

Cisco Catalyst SD-WAN Multitenancy (Cisco SD-WAN Releases 20.4.x and 20.5.x)

Table 1: Feature History

Feature Name	Release Information	Feature Description
Cisco Catalyst SD-WAN Multitenancy	Cisco SD-WAN Release 20.4.1 Cisco vManage Release 20.4.1	With Cisco Catalyst SD-WAN multitenancy, a service provider can manage multiple customers, called tenants, from Cisco SD-WAN Manager. In a multitenant Cisco Catalyst SD-WAN deployment, tenants share Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Validators and Cisco Catalyst SD-WAN Controllers. Tenant data is logically isolated on these shared resources.

- Overview of Cisco Catalyst SD-WAN Multitenancy, on page 1
- User Roles in Multitenant Environment, on page 4
- Hardware Supported and Specifications, on page 5
- Initial Setup for Multitenancy, on page 7
- Manage Tenants, on page 10
- Cisco SD-WAN Manager Dashboard for Multitenancy, on page 13
- Manage Tenant WAN Edge Devices, on page 18
- Tenant-Specific Policies on Cisco Catalyst SD-WAN Controllers, on page 19
- Manage Tenant Data, on page 19
- View OMP Statistics per Tenant on a Cisco SD-WAN Controller, on page 23
- View Tenants Associated with a Cisco SD-WAN Controller, on page 23
- Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment, on page 24

Overview of 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 Cisco SD-WAN Manager instances, Cisco Catalyst SD-WAN Validators, and Cisco Catalyst SD-WAN Controllers. The domain name of the service provider has subdomains for each tenant. For example, the `multitenancy.com` service provider can manage the tenants Customer1 (`Customer1.multitenancy.com`) and Customer2 (`Customer2.multitenancy.com`).

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

- 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.
- Multi-tenant 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.



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

You can find the IP address of the `vmanage_system` interface from the output of the **show interface description** command. Alternatively, you can launch the device SSH terminal from Cisco SD-WAN Manager and find the vmanage_system IP address from the first line of the log-in prompt.

  - Cisco SD-WAN Manager offers service providers an overall view of the SD-WAN multi-tenant deployment and allows a provider to manage the shared 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.
  - Cisco SD-WAN Manager allows tenants to monitor and manage their deployment. Through Cisco SD-WAN Manager, tenants can deploy and configure WAN edge devices. Tenants can also configure custom policies on assigned Cisco Catalyst SD-WAN Controllers.
- Multi-tenant 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.



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

You can find the IP address of the `vmanage_system` interface from the output of the **show interface description** command. Alternatively, you can launch the device SSH terminal from Cisco SD-WAN Manager and find the vmanage_system IP address from the first line of the log-in prompt.

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



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

You can find the IP address of the `vmanage_system` interface from the output of the **show interface description** command. Alternatively, you can launch the device SSH terminal from Cisco SD-WAN Manager and find the vmanage_system IP address from the first line of the log-in prompt.

  - 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.

  - Each pair of Cisco Catalyst SD-WAN Controllers can serve a maximum of 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.

- WAN Edge Devices:

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



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

You can find the IP address of the `vmanage_system` interface from the output of the **show interface description** command. Alternatively, you can launch the device SSH terminal from Cisco SD-WAN Manager and find the vmanage_system IP address from the first line of the log-in prompt.

  - A provider can manage the WAN edge devices only from provider-as-tenant view. In the provider view, Cisco SD-WAN Manager does not present 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.

- 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 vSphere ESXi or the Kernel-based Virtual Machine (KVM) hypervisor. Cisco Catalyst SD-WAN controllers can also be deployed in the cloud on Amazon Web Services (AWS) servers.

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 Manager IP address. When using a domain name, the domain name has the format `https://multitenancy.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 Cisco Catalyst SD-WAN 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 vManage 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 Catalyst SD-WAN Validators and Cisco Catalyst SD-WAN Controllers.
  - Add, modify, or delete tenants.
  - Monitor the overlay network.

