Multitenant WAN Edge Devices

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Table 1: Feature History

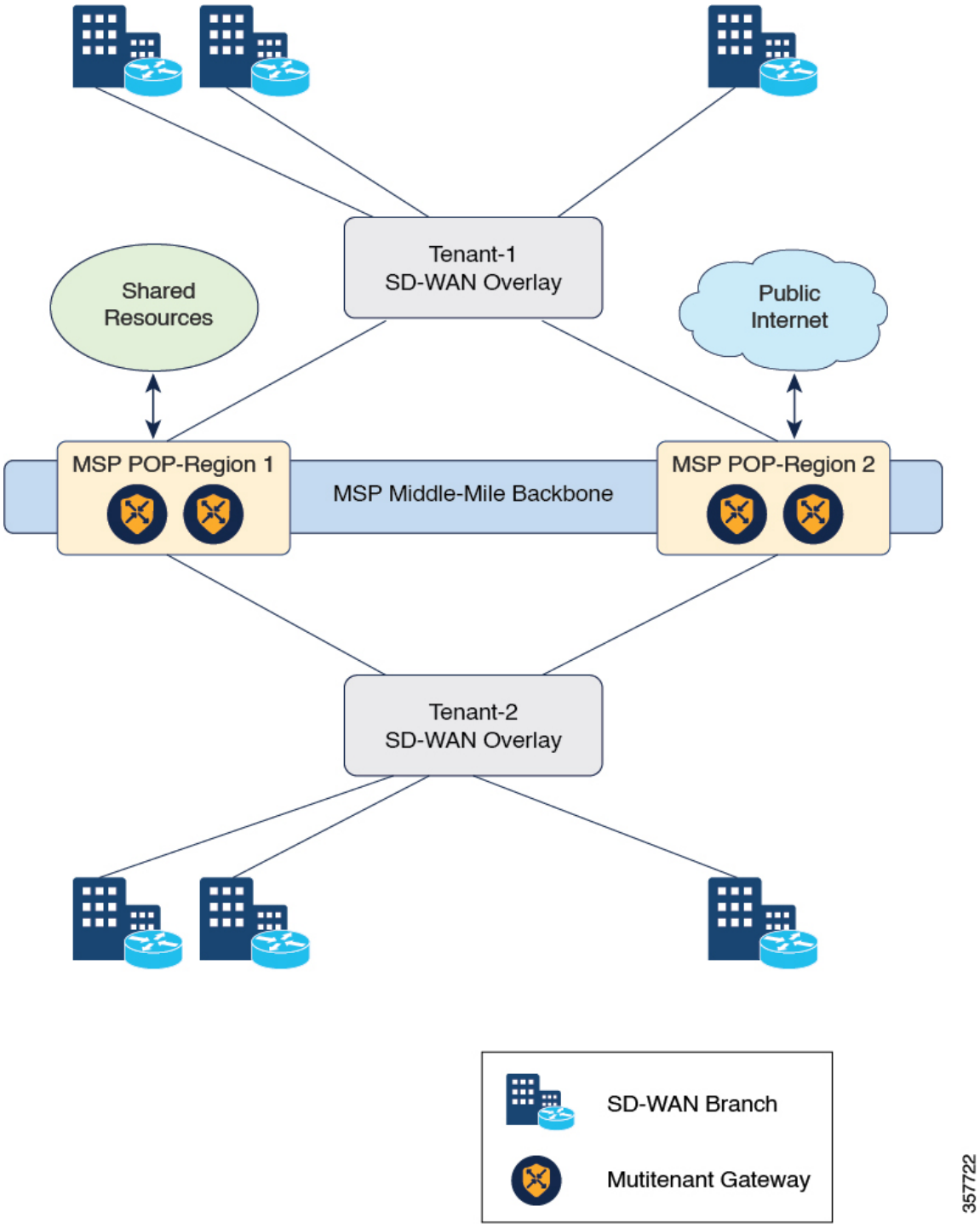
Feature Name	Release Information	Description
Multitenant WAN Edge Devices	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	With this feature, a service provider can deploy, configure, and manage multitenant WAN edge devices in a multitenant Cisco Catalyst SD-WAN deployment.
Distribute Device Resources Among Tenants Using Tiers	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a Cisco vManage Release 20.8.1	With this feature, you can define tiers and assign tenants to tiers. While defining a tier, you limit the amount of a multitenant WAN edge resource that is allocated to a tenant in the tier, when the tenant is onboarded to a multitenant WAN edge device. From this release, you can specify how many tenant VPNs can be created for a tenant belonging to a tier. In subsequent releases, tiers will be enhanced to support limits on the usage of additional device resources such as firewall, NAT, and TLOCs.

Feature Name	Release Information	Description
Enhanced Multitenant Tier Definition to include Route and TLOC Resource-Usage Limits	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1	This feature is enhanced to support route and TLOC resource-usage limits. A service provider can assign a tier to limit the routes and TLOC resource-usage to the tenant based on the service agreement.
Enhanced Multitenant Tier Definition to include NAT Limits	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	With this feature, you can configure maximum limit on NAT translations per tenant. From this release **Tier** is called **Resource Profile** in Cisco SD-WAN Manager.

Information About Multitenant WAN Edge Devices

As a service provider managing a multitenant Cisco Catalyst SD-WAN deployment, you may wish to deploy a multitenant WAN edge device in the overlay network to serve as a shared gateway for traffic belonging to multiple tenants. For example, you can deploy such a shared gateway in each regional point of presence (PoP). You can carry inter-region traffic belonging to multiple tenants through these shared gateways and the transport backbone linking the PoPs.

Figure 1: Multitenant WAN Edge Devices as Shared Gateways



Multitenant WAN edge devices isolate traffic belonging to different tenants by mapping a tenant service VPN (referred to as tenant VPN) to a device VPN (also referred to as the device VRF). Cisco SD-WAN Manager performs the mapping between the tenant and device VPNs when you onboard a tenant on a multitenant WAN edge device.

Multitenant WAN edge devices establish control connections with the Cisco SD-WAN Validator nodes specified in the bootstrap configuration, and then connect to nodes in the Cisco SD-WAN Manager cluster. When you onboard a tenant to a multitenant WAN edge device, the device establishes control connections to the Cisco SD-WAN Controller assigned to the tenant.

