

Cisco Catalyst SD-WAN Multitenancy

- Cisco Catalyst SD-WAN Multitenancy, on page 2
- Information about Cisco Catalyst SD-WAN multitenancy, on page 4
- Supported Devices and Controller Specifications, on page 10
- Restrictions, on page 11
- Initial Setup for Multitenancy, on page 13
- Expand a Multitenant Deployment to Support More Tenants and Tenant Devices, on page 21
- Manage Tenants, on page 23
- Cisco SD-WAN Manager Dashboard for Multitenancy, on page 31
- Manage Tenant WAN Edge Devices, on page 37
- Tenant-Specific Policies on Cisco SD-WAN Controller, on page 38
- Manage Tenant Data, on page 38
- View OMP Statistics per Tenant on a Cisco SD-WAN Controller, on page 42
- View Tenants Associated with a Cisco SD-WAN Controller, on page 42
- Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment, on page 42
- Migrate a Tenant from a Multitenant Cisco Catalyst SD-WAN Overlay to Single-Tenant Cisco Catalyst SD-WAN Deployment , on page 46
- Migrate Multitenant Cisco Catalyst SD-WAN Overlay, on page 50
- Upgrade Cisco Catalyst SD-WAN Controller and Edge Device Software, on page 53
- Multitenant Cisco SD-WAN Manager: Disaster Recovery, on page 54
- Multitenant Cisco SD-WAN Manager: Disaster Recovery in an Overlay Network with Virtual Routers, on page 59
- Multitenant Cisco SD-WAN Manager: Disaster Recovery After a Failed Data Center Becomes Operational, on page 65
- Replace Faulty Cisco SD-WAN Controller, on page 70
- RADIUS and TACACS Support for Multitenancy, on page 71
- Configure ISE, on page 77

Cisco Catalyst SD-WAN Multitenancy

Table 1: Feature History

Feature Name	Release Information	Description
Tenant Device Forecasting	Cisco SD-WAN Release 20.6.1 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. For more information, see Tenant Device Forecasting.
Migrate Multitenant Cisco Catalyst SD-WAN Overlay	Cisco SD-WAN Release 20.6.1 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. For more information, see Migrate Multitenant Cisco Catalyst SD-WAN Overlay.
Enhanced Cisco Catalyst SD-WAN Manager Dashboard for Multitenancy	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature ensures a consistent user experience across tenant and service provider dashboards. The Cisco Catalyst SD-WAN Manager dashboard provides visibility into the available resources on shared devices.
RADIUS and TACACS Support for Multitenancy	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Control Components Release 20.12.1	This feature enables support for Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS) authentication in a multitenant deployment on WAN edge devices. For more information, see Information about RADIUS and TACACS Support for Multitenancy.

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.
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.
Support for Remote AAA and Webhook Notifications Over Management VPN 512	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature provides increased security by allowing you to configure tenants to receive AAA traffic and webhook notifications over management VPN 512.
Configure RADIUS and TACACS Servers to Receive Authentication Requests Over Management VPN 512	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature provides increased security by allowing you to configure tenants to send and receive AAA traffic over WAN transport VPN 0 or management VPN 512. For more information, see Configure Remote AAA.
Support for Multitenancy Providers to View Tenant's Alarms and Events	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature allows providers to view tenant alarms and events. Multitenancy providers can enable or disable this feature for each tenant.
Support for Tenant to Access to Controller-Specific Information	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a	This feature enables tenants to access their controller-specific restricted information, which enhances visibility and simplifies management and troubleshooting within the Cisco Catalyst SD-WAN network. This improved visibility aids in addressing issues related to OMP, routing, control connections, and more.

Information about 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 controllers: Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Validator, and Cisco Catalyst SD-WAN Controller. The tenant data is logically isolated on these shared controllers.

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. For example, a service provider using the domain name `managed-sp.com`, can assign tenants Customer1 and Customer2 the subdomains `customer1.managed-sp.com` and `customer2.managed-sp.com` and manage them on the same set of Cisco SD-WAN controllers, instead of providing each customer a single tenant setup with a dedicated set of Cisco SD-WAN controllers.

Key features of Cisco Catalyst SD-WAN multitenancy include:

- 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.
- Multitenancy:
  - Multitenant Cisco SD-WAN Manager
  - Multitenant Cisco Catalyst SD-WAN Validators
  - Multitenant Cisco Catalyst SD-WAN Controllers
- Tenant-specific WAN edge devices.
- 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 the VMware ESXi 6.7 or later, or the Kernel-based Virtual Machine (KVM) hypervisor. Cisco Catalyst SD-WAN controllers can also be hosted on Amazon Web Services (AWS) servers 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 and enabling data collection on Cisco SD-WAN Manager. The service provider must enable cloud services on Cisco SD-WAN Manager in the provider view to facilitate the onboarding of the Cisco SD-WAN Analytics instance for the tenant overlay network.



Note Starting from Cisco SD-WAN Manager Release 20.13.1, a single node multitenancy is supported. Expand a single node cluster into a multitenant deployment.

Multitenant Cisco SD-WAN Manager

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

In the Provider view, Cisco SD-WAN Manager offers service providers an overall view of the SD-WAN multitenant deployment and allows a provider to manage all the Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller devices. Cisco SD-WAN Manager also allows service providers to monitor and manage the deployments of each tenant through Provider-as-Tenant view.

In the Tenant view, Cisco 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 Cisco Catalyst SD-WAN Validators

Cisco Catalyst SD-WAN Validators are deployed and configured by the service provider. Only the provider can access a Cisco Catalyst SD-WAN Validator through the SSH terminal.

Cisco Catalyst SD-WAN Validators serve WAN edge devices of multiple tenants as the devices are added to the overlay network.

Multitenant Cisco Catalyst SD-WAN Controllers

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

- When a tenant is created, Cisco SD-WAN Manager assigns two Cisco Catalyst SD-WAN Controllers for the tenant. The Cisco Catalyst SD-WAN Controllers form an active-active cluster.

  Each tenant is assigned only two Cisco Catalyst SD-WAN Controllers. Before a tenant is created, two Cisco Catalyst SD-WAN Controllers must be available to serve the tenant.

- When more than one pair of Cisco Catalyst SD-WAN Controllers are available to serve a tenant, Cisco SD-WAN Manager assigns to the tenant the pair of Cisco Catalyst SD-WAN Controllers connected to the lowest number of forecast devices. If two pairs of Cisco SD-WAN Controllers are connected to the

same number of devices, Cisco SD-WAN Manager assigns to the tenant the pair of Cisco SD-WAN Controllers serving the lowest number of tenants.

- From Cisco vManage Release 20.9.1, while onboarding a tenant to a multitenant deployment, you can choose the pair of multitenant Cisco 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 Controllers, if necessary. For more information, see Flexible Tenant Placement on Multitenant Cisco SD-WAN Controllers.
- Each pair of Cisco Catalyst SD-WAN Controllers can serve up to 24 tenants.
- Tenants can configure custom policies on the Cisco Catalyst SD-WAN Controllers assigned to them. Cisco SD-WAN Manager notifies the Cisco Catalyst SD-WAN Controllers to pull the policy templates. Cisco Catalyst SD-WAN Controllers pull the templates and deploy the policy configuration for the specific tenant.
- Only the provider can view events, audit logs, and OMP alarms for a Cisco Catalyst SD-WAN Controller on Cisco SD-WAN Manager.



