the same information, allowing changes to the VPN and time period.

Note In Cisco vManage Release 20.7.x and earlier, SAIE flow information is referred to as deep packet inspection (DPI).

View tunnels data

The **Application-Aware Routing** pane allows selection of tunnel criteria from the **Type** drop-down arrow:

- Loss
- Latency
- Jitter

Based on the selected criteria, the pane displays the 10 worst tunnels. For example, selecting **Loss** shows the 10 tunnels with the highest average loss over the last 24 hours.

A graphical representation of the data can be viewed for each tunnel, with the option to select a time period or specify a custom time period.

The **Application-Aware Routing** dialog box provides a more detailed view, displaying the 25 worst tunnels based on the chosen criteria: **Loss**, **Latency**, or **Jitter**.

View tenant alarms in provider dashboard

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 From the SD-WAN Manager menu, choose **Operated as Provider** > **Provider** > **Logs**.

Step 3 In the **Alarms** tab, toggle **View tenant alarms**.

Step 4 Optional: Filter alarms using **Advanced Filter** based on Tenant, Object Type, Object List, Severity, and Type.

Step 5 Optional: Click the bell icon on top to view all the notifications for tenant's alarms.

View tenant events in provider dashboard

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.
Step 2 From the Cisco SD-WAN Managermenu, choose **Operated as Provider** > **Provider** > **Logs**.
Step 3 In the **Events** tab, toggle **View tenant** events.
Step 4 Optional: Filter events using **Advanced Filter** based on Tenant, Object Type, Object List, Severity, and Type.

View OMP statistics per tenant on a Cisco SD-WAN Controller

To view OMP statistics for a specific tenant on a selected SD-WAN Controller.

Procedure

Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.
Step 2 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
Step 3 In the table of devices, click on the hostname of a SD-WAN Controller.
Step 4 In the left pane, click **Real Time**.
Step 5 In the **Device Options** field, enter `OMP` and select the OMP statistics you wish to view.
Step 6 In the **Select Filters** dialog box, click **Show Filters**.
Step 7 Enter the Tenant Name and click **Search**.

Cisco SD-WAN Manager displays the selected OMP statistics for the particular tenant.

View tenants associated with a SD-WAN Controller

Use these steps to view detailed connection information and the list of tenants associated with a SD-WAN Controller.

Procedure

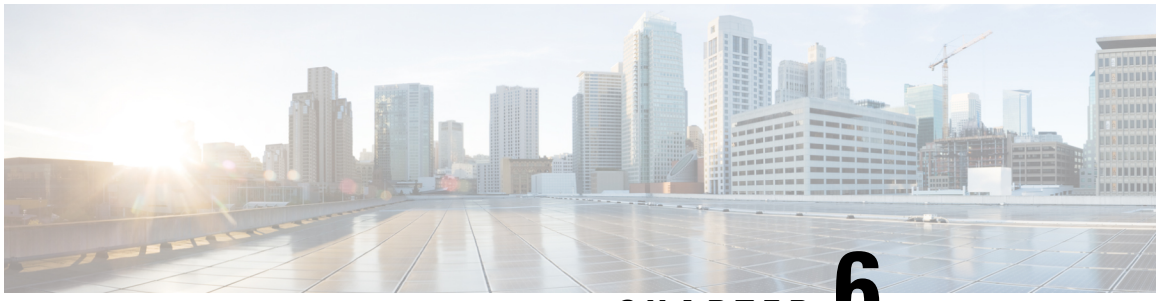
Step 1 Log in to Cisco SD-WAN Manager as the provider admin user.

Step 2 Click a **Controller** connection number to display a table with detailed information about each connection.

Cisco SD-WAN Manager displays a table that provides a summary of the SD-WAN Controller and their connections.

Step 3 For a SD-WAN Controller, click **...** and click **Tenant List**.

Cisco SD-WAN Manager displays a summary of tenants associated with the SD-WAN Controller.