The service provider must deploy, configure, and manage multitenant WAN edge devices. The devices and their states are displayed only in the Cisco SD-WAN Manager provider view. The provider, acting on behalf of the tenant, must deploy, configure, and manage single-tenant WAN edge devices owned by a tenant. The devices and their states are displayed in the tenant view or the provider-as-tenant view. When a tenant is onboarded to a multitenant WAN edge device, the multitenant WAN edge device can interoperate with single-tenant WAN edge devices owned by the tenant and other multitenant WAN edge devices to which the tenant is onboarded.

Resource Profiles (Tiers)

When you onboard many tenants on a multitenant WAN edge device, you may need to distribute the limited device resources among the tenants to ensure fair usage of resources or to implement different service-level agreements (SLAs). A tier lets you define and limit how much of each device resource a tenant assigned to the tier can consume. After creating a tier, when you onboard a tenant, you assign a tenant to a particular tier to apply the resource-usage limits to the tenant.

Usage Notes

- After you create a tier, you cannot modify the device-resource-usage limits specified in the tier. To apply a different set of limits to tenants, you must create a new tier and assign the relevant tenants to the new tier.
- You can delete a tier only when no tenants are assigned to it.

Resource Usage Limits in Resource Profiles (Tiers)

Table 2: Resource Usage Limits in Tiers

Resource Usage Limit	Description	Available From
Number of VPNs	Maximum number of tenant VPNs that can be created for a tenant belonging to the tier. Cisco SD-WAN Manager enforces the limit when you create a new tenant VPN for a tenant. • If you have already created the maximum number of tenant VPNs specified in the tier, Cisco SD-WAN Manager reports the error and doesn't apply the configuration.	Cisco IOS XE Release 17.8.1 and Cisco vManage Release 20.8.1

Resource Usage Limit	Description	Available From
Route-limit	The number of IPv4 unicast and IPv6 unicast routes that can be created for a tenant belonging to the tier. Route limit on a tenant is the sum of routes from all VRFs.	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1
TLOC	TLOC allows you to map transport interfaces to tenants. At least one TLOC needs to be selected per tier and you can include up to 16 TLOCs in a tier.	Cisco IOS XE Catalyst SD-WAN Release 17.10.1a Cisco vManage Release 20.10.1
NAT limit	The maximum limit on the number of NAT translations per tenant. Once the maximum limit has reached for a tenant, the packets are dropped and further translations are not allowed.	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1

Benefits of Multitenant WAN Edge Devices

As a managed service provider, by deploying multitenant WAN edge devices, you can

- reuse the edge devices and the interconnecting transport backbone to serve multiple tenants
- lower capital and operational expenditure
- provide faster access to tenants to shared resources, SaaS, and IaaS through the shared transport backbone
- manage tenant association with the devices, tenant-specific policies, and QoS requirements with Cisco SD-WAN Manager as the unified management interface

Supported Devices for Multitenant WAN Edge Devices

Device Family	Device Model
Cisco ASR 1000 Series Aggregation Services Routers	ASR 1001-HX ASR 1001-X ASR 1002-HX ASR 1002-X **Note** Cisco IOS XE Catalyst SD-WAN Release 17.9.1a is the last supported release for ASR 1001-X and ASR 1002-X.

Cisco Catalyst 8000V Edge Software	Catalyst 8000V
Cisco Catalyst 8300 Series Edge Platforms	C8300-1N1S-4T2X C8300-1N1S-6T C8300-2N2S-4T2X C8300-2N2S-6T
Cisco Catalyst 8500 Series Edge Platforms	C8500-12X C8500-12X4QC C8500L-8S4X
Cisco ISR 4000 Series Integrated Services Routers	ISR 4461

Prerequisites for Multitenant WAN Edge Devices

- You must have completed the initial setup for a multitenant Cisco Catalyst SD-WAN deployment.
  - Multitenant Cisco SD-WAN Validator and Multitenant Cisco SD-WAN Controller must run Cisco SD-WAN Release 20.7.1 or a later release software.
  - Multitenant Cisco SD-WAN Manager must run Cisco vManage Release 20.7.1 or a later release software.
  - Cisco IOS XE Catalyst SD-WAN devices must run Cisco IOS XE Release 17.7.1 or a later release software.

Restrictions for Multitenant WAN Edge Devices

- The provider must own, deploy, and manage all multitenant WAN edge devices in the deployment. The provider must also deploy and manage any single-tenant device owned by a specific tenant.
- You must configure unique system IP address for each WAN edge device in the multitenant Cisco Catalyst SD-WAN deployment, irrespective of whether the device is a multitenant device owned and managed by the provider or a single-tenant device owned by a tenant and managed by the provider on behalf of the tenant.
- You can configure a maximum of 16 SLA classes. You can either assign specific SLA classes to tenants or share SLA classes among tenants.
- You cannot migrate a single-tenant WAN edge device from the tenant-level to serve as a multitenant WAN edge device at the provider-level. You must decommission the single-tenant device and delete it from Cisco SD-WAN Manager, perform a factory reset on the device to erase the existing configuration, and onboard the device at the provider-level.
- Multitenant WAN edge device do not support the following:
  - Cloud Express and Multicloud workflows

- Zone-Based Firewall (ZBFW) and advanced security features
- Per-tenant DPI statistics
- Dynamic on-demand tunnels
- SNMP
- Per-tenant management of NAT resources
- OMP IPv6 route filtering
- OMP notifications

- Tenant limits takes precedence when VRF limits are also configured.

Configure Multitenant WAN Edge Devices

Configuration Workflow

Perform the following configuration procedures as the Provider admin user.

1. Complete Initial Setup for Multitenancy.
   a. Add Tenants.
   b. (Optional) Onboard Tenant-Owned WAN Edge Devices.

Note As the provider admin, you must onboard the devices from the provider-as-tenant view. Configure unique system IP address for each WAN edge device in the deployment across all tenant overlay networks.

