

Google Cloud Integration

Table 1: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Cloud Gateway with Google Cloud	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature allows branch sites to access workloads running in the Google Cloud. It also allows branch sites to send and receive traffic across different regions and sites through Google Cloud's global network. As part of the solution, cloud gateways are instantiated in different regions. Cloud gateways consist of a pair of Cisco Catalyst 8000V instances with their interfaces anchored in three different VPCs. This feature supports site-to-cloud and site-to-site connectivity.

Feature Name	Release Information	Description
Cisco SD-WAN and Google Service Directory Integration and Support for Cloud State Audit and Cloud Resource Inventory	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	With the integration of Google Service Directory with the Cisco Catalyst SD-WAN solution, you can discover your applications in the Google cloud using Cisco SD-WAN Manager. You can use the discovered applications to define application-aware routing policies in Cisco SD-WAN Manager. The Audit feature in Cisco SD-WAN Manager is now extended to Google Cloud integration. Use this option to ensure that the states of the objects in Google Cloud stay in sync with Cisco SD-WAN Manager state. Cloud Resource Inventory in Cisco SD-WAN Manager retrieves a detailed list of your cloud objects, their identifiers, the timestamps when such objects were created, and so on.
Horizontal Scaling of Cisco Catalyst 8000V Instances in a Cloud Gateway	Cisco vManage Release 20.9.1	With this feature, you can deploy between two and eight Cisco Catalyst 8000V instances as part of a cloud gateway in a particular region. In earlier releases, you can deploy exactly two Cisco Catalyst 8000V instances as part of a cloud gateway, with each instance deployed in a different zone of a region.

Feature Name	Release Information	Description
Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways	Cisco vManage Release 20.9.1	With this feature, you can configure some cloud gateways to support site-to-site and site-to-cloud connectivity, and other cloud gateways to support only site-to-cloud connectivity. This configuration flexibility is particularly beneficial in some Google Cloud regions that do not yet support site-to-site connectivity. In earlier releases, connectivity type is a global configuration. You configure all the cloud gateways to support site-to-site and site-to-cloud connectivity, or to support only site-to-cloud connectivity.

- Supported Platforms and Instances, on page 3
- Limitations and Restrictions, on page 4
- Overview of Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud, on page 5
- Google Service Directory Integration and Lookup, on page 6
- Connectivity Models, on page 7
- Configure Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud, on page 9
- Service Directory Lookup and Traffic Policies with Discovered Apps, on page 16
- Monitor Connectivity, on page 19
- Audit, on page 19
- View Cloud Resource Inventory, on page 21

Supported Platforms and Instances

Supported Platform

- Cisco Catalyst 8000V

Supported Instances for Google Cloud

- N1-standard-8
- N1-standard-4

Limitations and Restrictions

- Google Network Connectivity Center location support depends on Google offerings. For information on supported locations, see the Google Cloud documentation for information about Google Network Connectivity Center locations.
- Change in service types (standard or premium) is only applicable to cloud gateways that are created after the change only. The change doesn't apply to cloud gateways that are already created.
- Only one service account is supported per Google Cloud project.
- Only one cloud gateway is supported per Google region.
- You can’t create new cloud gateways if the following are in progress:
  - creation or deletion of a cloud gateway
  - creation or mapping of tags
- You can’t edit settings for cloud gateways that are already created.
- If the first cloud gateway has already been created, you can't change the following cloud global settings:
  - IP Subnet Pool
  - Cloud Gateway BGP ASN Offset
- Workload VPC subnets can’t have overlapping IP address spaces.
- For site-to-site connectivity, you must configure a VRF and a centralized control policy to enable the branch-to-site traffic to go through Google Cloud's global network. If there’s failure in Google Cloud's global network tunnel, traffic is expected to be dropped.
- For site-to-cloud connectivity, only one VPN can be mapped to one or more tags.
- When a VPN is mapped to one or more tags, ensure that the combined number of VPCs under such tags don't exceed the VPC peering limit specified by Google Cloud. Intra-tag and tag-to-tag connectivity relies on VPC peering, therefore, the number of VPC peering relations that come into effect because of the intra-tag and tag-to-tag mapping shouldn't exceed VPC peering limit specified by Google Cloud. The default VPC peering limit is 25. Contact Google Cloud support to get this limit increased. See the Google Cloud documentation for information about Google VPC Peering limits.
- Tag-to-tag mapping is always bidirectional.
- For VPN-to-tag mapping for site-to-cloud connectivity, the number of prefixes should not exceed the maximum number of custom route advertisements per BGP session by Google cloud region, which is 200.
- By default, 20 Google Cloud routers are available per project. Site-to-cloud connectivity requires two Google Cloud routers. If site-to-site connectivity is enabled, two additional Google Cloud routers are required per cloud gateway. Therefore, with the default Google Cloud router quota availability, keeping site-to-site functionality disabled, you can create 10 cloud gateways for site-to-cloud connectivity. If you enable site-to-site connectivity as well, a maximum of five cloud gateway can be created. If you require additional Google Cloud routers for more cloud gateway instantiation, request for increase in your Google Cloud router quota through the Google Cloud portal.