- **Provider-as-Tenant View**

When a provider user selects a specific tenant from the **Select Tenant** drop-down list at the top of the provider dashboard, Cisco 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.multitenancy.com` for a provider using the domain name `https://multitenancy.com`. When the user logs in, Cisco SD-WAN Manager presents the tenant view and displays the tenant dashboard.

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 Catalyst SD-WAN Controllers
- Upgrade the software on the tenant routers.

Hardware Supported and Specifications

The following platforms support multitenancy.

Table 2: Router Models

Platform	Router 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

The following hypervisors and deployment model are supported for multitenancy.

Table 3: Deployment Model

Specification	Description
Supported hypervisors	VMware, KVM, AWS (cloud-hosted by Cisco)
Cisco SD-WAN Manager Deployment Model	Cluster, 3 Cisco SD-WAN Manager instances with each instance running all Cisco SD-WAN Manager services.

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

Table 4: On-prem Deployment

Server	Cisco SD-WAN Manager	Cisco Catalyst SD-WAN Validator	Cisco Catalyst SD-WAN Controller
Deployment Model	Cluster	N/A	Non-containerized
Number of Instances	3	2	2 per 24 tenants
CPU **DRAM** **Hard Disk**	32 vCPU 72 GB 1 TB	4 vCPU 4 GB 10 GB	8 vCPU 16 GB 16 GB
NMS Service Distribution	Some services run on all three Cisco SD-WAN Manager instances in the cluster, while some services run on only one of the three instances in the cluster. Therefore, the CPU load may vary among the instances.	N/A	N/A

Note If DPI is enabled, we recommend that the aggregated DPI data across all Cisco SD-WAN Managere instances not exceed 350 GB per day.

Initial Setup for Multitenancy

Prerequisites

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

Table 5: Software Prerequisites for Cisco Catalyst SD-WAN Multitenancy

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

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.

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

1. Create three Cisco SD-WAN Manager instances and associated configuration templates. See Deploy Cisco SD-WAN Manager.
   a. While configuring Cisco SD-WAN Manager instances, configure the service provider organization name (`sp-organization-name`) and the organization name (`organization-name`).

      Example:

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

2. Configure one of the Cisco SD-WAN Manager instances to support multitenancy. See Enable Multitenancy on Cisco SD-WAN Manager, on page 8