2. Enable Multitenant WAN Edge Deployment.
3. Onboard WAN Edge Devices at the Provider Level.

Note
- Importing WAN edge device details from the Plug and Play (PnP) portal to Cisco SD-WAN Manager using **Sync Smart Account** is not supported. Export the device serial file from the PnP portal and import the file to Cisco SD-WAN Manager.
- Configure unique system IP address for each WAN edge device in the deployment across all tenant overlay networks.

4. Enable Multitenancy on Provider-Managed WAN Edge Devices.
5. Create Tiers.
6. Onboard Tenants to a Multitenant WAN Edge Device.
7. Create Tenant VPN for Onboarded Tenants.

8. (Optional) Configure Required Policies.

Enable Multitenant WAN Edge Deployment

Before You Begin

Ensure that every WAN edge device in the deployment, across tenants, is configured with a unique system IP address.

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
3. Find **MT Edge Deployment Settings** and click **Edit**.
4. For **Enable MT Edge Deployment**, click **Enabled**.

   By default, **Enable MT Edge Deployment** is **Disabled**.
5. Click **Save**.

If two or more WAN edge devices in the deployment are configured with the same system IP address, Cisco SD-WAN Manager reports an error. Modify the configuration of the WAN edge devices and try to enable multitenant WAN edge deployment.

Onboard WAN Edge Devices at the Provider Level

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. Upload the device serial number file to Cisco SD-WAN Manager. While uploading the file, choose the option to validate and send the device list to controllers.
3. Bootstrap the device using bootstrap configuration generated through Cisco SD-WAN Manager or manually create the initial configuration on the device.
4. If you are using Enterprise Certificates to authenticate the device, download the Certificate Signing Request (CSR) from Cisco SD-WAN Manager and get the CSR signed by the Enterprise CA. Install the certificate on Cisco SD-WAN Manager.
5. Create a configuration template for the device and attach the device to the template.

   While configuring the device, configure the service provider organization name as `sp-organization-name` and the tenant `organization-name`.

Enable Multitenancy on Provider-Level WAN Edge Devices

You can enable multitenancy on a provider-level WAN edge using the Multi Tenant parameter in the System template.

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

4. Find the System template of the provider-level WAN edge device for which you wish to enable multitenancy.
5. For the System template, click **…** and click **Edit**.
6. In the Basic Configuration area, find the **Multi Tenant** parameter. Initially, the parameter has a default scope and the default value **Off**. For the **Multi Tenant** parameter,
   a. Click the scope drop-down list and choose **Global** scope.
   b. Click **On** to enable multitenancy.
7. Click **Update** to save and apply the modified configuration.

The provider-level WAN edge device can serve more than one tenant.

Create a Resource Profile (Tier)

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 **Resource Profiles**.

   In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profiles** is called **Tiers**.

   Any existing tiers are displayed in a table.
4. Click **Add a Resource Profile**.

   In Cisco vManage Release 20.11.1 and earlier releases, **Add a Resource Profile** is called **Add Tier**.
5. In the **Add Tier** slide-in pane, do the following:
   a. Enter the following details:

Field	Description
Resource Profile Name In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profile Name** is called **Tier Name**.	Enter a unique name for the tier.
Maximum VPN	Enter the maximum number of VPNs that can be created on a multitenant WAN edge device for a tenant assigned to this tier. Minimum value: 1 Maximum value: The maximum number of VPNs that you can specify for a tier depends on the device model. See Table 3: Maximum Number of VPNs Supported by Each Device Model, on page 11.

Field	Description
NAT Limit (Optional)	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1 Enter the maximum number of NAT translations that are allowed on each tenant.
Route Limit (Optional)	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 (Optional) Specify IPv4 unicast or IPv6 unicast route limits. Route limit on a tenant is the sum of routes from all VRFs. Default value is 0. **Note** The value 0 means there is no route limit configured in the tier definition.
Route Limit Type	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 The following two route limit types can be configured for IPv4 or IPv6 routes on the device: • **Warning-only**: This option allows to install new tenant IPv4 or IPv6 routes even after total exceeds their respective limit. A warning message is shown on device console when IPv4 route limit or IPv6 route limit is exceeded. • **Warning with threshold**: This option allows to configure a warning threshold, which is the percentage of the route limit. A warning message is shown on device console when the threshold percentage of IPv4 route limit or IPv6 route limit is reached. When a tenant's total IPv4 or IPv6 routes exceed the configured IPv4 or IPv6 route limit, routes are rejected.
Threshold	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 Specify the route limit threshold value when you chose **Warning with threshold** option. When threshold percentage of IPv4 or IPv6 route limit is reached, a warning message is displayed on the device console. Range: 1 to 100.

Field	Description
Allowed Transport In Cisco vManage Release 20.11.1 and earlier releases, **Allowed Transport** is called **TLOC**.	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 Add TLOC details for the tier. For a tier, add at least one TLOC and up to 16 TLOCs. A TLOC definition includes the TLOC color and the encapsulation type. Range: 1 to 16
Color	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 Select the color from the drop-down list. The color attribute helps to identify an individual WAN transport tunnel.
Encapsulation	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1 Select encapsulation type as either GRE or IPSec per TLOC configuration.

Table 3: Maximum Number of VPNs Supported by Each Device Model

Device Model	Maximum Number of VPNs
ASR1001-X	80
ASR1001-HX	336
ASR1002-X	336
ASR1002-HX	336
C8500-12X4QC	336
C8500-12X	336
C8500L-8S4X	336
C8300-1N1S-6T	200
C8300-1N1S-4T2X	200
C8300-2N2S-6T	200
C8300-2N2S-4T2X	200
Catalyst 8000V	300
ISR4461	80

b. To add the tier, click **Save**. To discard your entries and close the slide-in pane, click **Cancel**.

After you click **Save**, the slide-in pane is closed and the new tier is listed in the table along with any existing tiers.

Onboard Tenants to a Multitenant WAN Edge Device

You can onboard tenants to a multitenant WAN edge device using the Tenant template. If you haven't onboarded a tenant to the device, create a tenant template, add tenants, and attach the tenant template to the device template. If you have onboarded tenants to the device, to onboard a new tenant, update the tenant template attached to the device.

When a new tenant is onboarded to the multitenant WAN edge device, the device establishes control connections to the Cisco SD-WAN Controllers assigned to the tenant.