- The dynamic routes learnt from workload VPCs at the site-to-cloud transit VPC are not further advertised to the BGP session with Cisco Catalyst 8000V instances in the cloud gateway. Therefore, these dynamic routes are not visible to Cisco Catalyst SD-WAN edge devices.
- IPv6 network addresses are not supported.
- The transit VPC hub in Network Connectivity Center can be deleted only if all the cloud gateways in a Google region are deleted.
- Transport location (TLOC) color **private1** is used only for site-to-site communication. Therefore, you should not use it for other interfaces.

Overview of Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud

This feature enables configuring a pair of redundant Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) instances in Cisco Catalyst SD-WAN cloud gateways, using the Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager. Using redundant routers to form the cloud gateway offers path resiliency to the public cloud. Using the Cisco Catalyst SD-WAN fabric, this feature enables your branch and data center devices to communicate with applications and services in Google Cloud. It also lets you achieve site-to-site connectivity using Google Cloud's global network.

The Cloud OnRamp for Multicloud workflow in Cisco SD-WAN Manager automates the bring-up of the WAN Virtual Private Cloud (VPC) and two transit VPCs in Google Cloud. The workflow also discovers your existing VPCs in geographical Google Cloud regions. You can then create tags for the discovered VPCs in Cisco SD-WAN Manager. These tags are used to map your service VPNs to specific VPCs in your public cloud infrastructure. This mapping enables the following—connectivity to your workload VPCs in Google Cloud, and site-to-site connectivity using Google Cloud's global network.

Horizontal Scaling of Cisco Catalyst 8000V Instances in a Cloud Gateway

Minimum release: Cisco vManage Release 20.9.1

You can deploy a minimum of two and a maximum of eight Cisco Catalyst 8000V instances as part of a cloud gateway in a particular region. By adding more than two instances, that is, horizontally scaling up the number of instances, you can increase the throughput. You can horizontally scale the number of instances between the minimum limit of two and the maximum limit of eight instances based on the required throughput.

When you deploy a cloud gateway with only two Cisco Catalyst 8000V instances, each instance is deployed in a different zone of the region to provide redundancy. When you deploy a cloud gateway with more than two instances, the instances are deployed in two or more zones for redundancy. The instances may not be evenly distributed among the zones.

Note Ensure that all the Cisco Catalyst 8000V instances that are part of a cloud gateway are of the same instance type.

Related Topics

Create and Manage Cloud Gateways, on page 14

Google Service Directory Integration and Lookup

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Google Service Directory is integrated with Cisco Catalyst SD-WAN. Google Service Directory is a catalog of your applications or services in Google Cloud. When you enable Service Directory Lookup in Cisco SD-WAN Manager, this integration allows Cisco SD-WAN Manager to discover your applications that are hosted in Google Cloud, and display them as Cloud Discovered applications. You can then use such applications to define application-aware routing policies.

For information on creating a Google Service Directory, and registering new services in your Google Service Directory, see Google documentation.

How Google Service Directory Lookup Works

1. Google Service Directory lookup is configured from the **Cloud Global Settings** and **Associate Cloud Account** windows in the **Cloud OnRamp for Multicloud** workflow in Cisco SD-WAN Manager.

   For accounts configured as Service Directory Lookup Capable, lookup results are displayed every 20 minutes in the Cisco SD-WAN Manager task bar.

2. Cisco SD-WAN Manager discovers applications in your Google Service Directory by looking up the Google regions associated with the account.

3. Cisco SD-WAN Manager finds the namespaces in the Google region associated with the account, followed by a list of services or applications in each of the namespaces.

4. Cisco SD-WAN Manager fetches the endpoint list and metadata for each service discovered under the namespace. The metadata or service annotation includes attributes such as the traffic profile.

   Cisco SD-WAN Manager looks for the keyword *trafficProfile* key in the list of annotations of the service. Next, it checks if the value against this key is one of the known SLA keywords—data, voice, video, critical, realtime, best-effort, or default. If the value does not match, the traffic profile for the service is set as default. If the keyword *trafficProfile* is not found, the traffic profile is set to default. The traffic profile of the service is automatically translated into an appropriate SLA class, which can be used while creating centralized policies.

   As part of the lookup, Cisco SD-WAN Manager verifies the endpoint list against your current Google Cloud mapping state. This determines whether the service is reachable through Cisco SD-WAN Manager.

5. Each discovered service that is reachable through Cisco SD-WAN Manager is cataloged as a Cloud Discovered application.

   The name of the cloud-discovered application is derived by concatenating the following: Google account name, region name, the name of the namespace, and the name of the service or application in Google cloud. The subfields of the names are joined together with a hyphen. The length of the cloud-discovered application name is subject to a limit of 59 characters. Cisco SD-AVC may have issues in adding the application if the name exceeds this character limit. This can result in the application not being used correctly in policies.

   Therefore, while deciding the name of the application in Google Cloud, we recommend that you consider the logic used for determining the name of the cloud-discovered application in Cisco SD-WAN Manager.

Note If a previously discovered service or application is no longer available in Google Cloud, Cisco SD-WAN Manager removes that application. If such an application is used in a policy, an alarm is generated and you need to remove the application from the policy manually. The packets meant for the removed service could still reach the cloud, but may be dropped after they reach the cloud.

