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, see Flexible Tenant Placement on Multitenant Cisco SD-WAN Controllers.

- 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 provider-as-tenant view. In the provider view, Cisco SD-WAN Manager does not show any WAN edge device information.

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	Cloud-delivered Catalys
Identity Services Engine (ISE) integration	Yes	No	No
Intent-based hub and spoke topology	Yes	No	No
Controller group affinity	Yes	No	No

Feature	Single Tenant	Multitenant	Cloud-delivered Catalys
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, see SSH Authentication using Cisco SD-WAN Manager on Cisco IOS XE Catalyst SD-WAN Devices.

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. For information on changing the default password, see Hardware and Software Installation.

- The **tenantadmin** user is part of the user group **tenantadmin**. Users in this group are permitted to perform all operations on the WAN edge devices of the tenants. You can add additional users to the **tenantadmin** group.
- You cannot modify the privileges of the **tenantadmin** group. On 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, see Configure User Access and Authentication.

- 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.

- Feature availability

  See Feature availability.

- 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
- Initial setup for Cisco Catalyst SD-WAN 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. See Deploy Cisco SD-WAN Validator.

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

Example:

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

Step 4 Create Cisco SD-WAN Controller instances. See Deploy the Cisco SD-WAN Controller.

- 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.

- 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 (say vManage1, vManage2, and vManage3) by installing the downloaded software image file. See Deploy Cisco SD-WAN Manager.

- Deploy SD-WAN Manager servers having the hardware specifications in the table Hardware Specifications to Support 50 Tenants and 1000 Devices of this document.
- Choose the Compute+Data persona for each SD-WAN Manager instance.

Step 3 Complete the following operations on vManage1:

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

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

e) Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

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 vManage2 and vManage 3:

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

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

d) Log in to the Cisco SD-WAN Manager Web Application Server.

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

f) Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

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 vManage1 GUI and add vManage2 to the cluster.

- vManage2 reboots before being added to the cluster.

- While vManage2 is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for vManage2 shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding vManage2 to the cluster.
- When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both vManage1 and vManage2, and their node personas.

Step 6 Repeat Step 5 and add vManage3 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. See Deploy Cisco SD-WAN Manager.

- 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, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy SD-WAN Manager servers having the hardware specifications in the table Hardware Specifications to Support 150 Tenants and 7500 Devices of this document.
- Choose the Compute+Data persona for three SD-WAN Manager instances (say vManage1, vManange2, and vManage 3). Choose the Data persona for the other three SD-WAN Manager instances (say vManage4, vManage5, and vManage6).

Step 3 Complete the following operations on vManage1:

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

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

e) Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

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 vManage2 and vManage 3:

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

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

d) Log in to the Cisco SD-WAN Manager Web Application Server.

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

f) Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

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 vManage1 GUI and add vManage2 to the cluster.

- vManage2 reboots before being added to the cluster.
- While vManage2 is being added to the cluster, on the **Administration** > **Cluster Management** page, the **Configure Status** for vManage2 shows **Pending**. You can monitor the System Generated Cluster Sync transaction to check the progress of the adding vManage2 to the cluster.
- When the operation is completed, on the **Administration** > **Cluster Management** page, you can view both vManage1 and vManage2, and their node personas.

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

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, see step 3.d in Add a New Tenant.

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**.

For more information on configuration using CLI template, see Device Configuration-Based CLI 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. See Deploy the Cisco SD-WAN Controller.
    - 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 (say vManage1, vManage2, and vManage3) by installing the downloaded software image file. See Deploy Cisco SD-WAN Manager.

- 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 Cisco SD-WAN Manager servers having the hardware specifications in the table 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 vManage1 through vManage3:

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 the following through the SD-WAN Manager:

1. Generate a Certificate Signing Request
2. After Symantec or your enterprise root CA has signed the certificate, install the signed certificate.
3. Log in to the Cisco SD-WAN Manager Web Application Server.
4. Ping the OOB interfaces on the other Cisco SD-WAN Manager instances and ensure they are reachable.
5. Configure the Cluster IP Address of the Cisco SD-WAN Manager Server.

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 the GUI of the existing 3-node SD-WAN Manager cluster and add vManage1 to the cluster.

a. vManage1 reboots before being added to the cluster.

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

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

Step 5 Repeat Step 4 and add vManage2 and vManage3 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, see Upgrade Cisco SD-WAN Manager Cluster.

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

Step 2 After the SD-WAN Managerr software is upgraded to Cisco vManage Release 20.6.1 or a later release, log in to the 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. For more information, see Add an Image to the Software Repository.

Step 4 Upgrade the Cisco SD-WAN Validator software to Cisco SD-WAN Release 20.6.1 or a later release. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.

Step 5 Enable maintenance window on SD-WAN Manager. For more information, see Configure or Cancel SD-WAN Manager Server Maintenance Window.

Step 6 Upgrade the SD-WAN Controller software to Cisco SD-WAN Release 20.6.1 or a later release. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.

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. For more information, see Upgrade the Software Image on a Device and Activate a New Software Image.