Before You Begin

Before onboarding the tenant to a multitenant WAN edge device, add the tenant to the multitenant deployment and create the tier with which you wish to associate the tenant.

Create a Tenant Template

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Find the device template for the multitenant WAN edge device to which you wish to onboard tenants.
4. For the device template, click **…** and click **Edit**.

   The device template is displayed.
5. Click **Additional Templates**.
6. In the **Additional Templates** area, click the **Tenant** template drop-down list and then click **Create Template**.
7. In the Tenant template form, do as follows:
   a. Enter a unique **Template Name**. The template name can contain up to 128 alphanumeric characters.
   b. Enter a **Description** for the template. The description can contain up to 2048 alphanumeric characters.
   c. In the **Tenant** area, click **New Tenant**.
   d. From the **Tenant Name** drop-down list, choose the tenant organization name.

      In Cisco vManage Release 20.11.1 and earlier releases, **Tenant Name** is called **Org Name**.
   e. From the **Resource Profile Name** drop-down list, choose a tier for the tenant.

      In Cisco vManage Release 20.11.1 and earlier releases, **Resource Profile Name** is called **Tier Name**.
   f. Click **Add**.
   g. Repeat **Step c** to **Step f** to add additional tenants.
8. Click **Save**.
9. For the device template, click **Update** to save and apply the modified configuration.
10. Select the target device in the left pane and click **Configure Devices**.

Update a Tenant Template

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Click **Feature**.
4. For the tenant template attached to the device, click **…** and click **Edit**.

   The tenant template is displayed.
5. In the Tenant template form, do the following:
   a. In the **Tenant** area, click **New Tenant**.
   b. From the **Org Name** drop-down list, choose the tenant organization name.
   c. From the **Tier Name** drop-down list, choose a tier for the tenant.
   d. Click **Add**.
   e. Repeat **Step a** to **Step d** to add additional tenants.
6. Click **Update**.

Create Tenant VPN for Onboarded Tenants

After onboarding a tenant to a multitenant WAN edge device, use the Cisco VPN template to create tenant VPNs. To isolate VPN traffic of one tenant from the VPN traffic of other tenants onboarded on the multitenant WAN edge device, Cisco SD-WAN Manager maps a tenant VPN ID to a device VPN ID while you create the tenant VPN.

Create a Cisco VPN Template

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Find the Device template for the multitenant WAN edge device to which you wish to onboard tenants.
4. For the device template, click **…** and click **Edit**.

   The device template is displayed.
5. Click **Service VPN**.
6. In the **Service VPN** area, click **Add VPN**.
7. In the **Add VPN** slide-in pane, click **Create VPN Template**.
8. In the **Create VPN Template** slide-in pane, do the following:
   a. Enter a unique **Template Name**. The template name can contain up to 128 alphanumeric characters.
   b. Enter a **Description** for the template. The description can contain up to 2048 alphanumeric characters.
   c. In the **Basic Configuration** area, map the tenant VPN ID to a device VPN ID:
      1. From drop-down list corresponding to **Tenant VPN**, choose the tenant organization name.

2. In the text field corresponding to **Tenant VPN**, enter the tenant VPN ID.
3. Click **Generate VPN ID**.

   A read-only **VPN** field displays the device VPN ID for the tenant VPN ID. This mapping is performed by Cisco SD-WAN Manager. For a tenant, Cisco SD-WAN Manager maps a particular tenant VPN ID to the same device VPN ID on all the multitenant WAN edge devices.

d. Configure other properties of the tenant VPN in the template.

e. Click **Save**.

9. In the **Add VPN** slide-in pane, move the template created in **Step 8** from **Available VPN Templates** to **Selected VPN Templates**.
10. Click **Next**.
11. Add any additional Cisco VPN templates as needed.
12. Click **Add**.
13. For the device template, click **Update** to save and apply the modified configuration.
14. Select the target device in the left pane and click **Configure Devices**.

Update a Cisco VPN Template

If you made a copy of an existing Cisco VPN template, you must modify the template for the new tenant VPN that you wish to create.

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
3. Click **Feature**.
4. For the copied Cisco VPN template, click **…** and click **Edit**.

   The Cisco VPN template is displayed.
5. In the Cisco VPN template form, do the following:

   a. In the **Basic Configuration** area, map the tenant VPN ID to a device VPN ID:

   1. From drop-down list corresponding to **Tenant VPN**, choose the tenant organization name.
   2. In the text field corresponding to **Tenant VPN**, enter the tenant VPN ID.
   3. Click **Update VPN ID**.

      A read-only **VPN** field displays the device VPN ID for the tenant VPN ID. This mapping is performed by Cisco SD-WAN Manager. For a tenant, Cisco SD-WAN Manager maps a particular tenant VPN ID to the same device VPN ID on all the multitenant WAN edge devices.

   b. Configure other properties of the tenant VPN in the template.

   c. Click **Update**.
6. Attach the Cisco VPN template to the device template of the target multitenant WAN edge device.

When you try to apply the tenant VPN configuration to the device, Cisco SD-WAN Manager checks the following:

1. The number of tenant VPNs that can be created for a tenant is restricted by the maximum number of the VPNs that is specified in the tier to which the tenant belongs. If the maximum number of tenant VPNs is already created for the tenant, Cisco SD-WAN Manager reports an error and does not apply the VPN configuration to the device.
2. Each device model supports a certain maximum number of device VPNs. On a multitenant WAN edge device, each tenant VPN is mapped to device VPN. If the maximum number of device VPNs supported by the device are already created and mapped to tenant VPNs, Cisco SD-WAN Manager reports an error and does not apply the configuration to the device.

Remove Tenant from a Multitenant WAN Edge Device

To remove a tenant from a multitenant WAN Edge Device, you must detach the tenant service VPN template from the device template and delete the tenant from the Tenant template.

1. Log in to Cisco SD-WAN Manager as the Provider admin user.
2. Remove the tenant service VPN template from the Device template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Find the device template for the multitenant WAN edge device to which you wish to onboard tenants.
   c. For the device template, click **…** and click **Edit**.

