Provisioning

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.

Getting Access to Cloud Hosted Controllers

Cisco managed Cloud Hosted controllers are by default closed for management access. Cisco does not allow access to 0.0.0.0/0 to the Cloud Hosted Cisco Catalyst SD-WAN Controllers for security reasons. It is expected that you have specific public IP prefixes within your enterprise VPN that you access from and hence only those will be allowed to be opened for access. You can restrict access by requesting to allow only https and ssh to be on the allowed list, for your given source IP prefixes.

Cloud-hosted controllers have private IP addresses on their interfaces. Each private IP address has a 1:1 NAT mapped to a public IP address on the cloud. These IP addresses do not change irrespective of whether the interface is configured to use static IP or DHCP. The IP addresses only change when the instance is recovered or replaced.

The allowed-list is applied to all the network interfaces of all the controllers that have public IP addresses.

Update Inbound Rules

You can update the allowed-list applied to your cloud-hosted controller set based on the overlay type.

1. Shared tenant overlay: To update or view the allowed-list applied to your cloud-hosted controller set, open a case with Cisco TAC support.

   You can request support for the following:

- Provide upto 5 IP prefixes to be allowed on the access-list
- Allow only `https` access to the IP prefixes for the web login to the Cisco SD-WAN Manager portal

2. Dedicated Overlay: To enable Cisco-hosted, cloud-based, single tenant dedicated controllers to add, delete, or modify cloud security group allowed-lists, use one of the following options:
   - You can login into the Cisco Catalyst SD-WAN Portal at https://ssp.sdwan.cisco.com and manage the access-list. You need to be the Cisco PNP Smart Account admin for the Smart Account where the overlay controller profile is based.
   - You can provide up to 200 IP prefixes to be allowed on the access-list.
   - You can open a Cisco TAC support case and provide the following information:
     - Overlay/VA name
     - Cisco SD-WAN Manager IP/FQDN
     - IP address
     - Specify whether to mark an IP address as allowed for all traffic or selected traffic (for example https, SSH, and so on).

Only the Smart Account administrator can access the Cisco Catalyst SD-WAN Portal which is used to view and perform operational tasks related to a customer's hosted-controller infrastructure, such as viewing the controllers' IP addresses and modifying the controllers' IP access lists. To disable SA administrator privileges for users, go to the Manage Smart Account section in Cisco Software Central, and remove the users as Smart Account administrators. Alternatively, use the IDP (identity provider) onboarding feature to grant trusted users access to the Cisco Catalyst SD-WAN Portal.

Cloud Hosted Controller IP Provisioning

The Cisco SD-WAN Manager fully qualified domain names (FQDN) are mapped to the VPN 512 public IP and is used for management access. The edge nodes, however, form a tunnel with the transport interface of the Cisco SD-WAN Manager, which is on VPN 0 and has a different public IP address. Cisco assigns FQDN to Cisco SD-WAN Manager and Cisco SD-WAN Validator for cloud hosting.

HTTP/HTTPs access is not available for Cisco SD-WAN Validator, and only Cisco SD-WAN Manager has web server and access to web/https.

Each controller instance has a private IP interface that is NATed to a public IP 1:1. In general, public and private IP addresses will not change for the instance interfaces. Private/Public IPs of Cisco SD-WAN Validator/Cisco Catalyst SD-WAN Controller/Cisco SD-WAN Manager changes only when an instance needs to be replaced or moved to a new region.

All customer edges communicate with the controllers via the DTLS/TLS ports. You can configure your on-prem firewall, either to any IP (0.0.0.0) for these specific DTLS/TLS ports, or may open it just to the current public IPs of the cloud controllers. For more information on DTLS/TLS ports, refer to Table 3 in Ports Used by Cisco SD-WAN Devices Running Multiple vCPUs section.