Note Starting from Cisco 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.

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

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, consult the Cloud-delivered Cisco SD-WAN Getting Started Guide.

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 Catalyst SD-WAN
Identity Services Engine (ISE) integration	Yes	Yes	No
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

Information About Tenant Migration in a Multitenant Deployment

(Minimum supported releases: 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 only supported with the Cisco Catalyst SD-WAN controllers deployed on-premises.

(Minimum supported releases: 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.

The tenant migration involves export of tenant data from the source Cisco SD-WAN Manager instance 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.

User Roles in Multitenant Environment

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

Provider Role

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

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

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



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

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

Cisco SD-WAN Manager offers two views to a provider:

- **Provider View**

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

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

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

- Provision and manage tenant routers
- Monitor overlay network of the tenant
- Create custom policies on the assigned Cisco 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 Cisco SD-WAN Manager.

Supported Devices and Controller Specifications

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

Table 3: Supported Devices

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

The following hypervisors are supported for multitenancy:

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

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

Table 4: Cisco 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

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

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

Hardware Specifications to Support 50 Tenants and 1000 Devices

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

Restrictions

- Feature availability

  See the feature availability described in Information about Cisco Catalyst SD-WAN multitenancy, on page 4.

- 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.

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

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

- Adding tenants

  If you add a second tenant immediately after adding a tenant, SD-WAN Manager adds them sequentially, and not in parallel.

- Re-adding a previously invalidated device

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

- Minimum SD-WAN Manager cluster for multitenant scenario

  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 3-Node SD-WAN Manager cluster is required for a multitenant deployment.

- Cannot upgrade devices while upgrading SD-WAN Controller or SD-WAN Validator

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

- Controller group

  The Controller group feature is not supported in multitenant mode.

- Site ID of edge devices

  The WAN edge device's site ID must be different from the SD-WAN Control Component site ID, when the SD-WAN Manager has different public and private IP addresses.

Restrictions for Migration of a Tenant from a Multitenant Overlay to a Single-Tenant Deployment

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1

- 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.

Initial Setup for Multitenancy

Prerequisites

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

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 vEdge Device	Cisco SD-WAN Release 20.6.1

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

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

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

- Follow the recommended hardware specifications in the *Supported Devices and Controller Specifications* section of this document.
- Log in to Cisco SD-WAN Manager as the provider **admin** user.

1. Create Cisco 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 SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, create a 6-node Cisco SD-WAN Manager Multitenant cluster.
2. 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.

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

3. 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 SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices across all tenants, deploy 16 Cisco SD-WAN Controllers.

   a. Add Cisco SD-WAN Controllers to the overlay network.

4. Onboard new tenants. See Add a New Tenant, on page 25.

Create a 3-Node Cisco SD-WAN Manager Multitenant Cluster

1. Download the Cisco vManage Release 20.6.1 or later software image from Cisco Software Download.
2. Create three Cisco SD-WAN Manager instances (say vManage1, vManage2, and vManage3) by installing the downloaded software image file. See Deploy Cisco SD-WAN Manager.

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

3. Complete the following operations on vManage1:
   a. Configure the following using the CLI:
      - System IP address
      - Site ID
      - Service Provider organization name (`sp-organization-name`)
      - Organization-name
      - 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

Note Configure only one default route in VPN 0.

   b. Enable Multitenancy on Cisco SD-WAN Manager, on page 18.

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

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

d. Complete the following through the Cisco 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.

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

Important Do not enable multitenancy on vManage2 and vManage3.

a. Configure the following using the CLI:

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

Note 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.

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

vManage2 reboots before being added to the cluster.

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

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

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

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

Create a 6-Node Cisco SD-WAN Manager Multitenant Cluster

1. Download the Cisco vManage Release 20.6.1 or later software image from Cisco Software Download.
2. Create six Cisco SD-WAN Manager instances by installing the downloaded software image file. See Deploy Cisco SD-WAN Manager.

Important

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

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

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

3. Complete the following operations on vManage1:

a. Configure the following using the CLI:

- System IP address
- Site ID

- Service Provider organization name (`sp-organization-name`)
- Organization-name
- 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

Note Configure only one default route in VPN 0.

b. Enable Multitenancy on Cisco SD-WAN Manager, on page 18.

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

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

d. Complete the following through the Cisco 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.

4. Complete the following operations on vManage2 through vManage6:

Important Do not enable multitenancy on vManage2 through vManage6.

a. Configure the following using the CLI:

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

Note 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 certificate, install the signed certificate.

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

e. Ping the OOB interfaces on the other 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.

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

vManage2 reboots before being added to the cluster.

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

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

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

Enable Multitenancy on Cisco SD-WAN Manager

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

Prerequisites

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

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

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

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

Note The **Domain** and **Cluster Id** values created in steps 5 and 6 serve as the Provider FQDN. Ensure these values conform to current DNS naming conventions. You can not modify these values after the configuration is saved. To change these values, a new Cisco 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 Cisco SD-WAN Controller

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
3. Click **Controllers**.

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

4. Click **Add Controller**.
5. In the **Add Controller** dialog box, do the following:
   a. In the **Controller Management IP Address** field, enter the system IP address of the Cisco 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**.

      If you select **TLS**, enter the port number to use for TLS connections. The default is 23456.

d. Check the **Generate CSR** check box for Cisco SD-WAN Manager to create a Certificate Signing Request.

e. Click **Add**.

6. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

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

   a. For the newly added Cisco 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.

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

8. Click **Install Certificate**.

9. In the **Install Certificate** dialog box, paste the **Certificate Text** or click **Select a file** upload the certificate file. Click **Install**.

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

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

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

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

    a. From the Cisco 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**.



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

    c. Find the template to be attached to the Cisco 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**.

Cisco SD-WAN Manager pushes the configuration from the template to the new controller.

In the **Configuration** > **Devices** page, the **Mode** for the Cisco SD-WAN Controller shows **Manager Mode**. The new Cisco 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 SD-WAN Release 20.6.3, 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

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.

1. Expand the existing 3-node Cisco SD-WAN Manager cluster to a 6-node cluster.
2. To support up to 100 tenants and 5000 devices, you must have 10 Cisco SD-WAN Controllers in the overlay. So, deploy 4 Cisco SD-WAN Controllers in addition to the 6 existing Cisco SD-WAN Controllers in the overlay.

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

   a. Create Cisco SD-WAN Controller instances. See Deploy the Cisco SD-WAN Controller.

   b. 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.

Note Starting from Cisco SD-WAN Manager Release 20.13.1, you can expand a single node cluster into 3 or 6 node clusters.

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

Note 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.

1. To support 100 tenants and 5000 devices: Upgrade the three Cisco 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* from the *Supported Devices and Controller Specifications* section of this document.

   From Cisco SD-WAN Release 20.6.3, Cisco vManage Release 20.6.3, to support 150 tenants and 7500 devices: Upgrade the three Cisco 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* from the *Supported Devices and Controller Specifications* section of this document.