      The device template is displayed.
   d. Click **Service VPN**.
   e. In the **Service VPN** area, check the check box for the VPN template to be removed.
   f. Click **Remove VPN**.
   g. Click **Update** to save and apply the modified configuration.
3. Delete tenant from the Tenant template:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. Click **Feature**.
   c. Find the Tenant template from which you should delete the tenant.
   d. For the Tenant template, click **…** and click **Edit**.
   e. In the Tenant section, find the organization name of the tenant you wish to delete.
   f. Click the Trash icon corresponding to the tenant organization name.
   g. Click **Update** to save and apply the modified configuration.

Delete a Tier

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 **Tiers**.

   Existing tiers are displayed in a table.
4. For the desired tier, click **…** in the **Actions** column, and then, click **Delete**.
5. In the **Delete Tier** dialog box, confirm that you wish to delete the tier.

   The tier is deleted and is no longer listed in the table.

Verify Configuration and Operation of Multitenant WAN Edge Devices

View Tenants Onboarded to Multitenant WAN Edge Device

- The following is a sample output of the **show sdwan running-config tenant** command.

```
Device# show sdwan running-config tenant

tenant "multitenancy-Customer1"
 tier
  tier-name tier_tenant1
  max-vpn   10
 !
 tenant-vpn 1
  device-vpn 1
 !
 tenant-tloc mpls ipsec
 !
 tenant-tloc public-internet ipsec
 !
!
tenant "multitenancy-Customer2"
 tier
  tier-name tier_tenant2
  max-vpn   12
 !
 tenant-vpn 1
  device-vpn 2
 !
 tenant-tloc mpls ipsec
 !
 tenant-tloc public-internet ipsec
 !
!
tenant "multitenancy-Customer3"
 tier
  tier-name tier_tenant3
  max-vpn   10
 !
 tenant-vpn 1
```

```
  device-vpn 3
 !
 tenant-tloc mpls ipsec
 !
 tenant-tloc public-internet ipsec
 !
!
tenant "multitenancy-Customer4"
 tier
  tier-name tier_tenant4
  max-vpn   10
 !
 tenant-vpn 1
  device-vpn 4
 !
 tenant-tloc mpls ipsec
 !
 tenant-tloc public-internet ipsec
 !
!
```

- The following is a sample output of the **show sdwan tenant-summary** command.

```
Device# show sdwan tenant-summary
tenants-summary max-tenants 30
tenants-summary num-active-tenants 4
                                    GLOBAL
ORG NAME                   ID      UUID
------------------------------------------------------------------------------
multitenancy-Customer1  16880   774cf81a-1d35-47f3-8c3f-ccb12506e09c
multitenancy-Customer2  23216   62c614be-fc18-4ed0-8f77-ddcd5196a412
multitenancy-Customer3  22400   48ba0449-f177-49c3-926c-a6d5077e34ae
multitenancy-Customer4  14624   61684731-4bda-40b9-9067-c2c9b846f8e8
```

- The following is a sample output of the **show tenant all** command.

```
Device# show tenant all

Tenant           ID          Tier             Tenant VPNs
-------------------------------------------------------------------------------------------------------------------------------
Tenant1         16880       tier_tenant1            1
Tenant2         23216       tier_tenant2            1
Tenant3         22400       tier_tenant3            1
Tenant4         14624       tier_tenant4            1
```

- The following is a sample output of the **show tenant mapping table** command.

```
Device# show tenant mapping table

Tenant        Tenant VPN         Device VPN          Active
-------------------------------------------------------------------------------------------------------------------------------
Tenant1          1                  1                 YES
Tenant2          1                  2                 YES
Tenant3          1                  3                 YES
Tenant4          1                  4                 YES
```

- The following is a sample output of the **show tenant Tenant1** command.

```
Device# show tenant Tenant1

Tenant Tenant1
```

```
  Tenant ID:     30176
  UUID:          5a8b858d-d090-4cc3-8321-a663b08043d3
  Flags:         0x0000
  Resource Limits (Tier "tier_tenant1"):
    Maximum IPv4 Routes           100 (warning-threshold:50)
    Maximum IPv6 Routes           100 (warning-only)
    Maximum NAT Sessions            3

  Mapping Entries:
    Tenant VPN       ->              Device VPN
    1                ->              1               (Active)
```

- The following is a sample output of the **show ip route tenant Tenant1** command.

```
Device# show ip route tenant Tenant1

Tenant name is Tenant1 (id:30176)
    route_limit: 100, warning_limit_percent: 50%
    route_count: 7, rejected_routes: 0

    vrf_name: 1, vrf_id: 4, tenant_vpn_id: 1 route_count: 7, rejected_routes: 0


Routing Table: 1
    Tenant Name: Tenant1, Tenant ID: 30176
    Rejected Routes in tenant: 0, Rejected Routes in this routing table: 0
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.11.0/24 is directly connected, GigabitEthernet4.101
L        172.16.11.2/32 is directly connected, GigabitEthernet4.101
m        172.16.21.0/24 [251/0] via 172.16.255.16, 2w4d, Sdwan-system-intf
m        172.16.31.0/24 [251/0] via 172.16.255.14, 2w4d, Sdwan-system-intf
S     192.168.11.0/24 [1/0] via 172.16.11.1
m     192.168.21.0/24 [251/0] via 172.16.255.16, 2w4d, Sdwan-system-intf
m     192.168.31.0/24 [251/0] via 172.16.255.14, 2w4d, Sdwan-system-intf
```

- The following is a sample output of the **show ipv6 route tenant Tenant1** command.

```
Device# show ipv6 route tenant Tenant1

Tenant name is Tenant1 (id:30176)
    route_limit: 100, warning_only: True
    route_count: 1, rejected_routes: 0

    vrf_name: 1, vrf_id: 4, tenant_vpn_id: 1 route_count: 1, rejected_routes: 0

IPv6 Routing Table - 1 - 1 entries
    Tenant Name: Tenant1, Tenant ID: 30176
```

```
    Rejected Routes in tenant: 0, Rejected Routes in this routing table: 0
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, ls - LISP destinations-summary, a - Application
       m - OMP
L   FF00::/8 [0/0]
     via Null0, receive
```