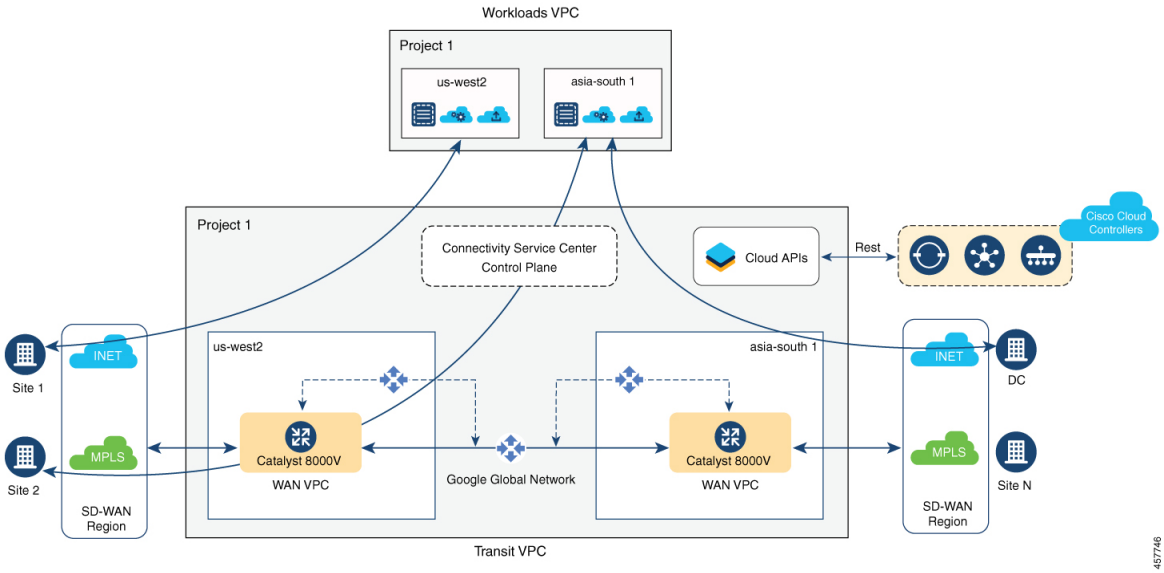
Connectivity Models

The Cisco Catalyst SD-WAN cloud gateway with Google Cloud feature supports the following connectivity models:

Site to Google Cloud

This use case is applicable when a branch site needs to access an application running in a VPC in Google Cloud. In this scenario, a branch site connects to the WAN VPC, which connects to the workload or applications VPC, through the site to cloud transit VPC.

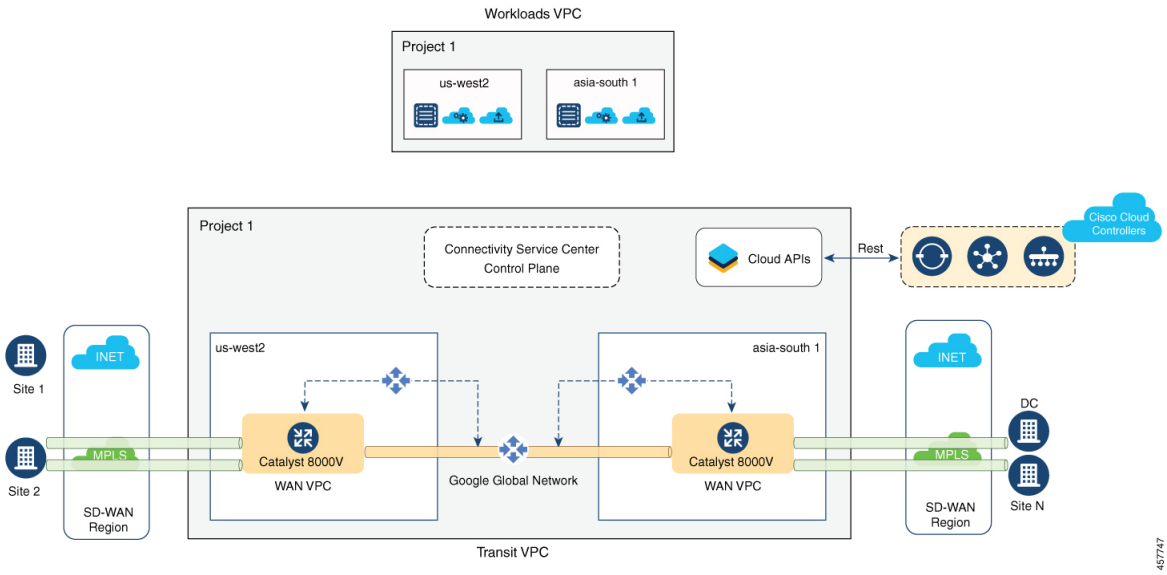
Figure 1: Site to Cloud Connectivity



Site to Site

This use case is applicable for connecting two branches, in different regions, through site-to-site transit VPC using Google Cloud's global network. While it's also possible to connect branches through the public internet, connecting them through Google Cloud's global network ensures optimized transit.