2. Download the Cisco vManage Release 20.6.1 or a later release software image from Cisco Software Download.
3. Create three Cisco SD-WAN Manager instances (say vManage1, vManage2, and vManage3) by installing the downloaded software image file. See Deploy Cisco SD-WAN Manager.

Important

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

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

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

4. Complete the following operations on vManage1 through vManage3:

Important Do not enable multitenancy on vManage1 through vManage3.

a. Configure the following using the CLI:

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

Note Configure only one default route in VPN 0.

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

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

c. Complete the following through the Cisco 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.

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

e. Ping the OOB interfaces on the other 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.

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

   vManage1 reboots before being added to the cluster.

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

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

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

Manage Tenants

Tenant Device Forecasting

While adding a new tenant to the multitenant Cisco Catalyst SD-WAN deployment, a service provider can forecast the number of WAN edge devices that 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 responds with an appropriate error message and the device addition fails.

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

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

Benefits:

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

View Specific Cisco Catalyst SD-WAN Controller Information in Tenant Dashboard

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

When adding a new tenant or modifying an existing tenant's information, providers can allow tenants to view their specific Cisco SD-WAN Controller information. The enhanced visibility into controller information allows tenants more efficient monitoring, management, and troubleshooting using Cisco Catalyst SD-WAN Manager. For more information about configuring tenant's access to Cisco Catalyst SD-WAN Controller information, see the following sections:

- Add a New Tenant, on page 25
- Modify Tenant Information, on page 29

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

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Operated as Provider** > **Provider** > **Logs**.
3. In the **Alarms** tab, toggle **View tenant alarms**.
4. Optional: Filter alarms using **Advanced Filter** based on **Tenant**, **Object Type**, **Object List**, **Severity**, and **Type**.
5. Optional: Click the bell icon on top to view all the notifications for tenant's alarms.

What to do next:

Subscribe to tenant's alarm notifications.

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

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Operated as Provider** > **Provider** > **Logs**.

3. In the **Events** tab, toggle **View tenant events**.
4. Optional: Filter events using **Advanced Filter** based on **Tenant**, **Object Type**, **Object List**, **Severity**, and **Type**.

Add a New Tenant

Prerequisites

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

  A Cisco SD-WAN Controller enters the `Manager` mode when you push a template onto the controller from Cisco SD-WAN Manager. A Cisco SD-WAN Controller in the `CLI` mode cannot serve multiple tenants.

- Each pair of Cisco SD-WAN Controllers can serve a maximum of 24 tenants and a maximum of 1000 tenant devices. Ensure that there at least two Cisco SD-WAN Controllers that can serve a new tenant. If no pair of Cisco SD-WAN Controllers in the deployment can serve a new tenant, add two Cisco SD-WAN Controllers and change their mode to `Manager`.
- If you add a second tenant immediately after adding a tenant, Cisco SD-WAN Manager adds them sequentially, and not in parallel.
- Each tenant must have a unique Virtual Account (VA) on **Plug and Play Connect** on Cisco Software Central. The tenant VA should belong to the same Smart Account (SA) as the provider VA.
- For an on-premises deployment, create a **Validator** controller profile for the tenant on **Plug and Play Connect**. The fields in the following table are mandatory.

Table 6: Controller Profile Fields

Field	Description/Value
Profile Name	Enter a name for the controller profile.
Multi-Tenancy	From the drop-down list, select **Yes**.
SP Organization Name	Enter the provider organization name.
Organization Name	Enter the tenant organization name in the format `<SP Org Name>-<Tenant Org Name>`. **Note** The organization name can be up to 50 characters. **Note** A mismatch of organization name format of the controller profile and the tenant creation leads to a failure in device sync up.
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

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

      The description can be up to 256 characters and can contain only alphanumeric characters.
   c. Enter the name of the organization.

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

      Enter the organization name in the following format:

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

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

Note The organization name can be up to 50 characters.

A mismatch of organization name format of the controller profile and the tenant creation leads to a failure in device sync up.

   d. In the **URL Subdomain Name** field, enter the fully qualified sub-domain name of the tenant.
      - The sub-domain name must include the domain name of the service provider. For example, for the `managed-sp.com` service provider, a valid domain name can be `customer1.managed-sp.com`.

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

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



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

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



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

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

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

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

f. Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, toggle **Controller Visibility** to enable the following in your tenant's dashboard:

- In the **Monitor** dashboard, the **Controller Components** card with the **Controller** option that has an active hyperlink to view tenant-specific controller information
- In the **Devices** page, controller details relevant to tenant
- In the **Certificates** page, certificate details relevant to tenant
- In **Devices** > **Real-time**, **Control Connections** and OMP statistics relevant to tenant.

g. Click **Save**.

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

Cisco SD-WAN Manager does the following:

- creates the tenant
- assigns two Cisco SD-WAN Controllers to serve the tenant and pushes a CLI template to these controllers to configure tenant information
- sends the tenant and Cisco SD-WAN Controller information to Cisco SD-WAN Validator.

What to do next:

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

Add a new tenant in Cisco-hosted multitenant environment

1. Log in to Cisco SD-WAN Manager as the provider **admin** user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
3. Click **Add Tenant**. In the **Add Tenant** dialog box:
   a. Enter a name for the tenant. It must be the same as the Virtual Account used for the tenant.
   b. Enter a description.
   c. Enter the name of the organization in the following format:

      `<Provider Org Name>-<Tenant Org Name>`

      For 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.

Note The organization name can be up to 50 characters.

   d. Enter the sub-domain URL in FQDN format.
      - The sub-domain name must include `sdwan.cisco.com`. For example, a sub-domain name can be `Eftt1.sdwan.cisco.com`.
      - Ensure the sub-domain name is unique by performing a `nslookup` or `ping` on the expected domain. If the domain can be found, use a new URL.

      The FQ sub-domain name of the tenant is automatically added to the DNS as part of the tenant creation process. After you add a tenant, it could take up to an hour before the fully qualified sub-domain name of the tenant is resolved by the DNS.
   e. In the **Number of Devices** field, enter the number of WAN edge devices that the tenant can deploy.

      If the tenant tries to add WAN edge devices beyond this number, Cisco SD-WAN Manager reports an error and the device addition fails.
   f. Choose Auto placement or manual option for controller assignment.
   g. Click **Save**.

What to do next:

After the process is complete, Cisco SD-WAN Manager automatically generates the controller profile in the tenant Virtual Account and the FQDN. You will receive an email after completion of the process.

View Tenant Information

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1

You can view the following tenant information from the **Tenant Management** > **Tenants** page:

- **Tenant Name**
- **Description**
- **Controllers**
- **Forcasted Edge Count**
- **Total Edge Count**: Total number of both multitenant and single-tenant edge devices.
- **Multi Tenant WAN Edge Devices**: To view the number of multitenant edge device, click the non-zero number.
- **Tenant-Provider VPN Mapping**: To view the tenant and device VPN mappings for the tenant, click the non-zero number.
- **Service Connector**: View the multitenant edge device that provides a VXLAN connectivity to tenants.
- **Notifications**: View whether webhook notifications are managed by the tenant or a provider.
- **AAA**: View whether remote AAA is managed by the tenant or a provider.
- **ISE**: Starting from Cisco IOS XE Catalyst SD-WAN Release 17.18.2, you can view if ISE is configured for a tenant or a provider.
- **Controller Visibility**: View whether controller visibility is enabled or disabled.