- The following is a sample output of the **Show run | sec tenant-definition** command.

```
Device# show run | sec tenant-definition

tenant-definition "Tenant1"
 global-tenant-id 45516
 universal-unique-id 696e6fa0-078c-47fb-81b1-40df3b04c8e1
 !
 tier tier_tenant6
  max nat-session 10
  max routes
   !
   address-family ipv4
    unicast-route-limit 15000 warning-threshold 80
   !
   address-family ipv6
    unicast-route-limit 15000 warning-threshold 80
 !
 tenant-vpn-id 1
  device-vpn 1
```

- The following is a sample output of the **show ip nat translations tenant Tenant1 total** command.

```
Device# show ip nat translations tenant Tenant1 total

Total number of translations: 2
```

- The following is a sample output of the **show logging | i TENANT** command.

```
Device# show logging | i TENANT

*Feb  4 21:10:33.625: %IOSXE-4-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000
TS:00000004456610265827 %NAT-4-PER_TENANT_MAX_ENTRIES: per-tenant maximum limit of 10
reached for 26144.
```

- The following is a sample output IPv4 WARNING-ONLY Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/18 09:16:23.973714834 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
09:16:23.973: %RIBTENANT-3-ROUTELIMITWARNING_ON: tenant(name:Tenant1, id:16880) ipv4
unicast route limit warning threshold: alarm_on
```

Note ROUTELIMITWARNING_ON: “alarm_on” means the route count has crossed the route limit.

```
Device# show ip route tenant "Tenant2"

2022/11/18 09:33:40.651174649 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
09:33:40.651: %RIBTENANT-3-ROUTELIMITWARNING_OFF: tenant(name:Tenant1, id:16880) ipv4
unicast route limit warning threshold:
alarm_off
```

Note ROUTELIMITWARNING_OFF: “alarm_off” means for the time being, route count is reduced and it has not crossed the warning/route limit.

- The following is a sample output of IPv6 WARNING-ONLY Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/18 09:11:23.589778787 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
09:11:23.589: %RIBTENANT-3-ROUTELIMITWARNING_ON: tenant(name:Tenant1, id:16880) ipv6
unicast route limit warning threshold: alarm_on
```

Note ROUTELIMITWARNING_ON: "alarm_on" means the route count has crossed the route limit.

```
Device# show ip route tenant "Tenant2 Inc"

2022/11/18 09:33:40.661037261 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
09:33:40.661: %RIBTENANT-3-ROUTELIMITWARNING_OFF: tenant(name:Tenant1, id:16880) ipv6
unicast route limit warning threshold:
alarm_off
```

Note ROUTELIMITWARNING_OFF: “alarm_off” means for the time being, route count is reduced and it has not crossed the warning/route limit.

- The following is a sample output IPv4 Warning Threshold Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/17 19:07:04.330712142 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 17
19:07:04.330: %RIBTENANT-3-ROUTELIMITWARNING_ON: tenant(name:Tenant2, id:23216) ipv4
unicast route limit warning threshold: alarm_on
```

Note ROUTELIMITWARNING_ON: “alarm_on” means the route count has crossed the warning threshold

```
Device# show ip route tenant "Tenant2"

2022/11/18 01:36:02.083288966 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
01:36:02.083: %RIBTENANT-3-ROUTELIMITWARNING_OFF: tenant(name:Tenant2, id:23216) ipv4
unicast route limit warning threshold: alarm_off
```

Note ROUTELIMITWARNING_OFF: “alarm_off” means means for the time being, route count is reduced and it has not crossed the warning threshold.

- The following is a sample output IPv4 Warning Threshold Route-Limit Exceeded Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/18 10:06:35.698972324 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 18
10:06:35.698: %RIBTENANT-3-ROUTELIMITEXCEEDED_ON: tenant(name:Tenant2, id:23216) ipv4
unicast route limit exceeded: alarm_on

2022/11/18 10:06:35.699002244 {iosrp_R0-0}{255}: [ribcmn] [16608]: (info): Failed to
add static route 192.168.202.0/24 to table(name:2, id:0x5) due to tenant(name:Tenant2,
 id:23216) route limit exceeded
```

Note ROUTELIMITEXCEEDED_ON: “alarm_on” means the route count has exceeded tenant route limit

```
Device# show logging process ios start last boot | i route limit

2022/11/17 20:12:02.090953653 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 17
20:12:02.090: %RIBTENANT-3-ROUTELIMITEXCEEDED_OFF: tenant(name:Tenant2, id:23216) ipv4
 unicast route limit exceeded: alarm_off
```

Note ROUTELIMITEXCEEDED_OFF: “alarm_off” means for the time being, route count is reduced and it has not exceeded the tenant route limit.

- The following is a sample output IPv6 Warning Threshold Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/17 19:41:31.886639286 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 17
19:41:31.886: %RIBTENANT-3-ROUTELIMITWARNING_ON: tenant(name:Tenant2, id:23216) ipv6
unicast route limit warning threshold: alarm_on
```

Note ROUTELIMITWARNING_ON: “alarm_on” means the route count has crossed the warning threshold

```
Device# show logging process ios start last boot | i route limit

2022/11/17 19:49:06.553836193 {iosrp_R0-0}{255}: [iosrp] [16608]: (ERR): Nov 17
19:49:06.553: %RIBTENANT-3-ROUTELIMITWARNING_OFF: tenant(name:Tenant2, id:23216) ipv6
unicast route limit warning threshold: alarm_off
```

Note ROUTELIMITWARNING_OFF: “alarm_off” means means for the time being, route count is reduced and it has not crossed the warning threshold.

- The following is a sample output IPv6 Warning Threshold Route-Limit Exceeded Syslog Messages.

```
Device# show logging process ios start last boot | i route limit

2022/11/17 05:07:19.326942097 {iosrp_R0-0}{255}: [iosrp] [17094]: (ERR): *Nov 17
05:07:19.326: %RIBTENANT-3-ROUTELIMITEXCEEDED_ON: tenant(name:Tenant2, id:7888) ipv6
unicast route limit exceeded: alarm_on

2022/11/17 05:07:19.327070153 {iosrp_R0-0}{255}: [ribcmn] [17094]: (info): Failed to
add static route 2001:C0A8:29C::/64 to table(name:2, id:0x1E000002) due to
tenant(name:Tenant2, id:7888) route limit exceeded
```

Note ROUTELIMITEXCEEDED_ON: “alarm_on” means the route count has exceeded tenant route limit.