3. Create a Cisco SD-WAN Manager cluster consisting of three Cisco SD-WAN Manager instances. See Cluster Management.
   - The Cisco SD-WAN Manager cluster must have three Cisco SD-WAN Manager instances. A cluster with more than three instances or fewer than three instances is not a supported configuration for Cisco Catalyst SD-WAN multitenancy.
   - While creating the Cisco SD-WAN Manager cluster, add the Cisco SD-WAN Manager instance configured to support multitenancy before adding the other two Cisco SD-WAN Manager instances.
4. Certify all instances of Cisco SD-WAN Manager. See Generate Cisco SD-WAN Manager Certificate.
5. Create and configure Cisco SD-WAN Validatorinstances. 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
   ```
6. Create Cisco SD-WAN Controller instances. See Deploy the Cisco SD-WAN Controllers.

   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 12 Cisco SD-WAN Controllers.

   a. Add Cisco SD-WAN Controllers to the overlay network.
7. Onboard new tenants. See Add a New Tenant.

Enable Multitenancy on Cisco SD-WAN Manager

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, multitenancy.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.

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** by attaching a template to the device.
    a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
    b. Click **Device Templates**.

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

c. Find the template to be attached to the Cisco 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**. The new Cisco SD-WAN Controller is ready to be used in your mutitenant deployment.

Manage Tenants

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. 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 Cisco SD-WAN 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**.

Field	Description/Value
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.
Primary Controller	Enter the host details for the primary Cisco SD-WAN Validator.

For a cloud deployment, the Cisco SD-WAN Validator controller profile is created automatically as part of the tenant creation process.

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.

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

   b. Enter a description of the tenant.

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

   c. Enter the name of the organization.

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

      Enter the organization name in the following format:

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

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



Note The organization name can be up to 50 characters.

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

      - The sub-domain name must include the domain name of the service provider. For example, for the `multitenancy.com` service provider, a valid domain name can be `Customer1.multitenancy.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 the Cisco SD-WAN Manager **Administration** > **Settings** > **Tenancy Mode** GUI navigation path.

- 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.

  When creating fully qualified domain names (FQDN) the following DNS entries are required:

  - **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. 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 Validators.

What to do next:

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

Modify Tenant Information

1. Log in to Cisco 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, modify the tenant name, description, or domain name.
   c. Click **Save**

Delete a Tenant

Before you delete a tenant, delete all tenant WAN edge devices. See Delete a WAN Edge Device from a Tenant Network, on page 19.

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 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** at the left bar.

- 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 Catalyst SD-WAN Validators, 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** > **Devices** screen, or access the **Tools** > **SSH Terminal** Screen.



Note In Cisco vManage Release 20.6.x and earlier releases, **Real Time** view is part of the **Monitor** > **Network** screen.

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 **Crashes**. 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 In Cisco vManage Release 20.6.x and earlier releases, **Real Time** view is part of the **Monitor** > **Network** screen.

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 In Cisco vManage Release 20.6.x and earlier releases, **Real Time** view is part of the **Monitor** > **Network** screen.

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** > **Devices** screen

    Cisco vManage Release 20.6.x and earlier: **Real Time** view from the **Monitor** > **Network** screen
  - **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 **Details**. You can choose to change the displayed health type and time period.

View DPI Flow Information of WAN Edge Devices

The **Top Applications pane** displays DPI flow information for traffic transiting routers in the overlay network.

Note DPI flow information is shown only for the last 24 hours. To view DPI 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 DPI 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

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 Catalyst SD-WAN Controllers

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 Catalyst SD-WAN Controllers serving the tenant. The user can configure a CLI policy or create the policy using the UI policy configuration wizard.

When you activate or deactivate a policy,

1. Cisco SD-WAN Manager identifies the Cisco Catalyst SD-WAN Controllers serving the tenant.
2. Cisco SD-WAN Manager notifies the Cisco Catalyst SD-WAN Controllers to pull the policy configuration.
3. Cisco Catalyst SD-WAN Controllers pull and deploy the policy configuration.
4. Cisco SD-WAN Manager reports the status of the policy pull by the Cisco Catalyst 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 over tenant view and as a provider. To know how to access tenant dashboard through different views, see User Roles in Multitenant Environment, on page 4.

- 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.
- When a backup or restore operation for a specific tenant is in-progress, other tenants are allowed to perform the backup and restore operations smoothly.
- 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 use the same Cisco SD-WAN Manager version for backup generation and restore operation.
- 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.multitenancy.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.multitenancy.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.multitenancy.com/dataservice/tenantbackup/delete?fileName=bkup_1579026919487_012820-180712_c09230904dfc40edb0d1e50b68b03002.tar.gz

Example:

```
https://Customer1.multitenancy.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

Table 7: Feature History

Feature Name	Release Information	Description
Migrate Single-Tenant Cisco Catalyst SD-WAN Overlay to Multitenant Cisco Catalyst SD-WAN Deployment	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature enables you to migrate a single-tenant Cisco Catalyst SD-WAN overlay to a multitenant deployment using a sequence of Cisco SD-WAN Manager API calls.

Before You Begin

- Before you begin the migration,
  - 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
  - Ensure that the Certificate Authority (CA) on both single-tenant and multitenant Cisco SD-WAN Managers are same.
  - Configure a maintenance window for the single-tenant overlay before performing this procedure. See Configure or Cancel vManage Server Maintenance Window.
- Minimum software requirements for the single-tenant overlay to be migrated:

Device	Software Version
Cisco SD-WAN Manager	Cisco vManage Release 20.5.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.5.1
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.5.1
Cisco vEdge Device	Cisco SD-WAN Release 20.4.1

- 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 20.5.1
Cisco SD-WAN Validator	Cisco SD-WAN Release 20.5.1
Cisco SD-WAN Controller	Cisco SD-WAN Release 20.5.1
Cisco vEdge Device	Cisco SD-WAN Release 20.5.1

- 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 `multitenancy.com` is the domain name of service provider, and the tenant name is `Customer1`, the tenant sub-domain name would be `Customer1.multitenancy.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.