Figure 2: Site to Site Connectivity



Note Site-to-site connectivity can't be enabled between specific cloud gateways or Google Cloud regions. It can be enabled only globally, between all your cloud gateways.

From Cisco vManage Release 20.9.1, after you enable site-to-site connectivity globally for all your cloud gateways, you can configure some cloud gateways so that they don't participate in site-to-site communication (see Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways, on page 8).

Note For the site-to-site connectivity use case, you can define a control policy for intelligent steering of traffic based on your requirement. For example, you may want to use the public internet and Google Cloud's global network for exchanging non-critical and critical traffic flows respectively. For more information, refer to Centralized Policy chapter in *Policies Configuration Guide*.

Decoupled Site-to-Site and Site-to-Cloud Connectivity Configuration for Cloud Gateways

Minimum release: Cisco vManage Release 20.9.1

Cisco vManage Release 20.8.1 and earlier releases: you enable or disable site-to-site connectivity for all the cloud gateways in your deployment using the global settings field **Site-to-site Communication**.

- If you disable site-to-site connectivity in the global settings, you can create cloud gateways only in regions that support site-to-cloud connectivity. These cloud gateways can participate in only site-to-cloud communication.

- If you enable site-to-site connectivity in the global settings, you can create cloud gateways only in regions that support site-to-site connectivity. These cloud gateways can participate in both site-to-site and site-to-cloud communication. However, fewer regions support site-to-site connectivity than regions that support only site-to-cloud connectivity. As a result, you have fewer options to take advantage of site-to-cloud connectivity.

From Cisco vManage 20.9.1: You enable or disable site-to-site connectivity for all the cloud gateways in your deployment using the global settings field **Site-to-site Communication**.

- If you enable site-to-site connectivity in the global settings, while creating a cloud gateway, you can choose whether the cloud gateway will participate in site-to-site communication or not, using the field **Involved in Site-to-site communication**.
  - If you decide that a cloud gateway will not participate in site-to-site communication, you can create the gateway in any region that supports only site-to-cloud connectivity.
  - If you decide that a cloud gateway will participate in site-to-site communication, you can create the gateway in any region that supports site-to-site connectivity. The cloud gateway can participate in both site-to-site and site-to-cloud communication in the supported region.

  As a result, you can create some cloud gateways that participate in site-to-site and site-to-cloud communication, and some that participate in only site-to-cloud communication.
- If you disable site-to-site connectivity in the global settings, you can create cloud gateways only in regions that support site-to-cloud connectivity. You cannot enable site-to-site connectivity for a particular cloud gateway if this type of connectivity is disabled globally.

Related Topics

Configure Cloud Global Settings, on page 12
Create and Manage Cloud Gateways, on page 14

Configure Cisco Catalyst SD-WAN Cloud Gateway with Google Cloud

This section describes how to configure the Cisco Catalyst SD-WAN cloud gateways with Google Cloud feature using Cisco SD-WAN Manager. The section also lists the prerequisites that should be met to be able to configure the feature.

Configuration Prerequisites

- You should have a subscription to Google Cloud. You need your Google Cloud account details to associate your account with Cisco SD-WAN Manager.
- To be able to register you Google Cloud service account in Cisco SD-WAN Manager, ensure that you have at least the following roles configured for your Google Cloud account:
  - Service Account User
  - Compute Instance Admin (v1)
  - Compute Network Admin

- Compute Public IP Admin
- Compute Security Admin
- Hub & Spoke Admin
- Spoke Admin

- Ensure that following Google Cloud APIs are enabled in the relevant project:
  - Compute API,
  - Billing API,
  - Network Connectivity Center Alpha API
- Ensure that Cisco SD-WAN Manager is connected to the internet and is able to communicate with Google Cloud to authenticate your account.
- Ensure that Cisco SD-WAN Manager has two Cisco Catalyst 8000V instances that are free to use for creating the WAN VPC. For throughput requirements that exceed 250 Mbps, Cisco Catalyst 8000V license is required.
- Ensure that all Cisco SD-WAN Control Components (Cisco SD-WAN Manager, Cisco SD-WAN Controller, and Cisco SD-WAN Validator) run Cisco SD-WAN Release 20.5.1 or later, and that Cisco Catalyst 8000V instances run Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or later.
- Ensure that two Cisco Catalyst 8000V instances are attached to the device template. For more information, see Attach Device to a Device Template.

Note Ensure that you attach the Cisco Catalyst 8000V to the factory default template for Google Cloud (Default_GCP_C8000V_Template_V01).

- Ensure that Cisco Catalyst SD-WAN TCP and UDP ports are open. For more information, see Firewall Ports for Cisco SD-WAN Deployments.

Attach Cisco Catalyst 8000V Instances to a Device Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Device Templates** is titled **Device**.

3. From the **Template Type** drop-down list, choose **Default**.

   A list of default templates is displayed.
4. Choose the factory default template for Google Cloud (Default_GCP C8000V_Template_V01).

5. Attach two Cisco Catalyst 8000V instances that are free to use, to the device template. For more information, see Attach Device to a Device Template.