```
Device# show logging process ios start last boot | i route limit

2022/11/17 05:15:32.132557582 {iosrp_R0-0}{255}: [iosrp] [17094]: (ERR): *Nov 17
05:15:32.132: %RIBTENANT-3-ROUTELIMITEXCEEDED_OFF: tenant(name:Tenant2, id:7888) ipv6
unicast route limit exceeded: alarm_off
```

Note ROUTELIMITEXCEEDED_OFF: “alarm_off” means for the time being, route count is reduced and it has not exceeded the tenant route limit.

View Tenant-Device Mapping on Cisco SD-WAN Validator

The following is a sample output of the **show support orchestrator tenant-uuid-map** command.

```
vBond# show support orchestrator tenant-uuid-map
-------------------------------------------------------------------------------------
|  Type  |             Chassis-num/uuid             | Tenant id list                 |
-------------------------------------------------------------------------------------
| vSmart | 0c90593a-0f40-4890-a980-5e14907482f7     | 18624,6672,27120               |
```

```
-------------------------------------------------------------------------------------
| vSmart | 8a083d5e-1350-4946-932e-237758bb2280     | 12448,6672,10384               |
-------------------------------------------------------------------------------------
| vSmart | c99c50da-3dff-4951-a598-b3cf71530e99     | 18624,12448,27120,10384        |
-------------------------------------------------------------------------------------
| vEdge  | c8k-24d9f68c-8c01-4e6c-813a-959752f30e73 | 18624,12448,6672,27120,10384   |
-------------------------------------------------------------------------------------
| vEdge  | c8k-fdd9c202-8756-4079-9a56-278e6635412b | 18624,12448,6672               |
```

You can view the tenant global ID on a multitenant WAN edge device using the **show sdwan tenant-summary** command. On a Cisco SD-WAN Controller, you can use the **show tenant-summary** command.

View Tenant-Cisco SD-WAN Controller Mapping on Cisco SD-WAN Validator

The following is a sample output of the **show tenant-mapping** command.

```
vBond# show tenant-mapping
VSMART
SERIAL

NUM       TENANT NAMES                                                              TENANT COUNT
-------------------------------------------------------------------------------------------------
12345990  [ "multitenancy-Customer6" "multitenancy-Customer4" "multitenancy-Customer3"
"multitenancy-Customer1" ]  4
12345992  -
                         0
12345994  [ "multitenancy-Customer6" "multitenancy-Customer5" "multitenancy-Customer3"
"multitenancy-Customer2" ]  4
12345997  -
                         0
12345998  -
                         0
12346001  [ "multitenancy-Customer5" "multitenancy-Customer4" "multitenancy-Customer2"
"multitenancy-Customer1" ]  4
```

View Tenant-Mapping on Cisco SD-WAN Controller

The following is a sample output of the **show tenant-summary** command.

```
vSmart# show tenant-summary
tenant-summary max-tenants 24
tenant-summary num-active-tenants 4
                                    TENANT  TENANT
TENANT ORG NAME                     ID      VPN ID
-------------------------------------------------
multitenancy-Customer1              1       1003
multitenancy-Customer2              2       1004
multitenancy-Customer3              3       1005
multitenancy-Customer4              4       1006
```

View Multitenant WAN Edge Device to Cisco SD-WAN Controller Connections

The following is a sample output of the **show sdwan control tenant-connections** command.

```
Device# show sdwan control tenant-connections

PEER LOCAL TENANT
SYSTEM IP COLOR NAME
-----------------------------------------------------------------------------------------------------
172.16.255.19 mpls multitenancy-Customer3
172.16.255.19 mpls multitenancy-Customer2
172.16.255.19 public-internet multitenancy-Customer3
172.16.255.19 public-internet multitenancy-Customer2
```

```
172.16.255.20 mpls multitenancy-Customer4
172.16.255.20 mpls multitenancy-Customer1 Inc
172.16.255.20 mpls multitenancy-Customer2 Inc
172.16.255.20 public-internet multitenancy-Customer4 Inc
172.16.255.20 public-internet multitenancy-Customer1 Inc
172.16.255.20 public-internet multitenancy-Customer2 Inc
172.16.255.24 mpls multitenancy-Customer4 Inc
172.16.255.24 mpls multitenancy-Customer1 Inc
172.16.255.24 mpls multitenancy-Customer3 Inc
172.16.255.24 public-internet multitenancy-Customer4 Inc
172.16.255.24 public-internet multitenancy-Customer1 Inc
172.16.255.24 public-internet multitenancy-Customer3 Inc
```

The PEER SYSTEM IP column shows the IP address of the Cisco SD-WAN Controller the multitenant WAN edge device is connected to. The TENANT NAME entry for a PEER SYSTEM IP shows the name of the tenant organization for which the connection to the Cisco SD-WAN Controller is established.

View OMP Information on a Multitenant WAN Edge Device

- The following is a sample output of the **show sdwan tenant** *tenant-name* **omp peers** command.

```
Device# show sdwan tenant multitenancy-Customer1 omp peers
R -> routes received
I -> routes installed
S -> routes sent

TENANT DOMAIN OVERLAY SITE REGION
ID PEER TYPE ID ID ID ID STATE UPTIME R/I/S
-----------------------------------------------------------------------------------------------------------
23216 172.16.255.19 vsmart 1 1 101 None up 1:13:42:12 24/24/22
23216 172.16.255.20 vsmart 1 1 102 None up 1:13:42:12 24/0/22
```

  The output shows the Cisco SD-WAN Controllers to which the multitenant WAN edge device is connected for the particular tenant and summarizes the OMP exchanges between the Cisco SD-WAN Controllers and the device.

- The following is a sample output of the **show sdwan tenant** *tenant-name* **omp routes** command.