CHAPTER 6

Multitenancy: Assigning Cisco SD-WAN Controllers to Tenants

Feature history for assigning Cisco SD-WAN Controllers to tenants

Table 15: Feature history

Feature name	Release information	Description
Flexible tenant placement on multitenant Cisco Catalyst SD-WAN Controllers	Cisco vManage Release 20.9.1	With this feature, while onboarding a tenant to a multitenant deployment, you can choose the pair of multitenant Cisco SD-WAN Controllers that serve the tenant. After onboarding a tenant, you can migrate the tenant to a different pair of multitenant Cisco SD-WAN Controller, if necessary.

Assigning SD-WAN Controllers to Tenants

Multitenancy

Multitenancy is a Cisco SD-WAN deployment model that

- allows multiple tenants to share the same Cisco SD-WAN infrastructure,
- assigns dedicated logical resources (such as controllers and organization names) to each tenant for isolation, and
- supports automatic or flexible placement of Cisco SD-WAN Controller during tenant onboarding.

Types of multitenancy assignments

There are two types of multitenancy assignments in Cisco SD-WAN:

- Automatic tenant placement: Cisco SD-WAN Manager automatically assigns controllers to tenants using an internal algorithm during onboarding.
- Manual tenant placement : You can manually select the pair of SD-WAN Controllers for a tenant based on utilization and resource availability.

Manual tenant placement

With manual tenant placement, you can select controller pairs during onboarding, view controller capacity (such as tenants, edge devices, CPU, and memory), and migrate tenants or add SD-WAN Controllers to optimize utilization.

Availability and configuration

From Cisco vManage Release 20.9.1, you can use manual tenant placement as an optional feature. By default, SD-WAN Manager performs automatic tenant placement, but you can enable manual placement to gain more control during onboarding.

SD-WAN Controller capacity limits

A multitenant SD-WAN Controller supports up to 24 tenants and 1000 tenant WAN edge devices across all tenants. During onboarding, the network administrator must select a pair of SD-WAN Controllers that can host one more tenant and connect to the tenant's forecasted number of WAN edge devices.

Optimization and migration

If a tenant adds more devices than forecast and the assigned SD-WAN Controllers cannot support them, the network administrator migrates the tenant to another SD-WAN Controller pair that has capacity. If no SD-WAN Controller pair has enough capacity, the network administrator migrates other tenants to different SD-WAN Controllers to free up resources and balance utilization. If this optimization still doesn't create enough capacity, the network administrator adds a new SD-WAN Controller pair and then migrates the tenant there.

Automatic tenant placement

With automatic tenant placement you can rely on the system to assign SD-WAN Controller pairs during onboarding, adjust forecasts if existing SD-WAN Controllers can handle more WAN Edge devices, or re-onboard/add controllers if capacity is exceeded.

Availability

Cisco supports automatic tenant placement in vManage in Release 20.8.x and earlier.

Algorithm criteria

The internal algorithm assigns SD-WAN Controllers by considering three factors:

- the number of tenant WAN edge devices forecasted for the tenant,
- the number of tenants already served by each SD-WAN Controller pair, and
- the number of WAN edge devices already connected to each SD-WAN Controller pair.

Benefits of automatic tenant placement on multitenant SD-WAN Controllers

This section highlights how strategic tenant placement enhances controller efficiency, performance, and overall network resilience.

Reliability & availability

Reduces the risk of simultaneous controller failures by allowing you to choose controllers deployed in different failure zones or regions in a cloud environment.

Performance & efficiency

- Minimizes latency by enabling you to select controllers located in the same geographical region as the tenant WAN edge devices.
- Improves performance and efficiency by letting you choose controllers based on available CPU, DRAM, hard disk resources, and their utilization.

Scalability

Provides scalability by allowing you to migrate tenants to different controllers when the tenant device forecast changes.