Note After you attach the instances, you should not specify **private1** as the color of the transport location (TLOC) because **private1** is used only for site-to-site communication.

Associate Your Google Cloud Account with Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Setup**, click **Associate Cloud Account**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
4. Enter the requested information:

Field	Description
Cloud Account Name	Enter a name for your Google Cloud account.
Description (optional)	Enter a description for the account.
Use for Cloud Gateway	Choose **Yes** to create a cloud gateway in your account. The option **No** is chosen by default.
Billing ID	(Optional) Enter the billing ID associated with your Google Cloud service account. **Note** Enter the billing ID only after the initial account association. If you provide a billing ID, it goes through an automatic validation process. **Note** This field is visible only if you choose the **Yes** option for the **Use for Cloud Gateway** field.
Service Directory Lookup **Note** This field is available in Cisco vManage Release 20.6.1 and later only.	Choose **Enabled** to allow Cisco SD-WAN Manager to discover services or applications in the Google Service Directory associated with the Cloud Account. The option **Disabled** is chosen by default.

Field	Description
Private Key ID	Click **Upload Credential File**. You must generate this file by logging in to Google Cloud console. The private key ID may be in JSON or REST API formats. The format depends on the method of key generation. For more details, see Google Cloud documentation. **Note** Ensure that the JSON file downloaded from Google Cloud does not have an entry with the name of **universe_domain**.

5. Click **Add**.

Configure Cloud Global Settings

Cloud global settings for a cloud provider apply to cloud gateways for the provider, unless you customize the settings on the **Create Cloud Gateway** page.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**. On the **Cloud OnRamp for Multicloud** window, click **Cloud Global Settings** in the Setup area.

Note The **Enable Configuration Group** option is reserved for future use.

2. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
3. To add global settings, click **Add**. If the cloud global settings are already configured, click **Edit** to modify them.
4. In the **Software Image** field, choose the software image of the WAN edge device for the WAN VPC. This should be a preinstalled Cisco Catalyst 8000V instance.
5. In the **Instance Size** field, from the drop-down list, choose an instance based on your requirements.
6. In the **IP Subnet Pool** field, specify the IP subnet pool for the SD-WAN cloud gateway in Google Cloud. This subnet pool needs prefixes between /16 and /21.
7. In the **Cloud Gateway BGP ASN Offset** field, specify the autonomous system number (ASN) for the cloud gateway for BGP peering. This is the starting offset for the allocation of ASNs for the cloud gateways and Google Cloud routers. Starting from the offset, 10 ASN values are reserved for allocating to the cloud gateways.

Attention This offset value cannot be modified after a cloud gateway is created.

8. For **Intra Tag Communication**, choose **Enabled**. This ensures that VPCs with the same tag can communicate with each other.

9. For **Site-to-Site Communication**, choose **Enabled** for site-to-site transit connectivity using the Google global network. Otherwise, choose **Disabled**.
10. In the **Site-to-Site Tunnel Encapsulation Type** field, choose the encapsulation from the drop-down list.
11. For **Service Directory Lookup Capable**, choose **Enabled** to allow Cisco SD-WAN Manager to discover Google Service Directory applications associated with this Google account. **Disabled** is chosen by default.



Note This field is available for Cisco vManage Release 20.6.1 and later only.

12. In the **Service Directory Poll Timer Value** field, the value is set to 20 minutes by default.

    This field is available for Cisco vManage Release 20.6.1 and later only.
13. In the **Network Service Tier** field, choose one of the Google Cloud service tiers.
    - PREMIUM: Provides high-performing network experience using Google global network.
    - STANDARD: Allows control over network costs.
14. Click **Save** or **Update**.

Discover Host VPCs and Create Tags

After you associate your Google Cloud account with Cisco SD-WAN Manager, you can discover your host VPCs in the regions associated with your Google Cloud account. This workflow shows your cloud infrastructure at a VPC level. You can create new tags for the discovered VPCs, or modify or delete existing tags. Tags are used to manage connectivity between the VPCs and Cisco Catalyst SD-WAN branch VPNs.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Discover** workflow, click **Host Private Networks**.
3. In the **Cloud Provider** field, choose **Google Cloud**.

   A list of discovered host VPCs displays in a table with the following columns: Cloud Region, Account Name, Host VPC Name, Host VPC Tag, Account ID, and Host VPC ID.
4. Click the **Tag Actions** drop-down list to do any of the following:
   - **Add Tag:** Create a tag for a VPC or a group of VPCs.
   - **Edit Tag:** Change the selected VPCs for an existing tag.
   - **Delete Tag:** Delete the tag for the selected VPC.

Create and Manage Cloud Gateways

When the first cloud gateway is created, three reserved VPCs are instantiated—WAN transit VPC, site-to-site transit VPC, and site-to-cloud transit VPC. Cisco Catalyst 8000V instances that are instantiated as part of the cloud gateway are anchored to the VPCs.

This procedure describes how to create a Cisco Catalyst SD-WAN cloud gateway with Google Cloud.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Manage**, click **Create Cloud Gateway**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
4. In the **Cloud Gateway Name** field, enter a name for your cloud gateway.

