

Multitenancy Tenant Management

- Feature history for tenant management, on page 1
- Tenant management, on page 1
- Add a new tenant, on page 3
- Manage tenant WAN edge devices, on page 7
- Manage tenant data, on page 9
- View tenants associated with a Cisco SD-WAN Controller, on page 13
- View OMP statistics per tenant on a Cisco SD-WAN Controller, on page 14

Feature history for tenant management

Developments in tenant management, by release.

Table 1: Feature history

Feature name	Release information	Description
Tenant Device Forecasting	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	With this feature, a service provider can control the number of WAN edge devices a tenant can add to their overlay network. By doing so, the provider can utilize Cisco Catalyst SD-WAN controller resources efficiently.

Tenant management

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

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

Tenant device forecasting

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

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

Benefits of tenant device forecasting

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

Restrictions for tenant management

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

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

Prerequisites for adding a tenant

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

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

Table 2: Controller profile fields

Field	Description/Value
Profile Name	Enter a name for the controller profile.
Multitenancy	From the drop-down list, select **Yes**.
SP Organization Name	Enter the provider organization name.

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

Add a new tenant

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

Procedure

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

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

Step 3 Click **Add Tenant**.

Step 4 Enter tenant information.

Table 3: Tenant information

Item	Description
Tenant Name	Enter a name for the tenant. The name must match the Virtual Account used for the tenant.
Tenant Description	Enter a description with up to 256 alphanumeric characters.
Organization Name	Enter the organization name (case-sensitive, unique per tenant). • Format: <Provider Org Name>-<Tenant Org Name> • Maximum length: 50 characters Example: If the provider organization name is 'EFT20.17-VA-Main – 841534' and the tenant organization name is 'T1', enter the organization name as **`EFT20.17-VA-Main – 841534-T1`**. The tenant organization name can be T1 for Tenant 1, T2 for Tenant 2, and so on.

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

Enter the fully qualified subdomain of the tenant.

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

Step 6 Configure DNS.

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

Provider level:

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

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

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

Tenant level:

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

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

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

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

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

Adding more devices than allowed will trigger an error.

Step 8 Click **Save**.

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

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

What to do next

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

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

View tenant information

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

Use these steps to view detailed information about a tenant.

Procedure

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

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

Table 4: Tenant details

Field	Description
Tenant Name	Name of the tenant.
Description	Tenant description
Controllers	SD-WAN Controllers assigned to the tenant.
Forecasted Edge Count	Predicted number of WAN edge devices.
Total Edge Count	Total number of both multitenant and single-tenant edge devices.
Multitenant WAN Edge Devices	Click the non-zero number to view the number of multitenant edge devices.
Tenant-Provider VPN Mapping	Click the non-zero number to view tenant and device VPN mappings.
Service Connector	Shows the multitenant edge device that provides VXLAN connectivity to tenants.
Notifications	Indicates whether webhook notifications are managed by the tenant or provider.
AAA	Indicates whether remote AAA is managed by the tenant or provider.
Controller Visibility	Indicates whether controller visibility is enabled or disabled.

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 8.

Use these steps to delete a tenant.

Procedure

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

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

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

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

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

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

Add a tenant in a Cisco-hosted multitenant environment

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

Procedure

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

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

Step 3 Click **Add Tenant**.

Step 4 Enter tenant information.

Table 5: Tenant information

Item	Description
Tenant Name	Enter a name for the tenant.
Tenant Description	Enter a description with up to 256 alphanumeric characters.

Item	Description
Organization Name	Enter the organization name (case-sensitive, unique per tenant). • Format: <SP Org Name>-<Tenant Org Name> • Maximum length: 50 characters Example: If the provider organization name is 'multitenancy' and the tenant organization name is 'Customer1', while adding the tenant, enter the organization name as multitenancy-Customer1. Any mismatch with controller profile causes device sync failure

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

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

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

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

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

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

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

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

Step 8 Click Save.

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

Manage tenant WAN edge devices

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

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

Add a WAN edge device to a tenant network

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

If you are adding a WAN edge device that you had previously invalidated and deleted from an overlay network, you must reset the device software after adding the device.

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

Procedure

Step 1 Log in to SD-WAN Manager.

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

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

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

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

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

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

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

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

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

a) Download the CSR from SD-WAN Manager.
b) Get the CSR signed by the Enterprise CA.
c) Install the certificate on SD-WAN Manager.

Delete a WAN edge device from a tenant network

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

Procedure

Step 1 Log in to SD-WAN Manager.

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

Step 2 Detach the device from any configuration templates.

Step 3 Delete the device.

Manage tenant data

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

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

Back up tenant data

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

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

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

Usage

Tenant data backup operations can be performed:

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

Allowed backup operations

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

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

Limitations

Defines the limitations of provider access for backing up data.

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

View back up data

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

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

Backup and restore guidelines for tenant data

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

Follow these guidelines for tenant backup and restore operations.

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

  If three files already exist, the earliest backup file is deleted when a new backup is generated.
- Backup files can also be downloaded and stored outside the Cisco SD-WAN Manager repository.
- Ensure the following parameter values match in both the backup file and the target setup:
  - Tenant ID
  - Organization Name

- SP Organization Name

Create data backup file

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

Procedure

Step 1 Log in to Cisco SD-WAN Manager.

- If you are a provider user, log in as the **admin**.

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

Step 2 Modify the URL path for REST API access.

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

Example:

https://<tenant_URL>/dataservice

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

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

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

Example:

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

Step 5 Verify the task status.

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

Example:

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

Step 6 Extract or download the backup file.

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

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

Step 7 List available backup files.

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

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

Restore tenant data backup file

Use these steps to restore tenant data backup file.

Before you begin

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

Procedure

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

Step 2 Log in to Cisco SD-WAN Manager.

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

Step 3 Get header information for the restore API:

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

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

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

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

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

Example:

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

Monitor backup data restore

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

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

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

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

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

Example:

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

Delete a tenant

Before you delete a tenant, delete all tenant WAN edge devices. See Delete a WAN edge device from a tenant network, on page 8.

Use these steps to delete a tenant.

Procedure

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

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

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

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

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

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

View tenants associated with a Cisco SD-WAN Controller

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

Procedure

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

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

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

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

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

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

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

Procedure

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

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

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

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

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

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

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

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

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