Restrictions for automatic tenant placement on multitenant SD-WAN Controllers

If you need to migrate a tenant to a different pair of SD-WAN Controllers, change the SD-WAN Controllers one at a time. This restriction ensures that one controller remains available to the tenant WAN edge devices and prevents traffic disruption. SD-WAN Controllers CLI templates must not contain tenant configuration. This configuration is added dynamically and managed internally by the device. If tenant configuration is present in any SD-WAN Controller CLI template, it must be removed to prevent issues during tenant migration or placement operations.

Prerequisites for automatic tenant placement on multitenant SD-WAN Controllers

Before adding new tenants, ensure that SD-WAN Controller, capacity limits, and account configurations meet the foundational requirements.

SD-WAN Controller requirements

- Ensure at least two Cisco SD-WAN Controllers are operational and visible in SD-WAN Manager before adding new tenants.
- Push a template from SD-WAN Managerto a controller to place it in Manager mode; a controller in CLI mode cannot serve multiple tenants.
- Verify that each SD-WAN Controller pair can support a maximum of 24 tenants and 1000 tenant devices. Ensure at least two controllers have capacity for a new tenant. If no pair can support a new tenant, add two controllers and switch them to Manager mode.

Tenant provisioning rules

- Add up to 16 tenants in a single operation. SD-WAN Manager provisions tenants sequentially, not in parallel.
- Do not start a second **Add Tenant** task while one is already in progress; otherwise, the second task fails.

Accounts and profiles

Each tenant requires a unique Virtual Account (VA) on Plug and Play Connect in Cisco Software Central. The tenant VA must belong to the same Smart Account (SA) as the provider VA. Depending on the deployment type, one of the following must be completed:

- On-premises deployments: Create a SD-WAN Validator controller profile for the tenant on Plug and Play Connect with these mandatory fields:

Table 16: Mandatory fields for on-premises validator controller profile

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

- For cloud deployments: SD-WAN Manager automatically creates the Validator Controller profile during tenant creation.

Assign SD-WAN Controllers to Tenants During Onboarding

Before you begin

Each tenant requires a unique Virtual Account (VA) on Plug and Play Connect in Cisco Software Central. The tenant VA must belong to the same Smart Account (SA) as the provider VA. Depending on the deployment type, one of these must be completed:

- On-premises deployments: Create a Cisco SD-WAN Validator controller profile for the tenant on Plug and Play Connect with these mandatory fields:

Table 17: Mandatory fields for on-premises validator controller profile

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

- For cloud deployments: SD-WAN Manager automatically creates the Validator Controller profile during tenant creation.

To provision and activate the tenant in SD-WAN Manager with the configured settings, follow these steps.

Procedure

Step 1 Log in to SD-WAN Manager as the provider admin user.

Step 2 From the menu, choose **Administration** > **Tenant Management**.

Step 3 Click **Add Tenant**.

Step 4 In the **Add Tenant** slide-in pane, click **New Tenant**.

Step 5 Configure tenant details:

Table 18: Tenant Configuration Fields

Field	Details
Name	Enter a name for the tenant. For cloud deployments, the tenant name must match the tenant VA name in Plug and Play Connect.
Description	Enter a description (up to 256 alphanumeric characters).
Organization name	Enter the tenant's organization name (case-sensitive, up to 64 characters). Use the format <SP Org Name>-<Tenant Org Name> Example: managed-sp-customer1
URL subdomain	Enter the tenant's fully qualified subdomain name. It must include the provider's domain name. Example: customer1.managed-sp.com. See DNS configuration table for deployment-specific steps.
Forecasted devices	Enter the maximum number of WAN edge devices the tenant can add. If this limit is exceeded, SD-WAN Manager blocks device addition.
Select two controllers	• Automatic placement (default): Ensure the field is set to Autoplacement. • Manual placement: **a.** Click the **Select two Controllers** drop-down list. SD-WAN Manager lists the hostnames of the available SD-WAN Controllers. For each SD-WAN Controller, SD-WAN Manager shows whether the controller is reachable and reports the utilization details. See utilizations details table for more information. **b.** Select two SD-WAN Controllers to assign to the tenant based on the utilization details.