Note Ensure that the name is in lowercase letters. See the Google Cloud documentation for information about Naming resources and Naming convention.

5. (Optional) Enter a **Description**.
6. In the **Account Name** field, chose your Google Cloud account name from the drop-down list.
7. In the **Region** field, choose a Google region from the drop-down list.
8. (Minimum release: Cisco vManage Release 20.9.1) **Involved in Site-to-site communication**: If the cloud gateway will participate in site-to-site communication, click **Yes**. If the cloud gateway will not participate in site-to-site communication, click **No**.

Note This field is enabled for configuration only when **Site-to-site Communication** is enabled in the global settings. When **Site-to-site Communication** is disabled in the global settings, this field is dimmed.

9. (Minimum release: Cisco vManage Release 20.10.1) From the **Site Name** drop-down list, choose a site for which you want to create the cloud gateway.
10. (Optional) In the **Settings** section, enter the requested information.

Note You can use either the cloud global settings or customize settings for individual cloud gateways using the fields below.

   a. In the **Software Image** field, choose the software image of the WAN edge device to be instantiated in the WAN VPC to connect your site to Google Cloud.
   b. In the **Instance Size** field, choose an instance size for Cisco Catalyst 8000V, based on your requirements.
   c. In the **IP Subnet Pool** field, specify the IP subnet pool to be used for the Google Cloud WAN VPC. This subnet pool needs prefixes between /16 and /21.

Note The IP subnet pool must not overlap with the IP subnet pool specified in Cloud Global Settings.

d. In the **Network Service Tier** field, choose one of the Google Cloud network service tiers from the drop-down list.

- PREMIUM: Provides high-performing network experience using Google Cloud global network.
- STANDARD: Allows control over network costs.

11. UUID (specify 2):

Cisco vManage Release 20.8.1 and earlier: Choose two Cisco Catalyst 8000V licenses from the drop-down list.

Cisco vManage Release 20.9.1 and later: Choose a minimum of two and a maximum of eight Cisco Catalyst 8000V licenses from the drop-down list.

Note

- All the Cisco Catalyst 8000v instances in a cloud gateway must be of the same instance type. Vertical scaling is not supported.
- From Cisco vManage Release 20.10.1, the UUIDs are auto-populated when you choose a site from the **Site Name** drop-down list.

Choose the UUIDs that you attached to the default Google Cloud template.

12. (Minimum release: Cisco vManage Release 20.10.1) In the **Multi-Region Fabric Settings** area, for **MRF Role**, choose **Border** or **Edge**.

This option is available only when Multi-Region Fabric is enabled.

13. Click **Add**.

Map VPC Tags and Branch Network VPNs

To enable VPC to VPN mapping, discover a set of VPCs in one or multiple Google regions and create a tag. Then select the service VPNs that you want to map the VPCs to using the same tags.

How Mapping and Connectivity Work

- You don't have to explicitly create connectivity. Based on VPC tags, connectivity is automatically established when cloud gateways are instantiated in a certain region or when tagging operations take place.
- Connectivity intent for inter-tag and intra-tag mapping can be defined independent of the presence of cloud gateways in various cloud regions. The intent is preserved and mapping is realized when a new cloud gateway or mapping change is discovered.
- When cloud gateways are instantiated in different regions, the mapping intents in those regions are automatically realized.

- Inter-tag and intra-tag mapping is based on VPC peering and automatically enables bidirectional connectivity only.
- Only one service VPN can be mapped to one or more tags.
- You can perform only a single cloud operation, such as, tagging, mapping, or, creation or deletion of a cloud gateway, at a time. When one operation is being performed, the others are locked.
- All cloud operations are time bound. For example, mapping operations time out after 60 minutes. On timeout, the operations are declared as failed. Timeout values cannot be configured.
- The Intent Management page doesn't autorefresh when a new mapping intent is being realized.

Prerequisites for Successful Mapping

- VPCs that are involved in mapping (as part of tags) require at least one subnet.
- Mapping relies on VPC peering. Subnets in peering VPCs must be compliant with RFC1918.
- VPCs cannot have overlapping classless interdomain routing (CIDR) addresses. Overlapping CIDR addresses leads to mapping failure.

View or Edit Connectivity

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Intent Management**, click **Cloud Connectivity**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.

   The window displays a connectivity matrix showing source VPNs, and their destinations. The following legend provides information about the status of the intent:

   - Blue: Intent Defined
   - Green: Intent Realized
   - Red: Intent Realized With Errors

   Click any of the cells in the matrix to get a more detailed status information.
4. To define or record a new intent, click **Edit**.
5. Choose the cells that correspond to a VPN and the VPC tags associated with it, and click **Save**.

Service Directory Lookup and Traffic Policies with Discovered Apps

To use services or applications from your Google Cloud account in Cisco SD-WAN Manager traffic policies, you need to first enable Service Directory Lookup in Cisco SD-WAN Manager, and then use the applications discovered from this lookup to create traffic policies.

Enable Service Directory Lookup

From Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Google Service Directory has been integrated with the Cisco Catalyst SD-WAN solution. With this integration, Cisco SD-WAN Manager can perform a lookup of the Google Service Directories that are part of your Google Cloud Account that is associated with Cisco SD-WAN Manager. Cisco SD-WAN Manager displays the applications or services in your Service Directory as custom applications, which can be used to define routing policies.