Modify Tenant Information

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

   The tenant information is displayed in a pane on the right.
4. To modify tenant data, do as follows:
   a. In the right pane, click the pencil icon.
   b. In the **Edit Tenant** dialog box, you can modify the following:
      - **Description**: The description can be up to 256 characters and can contain only alphanumeric characters.
      - **Forecasted Edge Count**: The number of WAN edge devices that the tenant can deploy.

        A tenant can add a maximum of 1000 devices.

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

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

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

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

c. (Optional) **Configure Services**: Set up service connectors to connect Cisco SD-WAN Manager to on-premises services such as AAA or custom webhook servers via the Cisco Catalyst SD-WAN overlay.

- **Service Connector IP**: Choose the service connector IP address from the drop-down list.
- **Service Connector Interface Name**: Choose the VXLAN tunnel endpoint (interface name) from the drop-down list.
- **Provider Managed - External Services**: Enable services to enforce provider-managed or tenant-managed configuration.
  - **Notifications**: Configure alarm notifications through custom webhook channels. Choose **Yes** to enable notifications and configure a provider-managed multitenant setup. The default value is **No**, making it a tenant-managed setup.
  - **AAA**: Configure remote AAA for managing tenants. Choose **Yes** to enable remote AAA and configure a provider-managed multitenant setup. The default value is **No**, making it a tenant-managed setup.
- **Identity Services Engine**: Configure ISE for providers or tenants. Choose **Yes** for provider-managed services. Choose **No** for tenant-managed services.

d. Starting from Cisco Catalyst SD-WAN Manager Release 20.16.1, toggle **Controller Visibility** to enable the following in your tenant's dashboard:

- In the **Monitor** dashboard, the **Controller Components** card with the **Controller** option that has an active hyperlink to view tenant-specific controller information
- In the **Devices** page, controller details relevant to tenant
- In the **Certificates** page, certificate details relevant to tenant
- In **Devices** > **Real-time**, **Control Connections** and OMP statistics relevant to tenant.

e. Click **Save**

Delete a Tenant

Before you delete a tenant, delete all tenant WAN edge devices. See Delete a WAN Edge Device from a Tenant Network, on page 37.

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

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

Cisco SD-WAN Manager Dashboard for Multitenancy

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

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

View Cisco Catalyst SD-WAN Validator Health Dashlet

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1

You can view the state of each Cisco Catalyst SD-WAN Validator, which is the cumulative state of the Cisco Catalyst SD-WAN Validator in a selected time window, and the number of Cisco Catalyst SD-WAN Validators in each state in the **Validator Health** dashlet on **Monitor Overview** dashboard.

You can filter the Cisco Catalyst SD-WAN Validator dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load**.

Click **View Details** to open the **Monitor > Devices** page to view the device health in table view.

View Cisco SD-WAN Manager Health Dashlet

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1

You can view the state of Cisco SD-WAN Manager in the **Manager Health** dashlet on **Monitor Overview** dashboard.

You can filter the Cisco SD-WAN Manager dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load**.

Click **View Details** to open the **Monitor > Devices** page to view the device health in table view.

View Cisco Catalyst SD-WAN Controller Health Dashlet

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1

You can view the list of tenants hosted on a particular device by clicking the **Controller** bar. You can view the state of each Cisco Catalyst SD-WAN Controller, which is the cumulative state of the Cisco Catalyst SD-WAN Controller in a selected time window, and the number of Cisco Catalyst SD-WAN Controllers in each state in the **Controller Health** dashlet on **Monitor Overview** dashboard.

You can filter the Cisco Catalyst SD-WAN Controller dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load**.

Click **View Details** to open the **Monitor > Devices** page to view the device health in table view.

View Multi Tenant WAN Edge Health Dashlet

Minimum supported releases: Cisco Catalyst SD-WAN Manager Release 20.12.1

You can view the state of each WAN edge device, which is the cumulative state of the devices in a selected time window, and the number of WAN edge devices in each state in the **Multi Tenant WAN Edge Health** dashlet on **Monitor Overview** dashboard.

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 Multi Tenant WAN Edge Health dashlet view based on the health status using the drop-down list for **Good Devices**, **Fair Devices**, and **Poor Devices** and also for **CPU Load**.

Click **View Details** to open the **Monitor > Devices** page to view the device health in table view.

View Tenant Activity, Device, and Network Information

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

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

  To display tenant-specific status summary information,

  1. Click a tenant name from the tenant list.

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

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

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

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

View Detailed Information of a Tenant Setup

Cisco SD-WAN Manager displays the tenant dashboard, which provides information about a tenant deployment when

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

View All Network Connections in the Tenant Overlay Network

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

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

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

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



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

View Information About Device Reboots

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

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

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

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

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

View Network Connections

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

- Control Up — total number of devices with the required number of operational control plane connections to a Cisco SD-WAN Controller
- Partial — total number of devices with some, but not all, operational control plane connection to Cisco SD-WAN Controllers.
- Control Down — total number of devices with no control plane connection to a Cisco SD-WAN Controller

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



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

View State of Data Connections for a Site

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

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

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



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

View Interface Usage for WAN Edge Interfaces

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

View WAN Edge Device Counts

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

- Total — total number of authorized serial numbers for WAN edge devices that have been uploaded on Cisco 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 WAN edge devices are marked as **Valid** in the **Configuration** > **Certificates** > **WAN Edge List** screen.
- Deployed — total number of deployed WAN edge devices. These are WAN edge devices that are marked as Valid and are now operational in the network.
- Staging — total number of WAN edge devices you configure at a staging site before they are made a part of the overlay network. These routers do not take part in any routing decisions and do not affect network monitoring through Cisco SD-WAN Manager.

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

View Aggregated State of WAN Edge Devices

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

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

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

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



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

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

View WAN Edge Device Loss, Latency, Jitter

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

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

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

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

View SAIE Flow Information of WAN Edge Devices

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

Note

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

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

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

View Tunnels Data

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

- Loss
- Latency
- Jitter

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

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

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

Manage Tenant WAN Edge Devices

Add a WAN Edge Device to a Tenant Network

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

1. Log in to Cisco SD-WAN Manager.

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

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

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

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

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

5. Bootstrap the device using bootstrap configuration generated through Cisco SD-WAN Manager or manually create the initial configuration on the device.
6. If you are using Enterprise Certificates to authenticate the device, download the CSR from Cisco SD-WAN Manager and get the CSR signed by the Enterprise CA. Install the certificate on Cisco SD-WAN Manager.

Delete a WAN Edge Device from a Tenant Network

1. Log in to Cisco SD-WAN Manager.

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

   If you're a tenant user, log in as the **tenantadmin**.
2. Detach the device from any configuration templates.
3. Delete a WAN Edge Router.

Tenant-Specific Policies on Cisco SD-WAN Controller

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

When you activate or deactivate a policy,

1. Cisco SD-WAN Manager identifies the Cisco SD-WAN Controllers serving the tenant.
2. Cisco SD-WAN Manager notifies the Cisco SD-WAN Controllers to pull the policy configuration.
3. Cisco SD-WAN Controllers pull and deploy the policy configuration.
4. Cisco SD-WAN Manager reports the status of the policy pull by the Cisco SD-WAN Controllers.