Table 19: Utilization details

Field	Description
Tenant hosting capacity	Each SD-WAN Controller can serve a maximum of 24 tenants. Tenant hosting capacity represents the number of tenants to which the Cisco SD-WAN Controller is assigned in the form of a percentage. This value indicates whether you can assign another tenant to this controller.
Used device capacity	Each SD-WAN Controller can support a maximum of 1000 tenant WAN edge devices. Used device capacity represents the number of tenant WAN edge devices connected to the SD-WAN Controller in the form of a percentage of the maximum capacity (1000 WAN edge devices). This value indicates whether the SD-WAN Controller can support the number of devices forecast for the tenant that you are onboarding.
Memory utilized	This value represents memory consumption as a percentage.
CPU utilized	This value represents CPU usage as a percentage.

Table 20: DNS configuration

Deployment type	DNS configuration steps
On-premises	• Add the tenant subdomain to DNS and map it to the IPs of the three SD-WAN Manager instances in the cluster. • Create a provider DNS A record from the provider's domain name and cluster ID. Example: `vmanage123.sdwan.cisco.com`. Validate: `nslookup vmanage123.sdwan.cisco.com`. • Create tenant DNS CNAME records mapping the tenant FQDN to the provider FQDN. Example: `customer1.sdwan.cisco.com`. Validate: `nslookup customer1.sdwan.cisco.com`. • If DNS is misconfigured, an authentication errors occurs.
Cloud	• The tenant subdomain is automatically added to DNS. • DNS resolution can take up to one hour after creation.

Step 6 Save the tenant configuration.

Step 7 To add another tenant, repeat steps 4 to 6.

When the task completes successfully, you can view the tenant information, including the assigned SD-WAN Controllers and Validators, on **Administration** > **Tenant Management**.

After completing the tenant addition steps, SD-WAN Manager performs the Create Tenant Bulk task, which:

- Creates the tenant.

- Assigns two SD-WAN Controllers and pushes CLI templates with the tenant information.
- Sends the tenant and controller details to SD-WAN Validator.

Update SD-WAN Controller placement for a tenant

You can migrate a tenant to a different pair of SD-WAN Controller if the currently assigned controllers cannot support the tenant's revised WAN edge device forecast.

During migration, change one controller at a time to ensure continuous availability and prevent traffic disruption.

Procedure

Step 1 Log in to SD-WAN Manager as the provider admin user.

Step 2 From the menu, choose **Administration** > **Tenant Management**.

Step 3 Locate the tenant to migrate and click **…** next to the tenant organization name.

Step 4 Click **Update Controller Placement.**

Step 5 In the **Update Controller Placement** slide-in pane, configure these:

a) Source Controller (currently applied)

1. Click the drop-down list to view the tenant's currently assigned controllers.
2. SD-WAN Managershows reachability and utilization details for each controller:
   - Tenant hosting capacity (max 24 tenants)
   - Used device capacity (max 1000 devices)
   - Memory utilization (%)
   - CPU utilization (%)
3. Select the check box next to one of the currently assigned controllers.

b) Destination controller

1. Click the drop-down list to view available controllers not currently assigned to the tenant.
2. SD-WAN Manager shows reachability and utilization details for each controller.
   - Tenant hosting capacity (max 24 tenants)
   - Used device capacity (max 1000 devices)
   - Memory utilization (%)
   - CPU utilization (%)
3. Select the checkbox next to the controller you want to assign.

Note
If the selected controller cannot support the tenant's devices, the update operation fails.

Step 6 Click **Update**.

Step 7 To change the second controller assigned to the tenant, repeat steps 5–6.

SD-WAN Manager starts the Tenant Controller Update task, migrating the tenant details from the previous controller to the new controller.

What to do next

After the task completes successfully, view the updated tenant information, including the assigned SD-WAN Controllers, on **Administration** > **Tenant Management**.