For Cisco SD-WAN Manager to be able to search through your Google Service Directory, you need to enable Service Directory Lookup in Cisco SD-WAN Manager.

Naming of Cloud-Discovered Custom Applications

Service Directory Lookup queries Google Cloud for services that you have defined in Google Cloud. Cisco SD-WAN Manager automatically creates custom applications in Cisco Catalyst SD-WAN for the services. To create the name of the custom application, Cisco SD-WAN Manager uses a combination of the following fields, as defined in Google Cloud: Google Cloud account name, Google Cloud region name, service name and namespace. The maximum length for the cloud-discovered custom application name is 59 characters, due to a limitation of the SD-AVC component.

You can view the application list page, showing the custom applications in Cisco SD-WAN Manager. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**, then click **Custom Options** and choose **Lists**. To view the custom applications that Cisco SD-WAN Manager has generated from the services discovered by Cloud OnRamp for Multicloud, click **Cloud Discovered**.

- Cisco SD-WAN Manager 20.6.x handles the 59-character limit as follows: When Cisco SD-WAN Manager uses the four fields described above to create a name for a custom application, if the name exceeds 59 characters, it truncates the name. Truncating the name may lead to name collisions.

  The account name and region name lengths are variable, so it is difficult to predict how many characters remain available for the service name and namespace, while remaining within the 59-character limit.

  To avoid exceeding the character limit, we recommend that when you define services in Google Cloud, use short names for service and name space names. The available length of these names depends on the combined length of the Google Cloud account name and Google Cloud region name.

  - The following example has long account and region names, requiring short service and name space names:

    Account name: gcp-organization-sw-dev
    Region name: australia-southeast1
    Service name: serv1
    Namespace name: nspace1

  - The following example has shorter account and region names, enabling longer service name and name space names:

    Account name: cisco
    Region name: us-west
    Service name: service-xyz
    Namespace name: dev-team

- Beginning with Cisco SD-WAN Manager 20.7.x, you can use longer, more meaningful names for the namespace and service name fields for a service defined in Google Cloud. If necessary, to meet the 59-character maximum, Cisco SD-WAN Manager may truncate part of the service name.

Cisco SD-WAN Manager applies a limit of 12 characters for the Google Cloud account name, a limit of 23 characters for the Google Cloud region name, and a limit of 8 characters for the namespace. Three (3) characters are used for a separator (-) in the custom application name. To remain within the 59-character limit without a truncated service name, use a maximum of 13 characters when providing a service name for a service in Google Cloud. If you use a longer name and the combination of these fields exceeds 59 characters, Cisco SD-WAN Manager truncates the name. If truncating the name causes a name collision with a previously defined custom application, Cisco SD-WAN Manager displays an alarm on the application list page. (Instructions for opening the application list page appear above.)

Before You Begin

Ensure that SD-AVC is enabled in Cisco SD-WAN Manager.

- Enable SD-AVC in Cisco SD-WAN Manager:
  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
  2. For the desired Cisco SD-WAN Manager instance, click **...**, choose **Edit**, and check the **Enable SD-AVC** check box.
- Ensure that Service Directory APIs are enabled for your Google Cloud account.

Enable Service Directory Lookup

1. Enable Service Directory Lookup from the **Associate Cloud Account** window in the **Cloud OnRamp for Multicloud** workflow.

   For more information, see the *Associate Your Google Cloud Account with Cisco SD-WAN Manager* topic in this chapter.
2. Under **Cloud Global Settings** enable the Google Account associated with Cisco SD-WAN Manager as **Service Directory Lookup Capable**, and configure the **Service Directory Poll Timer Value**.

Create Traffic Policies Using Cloud Discovered Apps

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Custom Options**.
3. Under **Centralized Policy**, click **Lists**.

   You are redirected to the **Application** section under **Policies**.
4. Click **Cloud Discovered**.

   A list of applications discovered from Google Service Directory Lookup is displayed.
5. Click **Map Traffic Profiles**. In the dialog box that appears, you can set or modify the traffic profiles for the discovered service.
6. For each of the traffic profiles, click **vManage SLA Classes** and choose an SLA class to map the application to.
7. Click **Save**.
8. Next, create an application list to include the cloud discovered applications.

9. To create a traffic policy using the discovered applications, click **Custom Options** > **Traffic Policy**, and then click **Add Policy**.

   To configure traffic rules on the application list for the cloud discovered applications, refer to Configure Traffic Rules section in the Application-Aware Routing chapter in *Policies Configuartion Guide*.

Monitor Connectivity

When you create a new cloud gateway, you can verify the bring-up and reachability of the Cisco Catalyst 8000V instances provisioned inside the cloud gateway.

Option 1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Cloud**, the **Network Snapshot** displays a summary of the cloud gateways, host VPCs, and WAN edge devices for various cloud providers.

   The upward arrow next to the WAN edge devices indicates the number of devices that are up. Click the arrow to view additional details of the devices.