Manage Tenant Data

Back Up Tenant Data

The tenant data backup solution of Cisco SD-WAN Manager multitenancy provides the following functionalities:

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

The following factors are applicable when using data backup solution:

- The tenant data backup solution operations can be performed by a tenant administrator in the tenant view and or by a provider administrator in the provider-as-tenant view. To know how to access tenant dashboard through different views, see User Roles in Multitenant Environment, on page 7.
- A tenant is allowed to perform the following backup operations at a particular time and must complete an operation before starting a new operation:
  - Back up a single configuration database
  - Download the backup file.
  - Restore or import backup files
  - Delete backup files.
  - List backup files
- A tenant backup file format is as follows:

`Bkup_tenantId_MMDDYY-HHMMSS_taskIdWithoutDash.tar.gz`

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

  The remaining tenants can continue with their backup operations.
- A tenant must perform backup and restore operations on Cisco SD-WAN Manager instances running identical Cisco SD-WAN Manager software versions.
- A tenant can store a maximum of three backup files in Cisco SD-WAN Manager and can download to store them outside Cisco SD-WAN Manager repository. If the tenant already has three backup files, a subsequent backup operation results in the earliest backup file being deleted and a new backup file being generated.
- Ensure that the following parameter values match in both the backup file and the setup where tenant has requested for a restore operation:
  - Tenant Id
  - Organization Name
  - SP Organization Name
- The tenant data backup solution creates a task in the tenant view of Cisco SD-WAN Manager. Therefore, the tenant can monitor the progress of the operation from the task view of the tenant dashboard.
- A provider cannot back up provider data using this solution. Therefore, the provider can back up all tenants information at once by backing up all tenants configuration database using CLI.

Create, Extract, and List Configuration Data Backup File

1. Log in to Cisco SD-WAN Manager.

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

   If you're a tenant user, log in as the **tenantadmin**.
2. In the address bar, modify the URL path with `dataservice` for the REST API connection.

   Example: `https://<tenant_URL>/dataservice`
3. Create a configuration backup file by using the following API:
   `https://<tenant_URL>/dataservice/tenantbackup/export`.
4. If the configuration backup file has been created successfully, Cisco SD-WAN Manager task view indicates that the backup file has been generated. You can view the process identifier of the created process or task.

   Example:

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

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

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

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

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

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

7. List backup files stored in Cisco SD-WAN Manager using the following API.

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

Restore and Delete Tenant Data Backup File

Before you begin:

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

1. Open Google Chrome, or another browser, and enable developer mode on it.
2. Log in to Cisco SD-WAN Manager.

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

   If you're a tenant user, log in as the **tenantadmin**.
3. To get header information of the restore API, do as follows:
   a. On the right side of the screen, click the **Network** tab to get the network capture view.
   b. In the network capture view, click the **Name** column to sort the listed items.
   c. Search and click **index.html**.
   d. Click the **Headers** tab and expand **Request Headers**.
   e. Choose all text under **Request Headers** and copy it to the clipboard.
4. Import backup files through the Postman UI:
   a. Open the Postman UI.
   b. To disable SSL certificate verification, click **Postman** > **Preferences** > **General** > **Request**. Turn off **SSL Certificate Verification**.
   c. In the Postman UI, create a new tab.

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

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

f. From the **GET** method drop-down list, choose **POST**.

g. In the **Paste request URL** field, paste the dedicated URL of the tenant and include `dataservice/tenantbackup/import`.

Example: `https://customer1.managed-sp.com/dataservice/tenantbackup/import`

h. Click the **Body** tab and select **form-data**.

i. Under **KEY** column, enter *bakup.tar.gz*

j. Under **VALUE** column, click **Select Files** and select a backup file to be imported.

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

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

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

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

Example:

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

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

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

6. Delete tenant data backup file through Postman UI.

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

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

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

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

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

Example:
`https://customer1.managed-sp.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c0923094dfc40ab0dle50c68c03002.tar.gz`

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

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

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

Example:

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

View OMP Statistics per Tenant on a Cisco SD-WAN Controller

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

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

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

View Tenants Associated with a Cisco SD-WAN Controller

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

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

Before You Begin

- Before you begin the migration,

- Migration of a single-tenant overlay to a multitenant deployment is only supported with the Cisco Catalyst SD-WAN controllers deployed on-premises. Migration is yet to be supported with cloud-hosted Cisco Catalyst SD-WAN controllers.
- Ensure that the edge devices in the single-tenant deployment can reach the Cisco 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 Cisco SD-WAN Manager
- Configure a maintenance window for the single-tenant overlay before performing this procedure. See Configure or Cancel SD-WAN Manager Server Maintenance Window.

- Minimum software requirements for the single-tenant overlay to be migrated:

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 Catalyst SD-WAN Controller	Cisco SD-WAN Release 20.6.1
Cisco vEdge Device	Cisco SD-WAN Release 20.6.1

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

Device	Software Version
Cisco SD-WAN Manager	Cisco vManage Release 20.6.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.6.1
Cisco Catalyst SD-WAN Controller	Cisco SD-WAN Release 20.6.1
Cisco vEdge Device	Cisco SD-WAN Release 20.6.1

- The software versions of the Cisco Catalyst SD-WAN controllers and WAN edge devices must be identical in both the single-tenant and multitenant deployments.
- We recommend that you use a custom script or a third-party application like Postman to execute the API calls.

Migration Procedure

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

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>, }`

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

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

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

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

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

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.

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

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

5. On the single-tenant Cisco 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>,
	}

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

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.

Note 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 Cisco SD-WAN Manager. If enterprise certificates are installed on the cloud-based WAN edge devices, the certificates are not affected by the migration. For more information, see Enterprise Certificates.

Migrate a Tenant from a Multitenant Cisco Catalyst SD-WAN Overlay to Single-Tenant Cisco Catalyst SD-WAN Deployment

Before You Begin

- 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 have the same Certificate Authority (CA). If not, recertify the devices after the migration is complete.
- Ensure that you check the CPU, memory, and disk size requirements of the destination overlay Cisco SD-WAN Controllers 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 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.
- Ensure that the Cisco SD-WAN Control Components in the source and destination overlays are using the same software release. The migration process does not check for a software release mismatch and a mismatch blocks the import of tenant data, causing the migration to fail.
- 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 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.
- Ensure that there are valid control connections from Cisco SD-WAN Manager to the WAN edge devices in the source overlay.
- Configure a maintenance window for the multitenant overlay before performing this procedure. See Configure or Cancel SD-WAN Manager Server Maintenance Window.

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

Migration Procedure

1. Export the 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>, }`

2. Check the status of the data export task in Cisco 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`

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 Cisco SD-WAN Manager, you can view the devices, templates, and policies imported from the multitenant overlay.

4. After the import, update information related to the device templates, policies, and other deployment-specific parameters. 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 Cisco SD-WAN Manager.

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.

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.

7. On the multitenant Cisco 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>, }`

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

8. After the migration is successfully complete, perform the following tasks:
   - If WAN edge devices have Cisco 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

Prerequisites

Minimum software requirements for Cisco Catalyst 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 vEdge Device	Cisco SD-WAN Release 20.3.3

Restrictions

- This migration procedure applies only to Cisco Catalyst 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 Cisco Catalyst SD-WAN controllers run Cisco SD-WAN Release 20.6.1 software.
- This migration procedure cannot be used to merge two or more multitenant overlays. Only one multitenant overlay can be migrated to the new setup at a time.