```
Device# show sdwan tenant multitenancy-Customer1 omp routes

Code:

C   -> chosen

I   -> installed

Red -> redistributed

Rej -> rejected

L   -> looped

R   -> resolved

S   -> stale

Ext -> extranet

Inv -> invalid

Stg -> staged

IA  -> On-demand inactive
```

```
U   -> TLOC unresolved

Reo -> reoriginated

                                                    PATH                    ATTRIBUTE


TENANT    VPN    PREFIX              FROM PEER        ID     LABEL    STATUS    TYPE
     TLOC IP          COLOR            ENCAP  PREFERENCE  REGION ID   REGION PATH

------------------------------------------------------------------------------------------------------------------------

23184     1      172.16.11.0/24      0.0.0.0          66     1003     C,Red,R   installed
  172.16.255.15    mpls              ipsec  -            None        65534

                                     0.0.0.0          69     1003     C,Red,R   installed
  172.16.255.15    public-internet   ipsec  -            None        65534

23184     1      172.16.31.0/24      172.16.255.19    5      1003     C,I,R     installed
  172.16.255.14    mpls              ipsec  -            None        65534

                                     172.16.255.19    6      1003     C,I,R     installed
  172.16.255.14    public-internet   ipsec  -            None        65534

23184     1      192.168.11.0/24     0.0.0.0          66     1003     C,Red,R   installed
  172.16.255.15    mpls              ipsec  -            None        65534

                                     0.0.0.0          69     1003     C,Red,R   installed
  172.16.255.15    public-internet   ipsec  -            None        65534

23184     1      192.168.31.0/24     172.16.255.19    7      1003     C,I,R     installed
  172.16.255.14    mpls              ipsec  -            None        65534

                                     172.16.255.19    8      1003     C,I,R     installed
  172.16.255.14    public-internet   ipsec  -            None        65534
```

- The following is a sample output of the **show sdwan tenant** *tenant-name* **omp services** command.

```
Device# show sdwan tenant multitenancy-Customer1 omp services

C   -> chosen

I   -> installed

Red -> redistributed

Rej -> rejected

L   -> looped

R   -> resolved

S   -> stale
```

```
Ext -> extranet

Stg -> staged

IA  -> On-demand inactive

Inv -> invalid

Reo -> reoriginated


ADDRESS                                                                    PATH    REGION

FAMILY   TENANT    VPN    SERVICE  ORIGINATOR     FROM PEER        ID      ID
LABEL    STATUS    VRF
-------------------------------------------------------------------------------------------

ipv4     23184     1      VPN      172.16.255.15  0.0.0.0          66      NA
1003     C,Red,R   1
                                                  0.0.0.0          69      NA
1003     C,Red,R   1
ipv6     23184     1      VPN      172.16.255.15  0.0.0.0          66      NA
1003     C,Red,R   1
                                                  0.0.0.0          69      NA
1003     C,Red,R   1
```

Related per-Tenant OMP commands:

- **show sdwan tenant** *tenant-name* **omp tlocs**
- **show sdwan tenant** *tenant-name* **omp multicast-routes**
- **show sdwan tenant** *tenant-name* **omp ipv6-routes**

Related global OMP commands:

- **show sdwan omp tloc-paths**
- **show sdwan omp summary**

View OMP Information on a Cisco SD-WAN Controller

- The following is a sample output of the **show tenant** *tenant-name* **omp peers** command.

```
vSmart# show tenant multitenancy-Customer1 omp peers
R -> routes received

I -> routes installed

S -> routes sent


                        DOMAIN    OVERLAY   SITE

PEER            TYPE    ID        ID        ID        STATE    UPTIME           R/I/S

-----------------------------------------------------------------------------------

172.16.255.14   vedge   1         1         400       up       23:09:40:04      4/0/0

172.16.255.15   vedge   1         1         500       up       0:14:33:55       0/0/0
```

```
172.16.255.24    vsmart  1         1         103       up        44:06:36:31      4/0/4
```

The output shows the other Cisco SD-WAN Controller serving the tenant and the multitenant or tenant-managed WAN edge devices connected to the Cisco SD-WAN Controller.

- The following is a sample output of the **show tenant** *tenant-name* **omp routes** command.

```
vSmart# show tenant multitenancy-Customer1 omp routes


--------------------------------------------------

omp route entries for vpn 1 route 172.16.33.0/24

--------------------------------------------------

            RECEIVED FROM:

peer            172.16.255.14

path-id         66

label           1005

status          C,R

loss-reason     not set

lost-to-peer    not set

lost-to-path-id not set

    Attributes:

     originator       172.16.255.14

     type             installed

     tloc             172.16.255.14, mpls, ipsec

     ultimate-tloc    not set

     domain-id        not set

     overlay-id       1

     site-id          400

     region-id        None

     region-path      65534

     preference       not set

     tag              not set

     origin-proto     connected

     origin-metric    0

     as-path          not set
```

```
     community        not set

     unknown-attr-len not set

.
.
.

---------------------------------------------------

omp route entries for vpn 1 route 192.168.33.0/24

---------------------------------------------------

            RECEIVED FROM:

peer            172.16.255.14

path-id         66

label           1005
status          C,R

loss-reason     not set

lost-to-peer    not set

lost-to-path-id not set

    Attributes:

     originator       172.16.255.14

     type             installed

     tloc             172.16.255.14, mpls, ipsec

     ultimate-tloc    not set

     domain-id        not set

     overlay-id       1

     site-id          400

     region-id        None

     region-path      65534

     preference       not set

     tag              not set

     origin-proto     static

     origin-metric    0

     as-path          not set

     community        not set

     unknown-attr-len not set
```

The command output shows the routes advertised by multitenant and tenant-managed WAN edge devices for the tenant VPNs.

View Per Tenant Policy Configuration on a Multitenant WAN Edge Device

To view per tenant policy configuration, use the following commands:

- **show sdwan tenant** *tenant-name* **policy from-vsmart**
- **show sdwan tenant** *tenant-name* **policy data-policy-filter**
- **show sdwan tenant** *tenant-name* **policy app-route-policy-filter**
- **show sdwan tenant** *tenant-name* **policy from-vsmart policy data-policy**
- **show sdwan tenant** *tenant-name* **policy from-vsmart policy app-route-policy**

Troubleshoot Multitenant WAN Edge Device Errors

Error Scenario	Log File
Device Onboarding	Cisco SD-WAN Manager: `/var/log/nms/vmanage-server.log`
Device Configuration Pull	Cisco SD-WAN Manager: `/var/log/nms/vmanage-server-deviceconfig-template.log` WAN edge device: `/bootflash/sdwan/cfgloader.log`