Option 2

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. In the **Workflows** section, click **Cloud Connectivity** under **Intent Management**.
3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.
4. Click any cell on the page to view the connectivity status of VPNs and VPC tags.

Audit

Starting from Cisco vManage Release 20.6.1, the **Audit** option in the **Cloud OnRamp for Multicloud** workflow is enabled for Google Cloud. Use this option to verify whether the Google Cloud state is in sync with Cisco SD-WAN Manager state. As part of the audit, if the cloud state is identified as out of sync with Cisco SD-WAN Manager state, Cisco SD-WAN Manager automatically tries to resolve the issues and bring parity in the states.

As part of the audit mechanism, the existence of cloud objects, their interrelationships, and their states are all verified against the connectivity intent defined in Cisco SD-WAN Manager. Cisco SD-WAN Manager then takes corrective action is taken if a mismatch is identified.

The following table provides details about the audit discrepancies and fixability for Google Cloud:

Table 2: Examples of GCP audit discrepancies

Anomaly / Trigger	Audit Findings / Error Message
Missing Network Connectivity Center (NCC) spokes	**Report Type**: NCC_HUB **Details**: Spoke <spoke-name> in region <region-id> is missing.

Anomaly / Trigger	Audit Findings / Error Message
Missing NCC Hubs	**Report Type:** NCC_HUB **Details:** NCC Hub: <Hub Name> not found.
Missing Google cloud routers (GCRs) - primary, secondary, or both	**Report Type:** GCR **Details**: <GCR Name> not found.
Missing site-to-cloud peering of VPCs mapped to VPNs in Cisco SD-WAN Manager	**Report Type**: MAPPING **Details**: Connectivity element was missing from response: [srcType:VPN dstType:VPC dst:<dst-vpc-id>]
Missing VPC peering of VPCs that are mapped to other VPCs in Cisco SD-WAN Manager	**Report Type:** MAPPING **Details:** Connectivity element was missing from response: [srcType:VP dstType:VPC dst:<dst-vpc-id>]
Missing custom routes	**Report Type:** Mapping **Details:** Connectivity element was missing from response: [srcType:VPI src:<C8Kv-Device-UUID>::<vpn-id> dstType:VPC dst:<vpc-id>]
Missing Border Gateway protocol (BGP) sessions	**Report Type**: MAPPING **Details**: BGP session is missing in GCR
Stale BGP sessions	**Report Type**: MAPPING **Details**: Stale prefixes found in BGP Sessions
Removal of a cloud gateway or any of its components	**Report Type:** CGW_ROUTER **Details:** CGW Router: [<CGW Instance name> <region-id>] Couldn't fi cloud (Irrecoverable error, user intervention needed to fix things in cloud
Issues with host VPCs with overlapping CIDRs	**Mapping Failure**: Additional details: Overlapping subnets part of mappi Mapping: VPN:<vpn id> --> <s2c vpc name, vpc-id, vpc-subnet> / <vpc na **Report Type**: Mapping **Details**: vpnAttachSpec with tunnelId: <c8kv uuid>::<vpn id> was miss
Issues with site-to-site VPCs	**Report Type:** TVPC **Details:** TVPC: [<s2c-vpc-id> S2S_VPC] not found in cloud (Irrecoverabl needed to fix things in cloud).
Issues with site-to-cloud VPCs	**Report Type:** TVPC **Details:** TVPC: [<s2c-vpc-id> S2C_VPC] not found in cloud (Irrecoverabl needed to fix things in cloud).
Issues with WAN VPCs	**Report Type:** TVPC **Details:**TVPC: [<s2c-vpc-id> WAN_VPC] not found in cloud (Irrecoverabl needed to fix things in cloud).

Anomaly / Trigger	Audit Findings / Error Message
Invalid GCP Credentials	**Report Type:** Account **Details:** Invalid GCP Credentials found for account Id <acc-id>

Note Audit-fix performs the same steps in both on-demand fix (that is, clicking the **Fix Sync Issues** button) and periodic audit followed by auto-correct.

View Cloud Resource Inventory

Starting from Cisco vManage Release 20.6.1, you can use the **Cloud Resource Inventory** option in Cisco SD-WAN Manager is enabled for Google Cloud. Use this option to view details of the cloud objects and their identifiers for the Google Cloud account associated with Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu. choose **Configuration** > **Cloud OnRamp for Multicloud**.
2. Under **Manage**, click **Gateway Management**.

   Your existing cloud gateways are displayed.
3. For the desired cloud gateway, click **…** and choose **Cloud Resource Inventory**.

The Cloud Resource Inventory options retrieves the following information for the selected cloud gateway:

- VPCs: WAN, site-to-site, and site-to-cloud VPCs.
- VPC Subnets: WAN, site-to-site, and site-to-cloud in each Google Cloud region associated with the Google Cloud account.
- VMs: A pair of Cisco Catalyst 8000V instances in each Google Cloud region.
- Google Cloud Routers: A pair each of site-to-cloud and site-to-site Google Cloud routers in each region.
- Hubs: An instance each of site-to-site and site-to-cloud Google Global Network hubs.
- Spokes: A pair of spokes from each region that is connected to the site-to-site and site-to-cloud hub.