Migration Procedure

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

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

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

   You're prompted to set a new password.

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

3. Upload the Cisco SD-WAN Release 20.6.1 software to Cisco SD-WAN Manager. For more information, see Add an Image to the Software Repository.
4. Upgrade the Cisco SD-WAN Validator software to Cisco SD-WAN Release 20.6.1. For more information, see Upgrade the Software Image on a Device.
5. Create two Cisco SD-WAN Controller instances running Cisco SD-WAN Release 20.6.1 software. See Deploy the Cisco SD-WAN Controller.

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

   a. Add Cisco SD-WAN Controllers to the overlay network.

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

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

   A maintenance window of 3 to 4 hours is recommended.

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

Method	`POST`
URL	`https://<vmanageip>:<port>`
Endpoint	`dataservice/tenant/vsmart-mt/migrate`
Authorization	Provider **admin** user credentials.

Body	Required Format: Raw JSON `{}`

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

In Cisco SD-WAN Manager, check the status of the migration task using the `processId` from the API response. During the migration task, the following changes are affected:

a. The older Cisco SD-WAN Controllers are invalidated and deleted from the overlay network.

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

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

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

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

Verify the Migration

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

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

   b. View Tenants Associated with a Cisco SD-WAN Controller, on page 42.

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

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

Upgrade Cisco Catalyst SD-WAN Controller and Edge Device Software

Prerequisites

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

Device	Software Version
Cisco SD-WAN Manager	Cisco vManage Release 20.4.1 or later
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.4.1 or later
Cisco Catalyst SD-WAN Controller	Cisco SD-WAN Release 20.4.1 or later
Cisco vEdge Device	Cisco SD-WAN Release 20.4.1 or later

Upgrade Procedure

1. Upgrade the software on the three Cisco 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.

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

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

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

Multitenant Cisco SD-WAN Manager: Disaster Recovery

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

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

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

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

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

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

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

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

To test disaster recovery, you can simulate a scenario in which the active Cisco 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

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

Restrictions

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

Configure a Standby Cisco SD-WAN Manager Cluster

1. Configure the standby Cisco SD-WAN Manager nodes with a similar running configuration as the active Cisco SD-WAN Manager nodes. Install local certificates on the standby Cisco SD-WAN Manager nodes.



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

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

With the standby Cisco SD-WAN Manager nodes configured in this manner, the overlay network is not aware of the standby Cisco SD-WAN Manager cluster.

Back Up the Active Cisco SD-WAN Manager Cluster Configuration

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

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

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

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

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

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

   In the following example, `db_backup.tar.gz` is copied from the active Cisco SD-WAN Manager node to the `/home/admin/` directory of a standby Cisco 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 Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

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

Note

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

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

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

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

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

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

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

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

   b. Verify that the page displays all active and standby Cisco SD-WAN Manager nodes.

4. On the standby Cisco SD-WAN Manager nodes, enable the transport interface on VPN 0.

   Use one of the following two methods:

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

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

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

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

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

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

b. Click **Controllers**.

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

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

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

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

6. Disconnect the active Cisco SD-WAN Manager nodes from the overlay network.

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

Use one of the following two methods:

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

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

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

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

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

Send the list of controllers:

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

b. Click **Controllers**.

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

c. Click **Send to Validator**.

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

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

8. Verify that the following are intact:

- Policies
- Templates
- Controller and WAN edge device lists

9. Verify the valid Cisco SD-WAN Manager nodes.

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

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

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

In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

10. Invalidate the previously active Cisco SD-WAN Manager nodes.

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

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

b. Click **Controllers**.

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

c. For each previously active Cisco SD-WAN Manager node, click **...** and click **Invalidate**.

11. Verify the valid Cisco SD-WAN Manager nodes.

    a. Log in to the CLI of each Cisco 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 Cisco SD-WAN Manager nodes are listed.

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

       In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

The Cisco SD-WAN Manager cluster that was initially the standby cluster is now the active Cisco SD-WAN Manager cluster.

Multitenant Cisco SD-WAN Manager: Disaster Recovery in an Overlay Network with Virtual Routers

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

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

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

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

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

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

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

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

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

Prerequisites

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

Restrictions

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

Configure a Standby Cisco SD-WAN Manager Cluster

1. Configure the standby Cisco SD-WAN Manager nodes with a similar running configuration as the active Cisco SD-WAN Manager nodes. Install local certificates on the standby Cisco SD-WAN Manager nodes.



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

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

With the standby Cisco SD-WAN Manager nodes configured in this manner, the overlay network is not aware of the standby Cisco SD-WAN Manager cluster.

Back Up the Active Cisco SD-WAN Manager Cluster Configuration

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

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

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

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

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

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

   In the following example, `db_backup.tar.gz` is copied from the active Cisco SD-WAN Manager node to the `/home/admin/` directory of a standby Cisco 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 Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

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

Note

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

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

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

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

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

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

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



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

   b. Verify that the page displays all active and standby Cisco SD-WAN Manager nodes.

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

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

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

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

6. On the standby Cisco SD-WAN Manager nodes, enable the transport interface on VPN 0.

   Use one of the following two methods:

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

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

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

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

7. Add each standby Cisco SD-WAN Manager node to the overlay network.

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

   b. Click **Controllers**.



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

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

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

e. Repeat **Step 7c** and **Step 7d** for every Cisco SD-WAN Validator.

8. Disconnect the active Cisco SD-WAN Manager nodes from the overlay network.

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

Use one of the following two methods:

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

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

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

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

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

Send the list of controllers:

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

b. Click **Controllers**.

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

c. Click **Send to Validator**.

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

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

10. Verify that the following are intact:
    - Policies
    - Templates
    - Controller and WAN edge device lists

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

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

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

       In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

12. Invalidate the previously active Cisco SD-WAN Manager nodes.

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



Note
- After you invalidate the Cisco SD-WAN Manager nodes, the nodes cannot be reused without performing additional steps that are beyond the scope of this document.
- When you invalidate the previously active Cisco SD-WAN Manager nodes, Cisco SD-WAN Manager marks the nodes as invalid and sends an update to all controllers. However, Cisco SD-WAN Manager does not send an updated list of valid Cisco SD-WAN Manager UUIDs to Cisco SD-WAN Validator immediately because the previously active Cisco 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 Cisco SD-WAN Manager nodes.

  Cisco 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 Cisco SD-WAN Manager. Cisco SD-WAN Manager sends the updated list of valid Cisco SD-WAN Manager UUIDs to Cisco SD-WAN Validator only after the cloud WAN edge devices have been moved to the active Cisco 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 Cisco SD-WAN Manager nodes.

    a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

    b. Click **Controllers**.

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

c. For each previously active Cisco SD-WAN Manager node, click **...** and click **Invalidate**.

13. Verify the valid Cisco SD-WAN Manager nodes after 24 hours.

    a. Log in to the CLI of each Cisco 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 Cisco SD-WAN Manager nodes are listed.

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

       In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controllers.