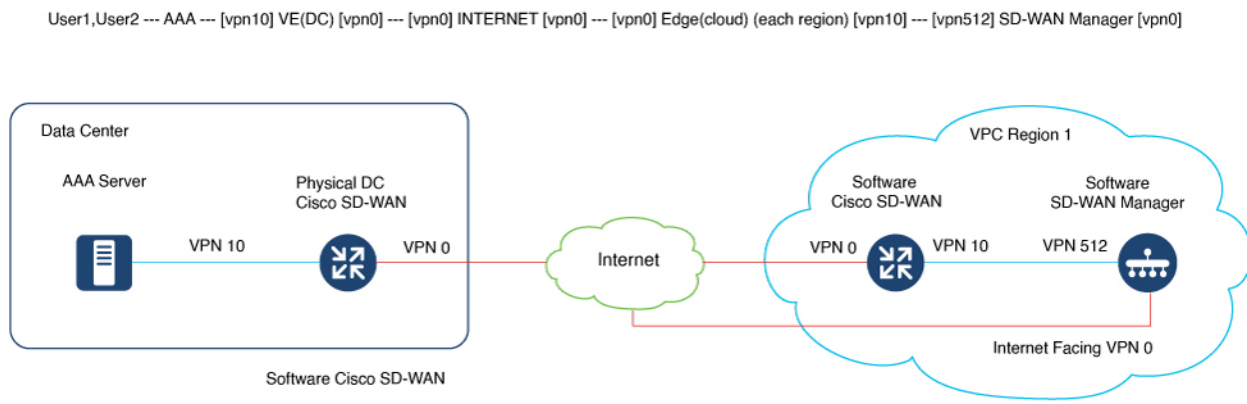
Custom IP Prefixes for Cloud Hosted Controllers

Note Custom IP prefixes are applicable only if you use Cisco-hosted, cloud-based, dedicated single tenant controllers. These are not applicable for shared tenant overlays.

There are certain use-cases, where you may need custom network prefix-based IPs on the cloud controller interfaces for management access and control. For example,

- To access the management VPN 512 of Cisco SD-WAN Manager and Cisco SD-WAN Validator or Cisco SD-WAN Controller devices over Cisco Catalyst SD-WAN tunnel with AAA or TACACS based authentication.
- To send syslog from Cisco SD-WAN Manager over VPN 512 to a syslog server over Cisco Catalyst SD-WAN tunnel.

Figure 1: AAA TACAS



By default, the Cisco-managed cloud hosted controllers are deployed with 10.0.0.0/16 based subnets, including the VPN 512 subnet. If you add the cloud Cisco Catalyst SD-WAN and bring the VPN 512 subnet as a reachable subnet within your fabric, it might conflict with an existing subnet.

In such cases, you need to share a /24 prefix for each of the two regions of deployment of controllers. These IP prefixes are used to create the controllers, and the subnets are then configured to be available within the Cisco Catalyst SD-WAN fabric.

Request for Cloud Gateways for Post Overlay Provisioning:

Open a case for CloudOps at TAC-CSOne with the following details:

1. To enable AAA or TACACs, you need to provide IP prefixes, unused within your existing fabric, that you can use to create the controllers (original controllers are shutdown, snapshotted, and cloned back).

   Each region in which the controllers are set up has one /24 Cisco Catalyst SD-WAN fabric wise unique custom subnet. Each overlay has two regions, so we need two subnets.

2. Admin credentials to the Cisco SD-WAN Validator, Cisco SD-WAN Controller and Cisco SD-WAN Manager devices.

You can provide credentials at the start of the actual change window.