The Cisco SD-WAN Manager cluster that was initially the standby cluster is now the active Cisco SD-WAN Manager cluster.

Multitenant Cisco SD-WAN Manager: Disaster Recovery After a Failed Data Center Becomes Operational

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

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

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

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

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

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

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

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

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

to be the active Cisco 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.

Check the Configuration of the Standby Cisco SD-WAN Manager

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



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

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

With the standby Cisco SD-WAN Manager nodes configured in this manner, the overlay network is not aware of the standby Cisco SD-WAN Manager cluster.

Back Up the Active Cisco SD-WAN Manager Cluster Configuration

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

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

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

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

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

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

   In the following example, `db_backup.tar.gz` is copied from the active Cisco SD-WAN Manager node to the `/home/admin/` directory of a standby Cisco 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 Cisco SD-WAN Manager Cluster Using the Configuration Database Backup

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



Note

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

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

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

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

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

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

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



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

   b. Verify that the page displays all active and standby Cisco SD-WAN Manager nodes.

4. On the standby Cisco SD-WAN Manager nodes, enable the transport interface on VPN 0.

   Use one of the following two methods:

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

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

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

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

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

5. Add each standby Cisco SD-WAN Manager node to the overlay network.
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
   b. Click **Controllers**.



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

   c. For a Cisco SD-WAN Validator, click **...** and click **Edit**.
   d. In the **Edit** dialog box, enter the following details of the Cisco SD-WAN Validator: WAN transport IP address, username, and password.
   e. Repeat **Step 5c** and **Step 5d** for every Cisco SD-WAN Validator.

6. Disconnect the active Cisco SD-WAN Manager nodes from the overlay network.



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

   Use one of the following two methods:
   a. Shut down the transport interface in VPN 0: On the CLI of each active Cisco SD-WAN Manager node, run the **shutdown** command.

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

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

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

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

   Send the list of controllers:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.
   b. Click **Controllers**.



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

c. Click **Send to Validator**.

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

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

8. Verify that the following are intact:

- Policies
- Templates
- Controller and WAN edge device lists

9. Verify the valid Cisco SD-WAN Manager nodes.

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

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

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

In the command output, verify that the chassis numbers of the active and previously active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controller.

10. Invalidate the previously active Cisco SD-WAN Manager nodes.



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

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Certificates**.

b. Click **Controllers**.

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

c. For each previously active Cisco SD-WAN Manager node, click **...** and click **Invalidate**.

11. Verify the valid Cisco SD-WAN Manager nodes.

a. Log in to the CLI of each Cisco 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 Cisco SD-WAN Manager nodes are listed.

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

In the command output, verify that the chassis numbers of only the active Cisco SD-WAN Manager nodes are listed. Also, check whether the device is connected to the active Cisco SD-WAN Manager nodes and the Cisco Catalyst SD-WAN Controllers.

The Cisco SD-WAN Manager cluster that was initially the standby cluster is now the active Cisco SD-WAN Manager cluster.

Replace Faulty Cisco SD-WAN Controller

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

1. Create a Cisco SD-WAN Controller instance. See Deploy the Cisco SD-WAN Controller.
2. Add the Cisco SD-WAN Controller to the overlay network.
3. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
4. Click **Controllers**.

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

5. For the faulty Cisco SD-WAN Controllers, click **...** and click **Invalidate**.

The **Invalidate** dialog box appears.

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

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 Cisco SD-WAN Controller that should replace the faulty instance.

c. Click **Invalidate**.

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

RADIUS and TACACS Support for Multitenancy

Information about RADIUS and TACACS Support for Multitenancy

From Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, Cisco SD-WAN Manager supports for RADIUS and TACACS servers in a multitenant deployment.

RADIUS

RADIUS is a distributed client and server system that secures networks that have authorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information.

TACACS

TACACS is a security application that provides centralized validation of users attempting to gain access to an access point. Unlike RADIUS, TACACS does not authenticate wireless client devices accessing the network through an access point.

TACACS provides for separate and modular authentication, authorization, and accounting. Each service can be tied into its own database to take advantage of other services available on that server or on the network.

TACACS administered through the AAA security services can provide these services:

- Authentication: Provides complete control of authentication through login and password dialog, challenge and response, and messaging support.
- Authorization: Provides fine-grained control of user privileges for the duration of the session, including access control, session duration, or protocol support. You can also enforce restrictions on the commands to execute a TACACS authorization feature.
- Accounting: Collects and sends information used for billing, auditing, and reporting to the TACACS daemon. Network managers can use the accounting feature to track administrator activity for security audit or to provide information for user billing. Accounting records include administrator identities, start and stop times, executed commands, number of packets, and number of bytes.

Note NAT is not supported between Cisco SD-WAN Manager and the multitenant connector.

Prerequisites for Cloud Multitenant with On-Prem Per-tenant AAA and Provider AAA

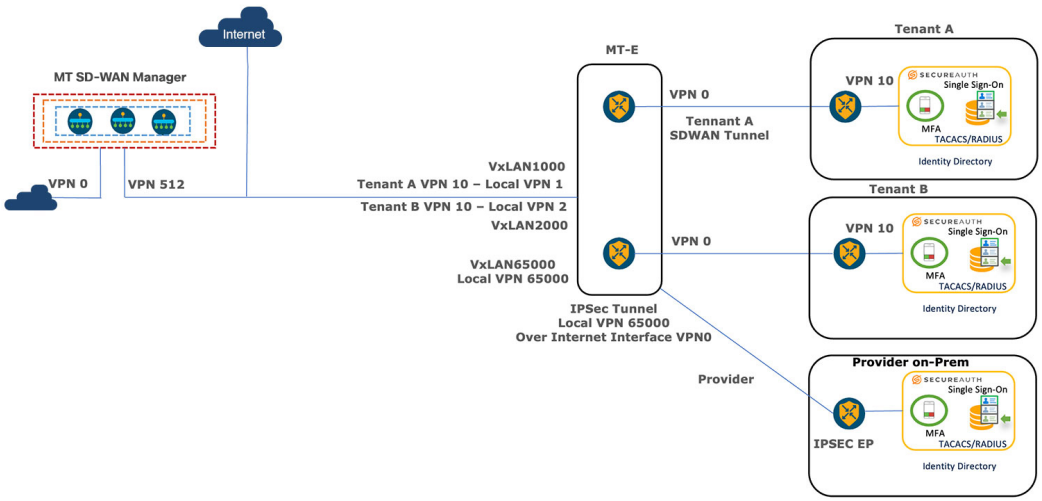
Prerequisites for Cloud Multitenant with On-Prem Per-tenant AAA and Provider AAA

- A Multitenant edge connector is onboarded in Cisco SD-WAN Manager.
- Provider can have tenant configurations only through a device or feature template.
- The edge connector is on the same premises as the controllers.
- Cisco SD-WAN Manager is configured with VPN 512 interface.
- VxLAN tunnels must use the VPN 512 interface as the underlay.
- In a Cisco SD-WAN Manager cluster, there is a VxLAN tunnel created between each Cisco SD-WAN Manager node and the edge connector.
- A provider's RADIUS and TACACS server cannot be shared with the tenant.
- RADIUS and TACACS server authentication is within the tenant network.
- Multiple RADIUS and TACACS servers are used for the same tenant.
- A tenant's RADIUS and TACACS server is on-prem or cloud-hosted.

Note You must configure an external AAA server and provide mapping between the user and the Viptela groups to authentication. For example, Viptela-Group-Name as basic, tenantadmin, or operator.

The following illustration shows the architecture of the cloud multitenancy with on-prem per tenant and provider AAA.

Figure 1: Cloud Multitenant with On-Prem Per-tenant and Provider AAA



Workflows to Configure Remote AAA

Enable Multitenancy

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Edit** adjacent to the **Tenancy Mode Tenancy Mode**. If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.
3. Click **Multitenant**.
4. In the **Domain** field, enter the domain name of the service provider (for example, managed-sp.com).
5. Enter a **Cluster Id** (for example, cluster-1 or 123456).
6. Click **Save**. If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Proceed** to confirm that you want to change the tenancy mode.

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

For information about configuring AAA using feature templates for a single tenant, see Configuring AAA using Cisco SD-WAN Manager Template.

Configure the Tenant

To on board the Edge Connector in a Cisco SD-WAN Manager provider, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Tenant Management**.
2. Click **Edit** adjacent to the **Tenant**.

   The **Edit Tenant** window is displayed.
3. Enter the description in the **Description** field.
4. Enter the edge number in the **Forecasted Edge** field.
5. Enter the sub-domain URL in the **URL Subdomain** field.
6. Enable the **Edge Connector** option.
7. Choose the **Edge Connector IP** from the drop-down list.
8. Choose the VXLAN tunnel endpoint from the **Edge Connector VTEP Interface Name** drop-down list.

   For a cloud deployment, it is essential to provision the Cloud-hosted SD-WAN Control Components and gateway with the third interface **GigabitEthernet3** for AAA. When selecting the VXLAN tunnel endpoint from the **Edge Connector VTEP Interface Name** drop-down list, choose **GigabitEthernet3**. Selecting any other interface, such as **VPN 0** or **VPN 512**, might result in misconfiguration.
9. Click **Save**.

Configure Remote AAA

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

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **Remote AAA**.
3. Expand the **Remote AAA** tab to configure remote AAA.
4. Enter the order in which to attempt different authentication methods in the **Authentication Order** field.
5. Choose the option in **Authentication Fallback** to fallback if higher-priority authentication fails.
6. Choose the **Admin Authentication Order** to authenticate a tenantadmin user according to the authentication order.
7. Enable or disable audit logs in the **Disable Audit Logs** field.
8. Enable or disable user accounting in the **Enable/disable user accounting** field.
9. Click **Save** to save the changes.

Configure RADIUS

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **Remote AAA**.
3. Expand the **RADIUS** tab to configure a RADIUS server.
4. Enter the duration to wait for replies from the RADIUS server in the **Timeout** field.
5. Enter the number of times you want to contact a RADIUS server in the **Retransmit Count** field.
6. Click **New RADIUS Server** to add a new RADIUS server.

Field	Description
Radius Server Details	
Address	Enter the IP address of the RADIUS server.
Authentication Port	Enter the port to connect to the RADIUS server.
Accounting Port	Enter the port used to connect to the server.
Key	Enter the password to access the RADIUS server.
Secret Key	Enter the AES encrypted key to access the RADIUS server.
Priority	Enter the server priority.
VPN ID	Enter the VPN in which the RADIUS server. **Note** This option is available in Cisco Catalyst SD-WAN Manager Release 20.15.x and earlier.

Field	Description
VPN IP Subnet	Enter the VPN IP subnet (VXLAN tunnel VPN IP subnet) in which the RADIUS server is located. **Note** This option is available in Cisco Catalyst SD-WAN Manager Release 20.15.x and earlier.
Network Connectivity **Note** This Network Connectivity option is available from Cisco Catalyst SD-WAN Manager Release 20.16.1.	
Source VPN	Choose from these VPN options, the location of the RADIUS server: • **0**: Transport VPN. • **512**: Management VPN. Configure these fields only if you have specified the tenant to manage the AAA server. These fields do not appear if the multitenant setup is configured to be managed by the provider. • (Optional) **Source Subnet**: Enter the VPN IP subnet that is unique within the tenant network. • (Optional) **Destination VPN**: Enter the VPN in which the RADIUS server is located.

7. Click **Save** and **Add**.

Configure TACACS

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users**.
2. Click **Remote AAA**.
3. Expand the **TACACS** tab to configure TACACS.
4. Enter the duration to wait for replies from the TACACS server in the **Timeout** field.
5. Choose the TACACS authentication type from the **Authentication** drop-down list.
   - ASCII
   - PAP
6. Click **New TACACS Server** to add a new TACACS server.

Field	Description
TACACS Server Details	
Address	Enter the IP address of the TACACS server.

Field	Description
Authentication Port	Enter the port to connect to a TACACS server.
Key	Enter the password to access the TACACS server.
Secret Key	Enter the AES encrypted key to access the TACACS server.
Priority	Enter the TACACS server priority.
VPN ID	Enter the VPN in which the TACACS server. **Note** This option is available in Cisco Catalyst SD-WAN Manager Release 20.15.x and earlier.
VPN IP Subnet	Enter the VPN IP subnet in which the TACACS server is located. **Note** This option is available in Cisco Catalyst SD-WAN Manager Release 20.15.x and earlier.
Network Connectivity **Note** The Network Connectivity option is available from Cisco Catalyst SD-WAN Manager Release 20.16.1.	
Source VPN	Choose from these VPN options, the location of the TACACS server: • **0**: Transport VPN. • **512**: Management VPN. Configure these fields only if you have specified the tenant to manage the AAA server. These fields do not appear if the multitenant setup is configured to be managed by the provider. • (Optional) **Source Subnet**: Enter the VPN IP subnet that is unique within the tenant network. • (Optional) **Destination VPN**: Enter the VPN in which the TACACS server is located.

7. Click **Add**.

Verify RADIUS and TACACS Configuration for Multitenancy

The following is a RADIUS and TACACS configuration example on Cisco IOS XE Catalyst SD-WAN devices through CLI:

```
Device# interface GigabitEthernet4

 description   VTEP Interface
```

```
 no shutdown

 arp timeout 1200

 ip address 172.1.1.101 255.255.255.0

 no ip redirects

 ip mtu    1500

 load-interval 30

 mtu           1500

 negotiation auto

exit
```

Use the **show ip interface brief** command to show the AAA configuration:

```
Device# show ip interface brief | i <VPN IP SUBNET of VxTunnel>

Where <VPN IP SUBNET of VXTunnel> is one that is configured under Tenant - > Administration
 -> Remote AAA
```

The output shows one tunnel per one node. If there are three nodes in a cluster, the output displays three tunnels in the subnet.

Configure ISE

Before you begin

Choose who manages ISE, provider or tenant.

1. From the SD-WAN Manager menu, choose **Administration** > **Tenant Management.**.
2. Go to the tenant and from the **Identity Service Engine** dropdown, choose one of these:
   - For Provider-managed services, choose **Yes**.
   - For Tenant-managed services, choose **No**.

Procedure

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

Step 2 Follow the steps in Configure Cisco ISE in Cisco SD-WAN Manager for Multitenancy.