3. You can schedule eight-hour maintenance window after the preapproval and prechecks completed by CloudOps engineer.
4. Enable DNS for Cisco SD-WAN Validator and configure all the controllers prior to start of the process.
5. Ensure that GR is set to default of 12 hours or more on Cisco Catalyst SD-WAN or Cisco SD-WAN Controller devices.
6. Reserve two available Cloud Cisco Catalyst SD-WAN UUIDs through PNP and attach to Cisco SD-WAN Manager.
7. Supported only for Single Tenant Single Node Cisco SD-WAN Manager overlays and Single Tenant Cluster Node Cisco SD-WAN Manager overlays for provisioned controllers, and all new to-be-provisioned controller sets. This feature is not supported for Cisco Multi-tenant Cisco SD-WAN Manager cluster overlay.
8. It is recommended that Cisco SD-WAN Manager have templates attached to Cisco SD-WAN Validator, Cisco SD-WAN Controller, and if existing cloud Cisco Catalyst SD-WAN devices from Cisco.

Configuration of Cloud Gateways Post Cisco Provisioning

1. Once Cisco CloudOps has completed the provisioning of the cloud gateways next to the cloud hosted controllers, CloudOps shares the public & private IP assignments for each cloud gateway to the customer. They are in the format (VPN 512, VPN 0, VPN X).

   Cisco CloudOps will share the credentials for the newly provisioned cloud gateways.
2. The cloud gateways have their VPN 512 & VPN X interfaces in the same subnet as the VPN 512 of the controllers in that region.

   The cloud gateways provisioned by the Cisco CloudOps are specifically for the AAA/TACACS purpose and always created in the above network layout format.

   If there are any reachability issues to the cloud gateway, the issue generally lies with the interface IP or route configurations in the cloud gateway.
3. Also, note that the public & private IPs are 1:1 NAT'd and assigned to the cloud gateway interfaces. The gateway interface itself may be configured with dhcp, but it will always get the same IP from Cloud.

   For VPN X interfaces, you will need to configure the static IP, exactly as the one shared by Cisco CloudOps.

   Random IPs within the subnet cannot be used.
4. The cloud gateways are subject to the same Inbound allowed access-list as the controllers, as they are provisioned in the same unique environment per overlay.

   You must login via SSH to the gateway public IPs and the credentials provided.
5. You must now configure the new cloud gateways with the necessary configurations. For example, site-id, system IP, organization name, Cisco SD-WAN Validator DNS or IP, and so on.
6. If you are using Enterprise root-ca, then you must upload and install the same on the cloud gateways as well.

7. You may configure AAA/TACACS on the Cisco SD-WAN Manager with auth-fallback to local with local having the viptelatac/ciscotacro/ciscotacrw user enabled. This allows Cisco support to login and troubleshoot issues when required.

8. You would need to acquire an unused cloud gateway UUID from the device list of the Cisco SD-WAN Manager, one per cloud gateway provisioned.

   If you don't have any cloud gateway UUID available in the WAN Edge Device list on your Cisco SD-WAN Manager, then you may need to login into the Cisco PNP portal, on the overlay's associated Smart Account and Virtual Account, and Add Software Devices (VEDGE-CLOUD-DNA) and then Sync Smart Account on the Cisco SD-WAN Manager.

9. You must then activate the UUID on the cloud gateways to allow them to be authenticated by the Cisco SD-WAN Manager and join the Cisco Catalyst SD-WAN fabric.

10. You must configure the controllers' (Cisco SD-WAN Manager, Cisco SD-WAN Validator, Cisco SD-WAN Controller) VPN 512 with a specific static route for customer's Enterprise subnets (from customers admin team intend to access the controllers for management) to point to the cloud gateway's VPN X static IP.

11. For an overlay hosted by Cisco on Azure, please open a Cisco TAC case and provide the specific enterprise subnet prefixes, from where the connectivity to the VPN 512 of the controllers is required.

    The Azure subnet default gateway is the defacto gateway even if you configure the gateway service VPN IP to be the gateway for your enterprise subnets. Hence in addition to your configuration on VPN 512 on the controllers, there is additional configuration needed on the Azure side. Cisco will help apply an Azure Route Table (RT) entry for each of the necessary Enterprise subnets and also enable IP forwarding on the cloud gateway interfaces.